

Release Notes

FortiDeceptor DaaS 26.1.0



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



January 28, 2026

FortiDeceptor DaaS 26.1.0 Release Notes

50-254-1249873-20250128

TABLE OF CONTENTS

Change Log	4
Introduction	5
FortiDeceptor DaaS Version 26.1.0	6
What's new	6
Product integration and support	7

Change Log

Date	Change Description
2026-01-28	Initial release version 26.1.0.

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 26.1.0

This document provides information about FortiDeceptor DaaS version 26.1.0 build 80.

What's new

FortiDeceptor DaaS 26.1.0 includes the following new features and enhancements:

Multiple region selection

Region checks now occur at login. When you sign in to FortiDeceptor DaaS, your account's region is validated. If your account is associated with the wrong region, you will be prompted to switch regions before continuing. Changing regions does not transfer configuration or deployed assets; only licensing is retained. You can also change your region at any time from the FortiDeceptor DaaS toolbar.

Product integration and support

Supported models	FortiDeceptor Edge FDC100G, FortiDeceptor Edge virtual appliance (FDCVME)
Virtualization Environment	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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



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.