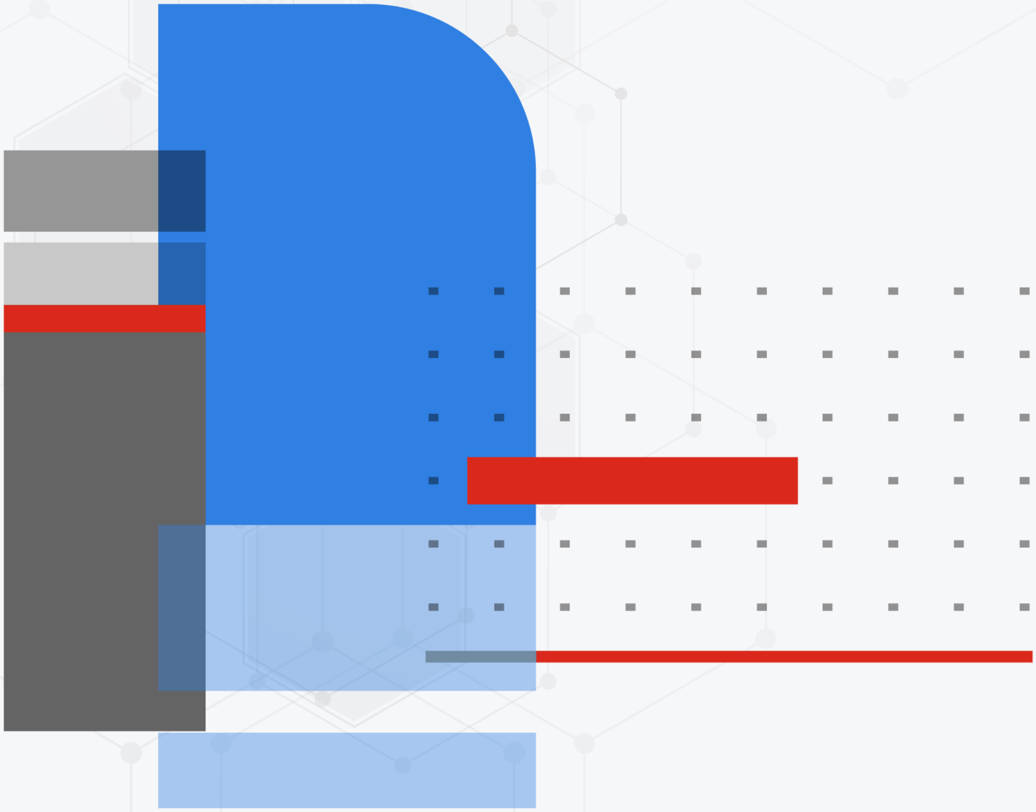
FORTINET

Release Notes

FortiDeceptor DaaS 24.3



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

October 15, 2024
FortiDeceptor DaaS 24.3 Release Notes
50-243-1079605-20241015

TABLE OF CONTENTS

Change Log

Date	Change Description
2024-10-03	Initial release version 24.3.
2024-10-15	Updated FortiDeceptor DaaS Version 24.3 on page 6.

Introduction

FortiDeceptor DaaS Cloud is a cloud-based platform providing cyber Deception-as-a-Service.

Cyber deception has emerged as an effective and offensive threat detection technology that offers protection for IT/IoT/OT networks and infrastructure. Deception technology can be used across enterprise networks by placing decoys, deception tokens (breadcrumbs), and lures.

FortiDeceptor DaaS provides early detection and isolation of sophisticated human and automated attacks by deceiving attackers into revealing themselves.

Key features:

- FortiDeceptor DaaS provides an intuitive method to configure and monitor deception assets with Wizard-based deployment. FortiDeceptor creates Decoys based on default templates. These Decoys span several OS types, including Windows Desktop/Server, Linux, VPN, IoT, and OT. Once deployed, it automatically performs asset (active/passive) discovery, creates asset inventory, and recommends optimized decoy placement.
- Deployment deception decoys and lures from the cloud platform communicate directly to on-premise or cloud networks.
- FortiDeceptor DaaS Captures and analyzes malware that is detected by the Deception decoys and provides detailed forensics, collects IOCs and TTPs.
- Infected endpoints that are detected by the Deception decoys can be quarantined away from the production network.
- Integration with Fortinet Security Fabric and third-party security controls like FW, SIEM, SOAR, EDR, NAC, and SANDBOX.

