Release Notes

FortiDeceptor DaaS 25.3.a

F⊡RTINET.

TABLE OF CONTENTS

Change Log

Date	Change Description
2025-10-23	Initial release version 25.3.a.

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 25.3.a

This document provides information about FortiDeceptor DaaS version 25.3.a build 80.

What's new

FortiDeceptor DaaS 25.3.a includes the following new features and enhancements:

Incident Alerts Reporting & Email Alerts

FortiDeceptor DaaS provides a new email alerting module that allows incident alerts to be sent via email.

The FortiDeceptor DaaS email alerting module allows sending incident alerts using email:

- To multiple recipients.
- Based on a specific incident alert parameter.
- Based on several incident alert parameters.

SIEM & Logs

FortiDeceptor DaaS now has the ability to send alerts over syslog to a local log server system like SIEM, FortiAnalyzer, and more.

The FortiDeceptor DaaS configuration will allow the configuration of a particular FortiDeceptor edge device as an agent and pushes the logs from the DaaS platform to the on-premise or cloud edge device. The FortiDeceptor edge device will then redirect the logs to remote log servers like SIEM, FortiAnalyzer, and more.

General

FortiDeceptor DaaS continues to publish more decoys, offering the same features as the FortiDeceptor on-premise version.

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

FORTINET