FortiDeceptor DaaS Version 24.3

This document provides information about FortiDeceptor DaaS version 24.3 build 80.

What's new

FortiDeceptor DaaS 24.3 includes the following new features and enhancements:

Dynamic malware analysis

- FortiDeceptor DaaS supports FortiSandbox for dynamic malware analysis captured by the Deception decoys.

Network

- FortiDeceptor DaaS uses a remote EDGE device with the Layer2 tunnel for decoy connectivity. This network tunnel is a key platform component, therefore we have added an alert notification email when a remote EDGE device goes offline. In addition, we added a GUI widget that will present the tunnel's real-time status, including deployment network information, tunnel online/offline status, tunnel uptime and creation time.

Tunnel traffic encryption

- FortiDeceptor DaaS requires end users to manually copy the authentication key from the DaaS GUI to the remote EDGE device for tunnel traffic encryption. We have improved and introduced a new command tunnel that allows the remote EDGE device to download the authentication key automatically. This provides more flexibility to the DaaS admin, allowing them to refresh the tunnel encryption at any time.

Device status

- We have added a new widget to show the EDGE device status and related decoys.

Organization Units (OU)

- FortiDeceptor DaaS data view support for organization OU is now similar to the DaaS MSSP. This allows organization users to select an OU and access a specific data view page to view incidents for all accounts under that OU.

FortiCloud profiles

- The current FortiDeceptor DaaS service hosts a separate version of profile and permission control, thus requiring the user to configure the profile and permission settings on both the FortiCloud portal and DaaS service side. We have improved the user experience by allowing the end user to configure the profile settings on the FortiCloud portal side. When the end user logs in, the user settings are automatically synced to the DaaS service side.

General

- The FortiDeceptor DaaS Deployment Wizard is based on fixed GUI modules to provide service configuration interfaces for different decoy templates. We have implemented a dynamic GUI conductor with a list of configuration modules and corresponding service definitions to expand and improve the Deployment Wizard.
- We have improved the FortiDeceptor DaaS TTU component for more functionality and scalability.

Product integration and support

Supported models	FortiDeceptor Edge FDC100G, FortiDeceptor Edge virtual appliance (FDCVME)
Virtualization Environment	• AWS • Azure • GCP • Hyper-V • KVM • Nutanix Acropolis • VMware ESXi 5.1, 5.5, 6.0, 6.5, 6.7 and 7.0.
Browser support	• Microsoft Edge version 42 and later • Mozilla Firefox version 61 and later • Google Chrome version 59 and later • Opera version 54 and later • Other web browsers may function correctly but are not supported by Fortinet.
Supported languages	English

Known issues

Bug ID	Description
910763	*Deployment*: Remove support for deploying different decoys with the same IP.
998112	*Fabric*: Configuring different agents is not supported on the same PAN device.
998495	*Deployment*: Block duplicate IPs under the same VLAN license.
1017051	Add support for external IdP users.
1024453	Improve the format of emails sent to DaaS administrators.
1028592	*Reports*: Improve the PDF of the Incident report.
1057292	*GUI*: Allow users to right-click to copy in a table.
1079162	*Deployment*: XMPP and ScadaBR decoy details are missing the *URL* row.
1083036	*Analysis*: VNC appears a *GTP-C* in the *Protocol* column of the *Analysis* page.

Resolved issues

Bug ID	Description
921800	Integrate FortiDeceptor DaaS with FortiSandbox Cloud for suspicious files inspection.
992421	FortiDeceptor DaaS does not support overlap for different devices.
1018612	*Fabric*: Improve tool tips and messaging.
1032903	*Incidents*: CSV export should only include the *Incident* column.
1053110	FortiDeceptor DaaS submissions should use the same name in FortiSandbox logs and reports.
1077842	*Deployment*: Improve the *Deployment Wizard* to support dynamic templates.
1080069	Remove Vue2
1082956	*GUI*: Add a scroll bar to the *Company* dropdown list.

www.fortinet.com

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.