FortiDeceptor

A Non-Intrusive, Agentless Deception Solution to Detect and Stop Active In-Network Attacks

FortiDeceptor is Fortinet's non-intrusive, agentless deception platform that puts the power back into the hand of defenders, with the ability to deceive attackers into engaging with fake assets and ultimately revealing themselves.

A force multiplier to current security defenses, FortiDeceptor combines the concept of honeypot with threat analytics and threat mitigation capabilities. This is achieved by distributing a layer of deception assets across the network—decoys and tokens, such as fake keys and files on endpoints and servers—and creating a system of traps that look and operate like any other real asset across IT, OT, and IoT networks, intended to deceive, detect, and isolate known and unknown human and automated attacks.

With FortiDeceptor, instead of waiting for the threat actor to make a mistake and then detect their presence, you can now embrace an active defense approach where any step the attacker takes—whether they try to escalate privileges or run malware—becomes an opportunity for you to detect them.

Feature Benefits

- Provide actionable insights, increase SOC effectiveness
- Extend support to challenging areas (IoT and OT environments)
- Provide early, substantiated warning (no false-positives)
- Scale automatically as the risk level increases
- Detect new or unknown threats and malicious insiders
Early Threat Detection, Minimal Network Impact

FortiDeceptor works by deploying and running decoys from the FortiDeceptor console using available IP addresses. As decoys leverage unused IP addresses across the different network segments, they do not impact network availability and, to the attacker, they seem like an integral part on your network. These IP addresses do not correspond to any real host or device on the network.

The FortiDeceptor platform consists of several deception components that together provide an authentic and scalable layer of deception assets that are identical to other assets across your network. These decoys are fake assets, such as industrial control systems, medical devices, ATMs, tank gauges, POS devices, IoT devices, network infrastructure, and more, that run real operating systems and services and generate fake but limited traffic to lure attackers to them, diverting them away from sensitive assets. FortiDeceptor provides an extensive inventory of decoys. You can also ‘bring your own decoys’ and upload your own golden images.

To expand the deception layer event further, FortiDeceptor places breadcrumbs (or tokens) on real endpoints and servers. These are fake documents, files, or fake credentials, that attackers look to leverage to move laterally or encrypt. The breadcrumbs, which are indistinguishable from real files and credentials, are designed to deceive the attacker or malware to laterally move to the decoy. FortiDeceptor immediately detects any use of fake credentials, generates alerts, and automatically isolates the endpoint using built-in endpoint isolation capabilities or security orchestration, automation, and response (SOAR) playbooks.

Accelerated Incident Response

The solution generates high-fidelity, zero false-positive alerts, providing security teams with a unique advantage over malicious activity, and unparalleled visibility to detect and stop attacks, credential thefts, lateral movement, and malware activity. It also provides compensating security control when patching or when other security controls aren’t an option. A good example of this is in OT environments where patches aren’t available; even when patches are available, the time and effort required for maintenance is arduous.

Once a malware or human attacker engages with a fake or a decoy asset, an alert is generated and sent to security information and event management (SIEM), SOAR, or any threat intelligence platform you’re using. The decoy then starts capturing and analyzing the activities in real time and generates threat intelligence using eight built-in intelligence engines for detailed and accurate analysis.

FortiDeceptor does not require highly skilled security analysts to deploy or manage the solution. It centralizes and automates the entire process—from deception deployment to evidence analytics to quarantined and unquarantined attacks to the implementation of dynamic protection layers.
Protection Against Evolving Threats

To combat emerging threats, FortiDeceptor enables on-demand creation of deception decoys based on newly discovered vulnerabilities or suspicious activity, providing automated, dynamic protection across IT, OT, and IoT environments.

• **Implement zero-day protection**: Attackers often target vulnerable assets first. With FortiDeceptor's advanced outbreak feature, you can now purposefully deploy decoys with recently disclosed vulnerabilities to attract, automatically detect, and quarantine malicious activities early in the kill chain. When a vulnerability is reported by FortiGuard Labs, the vulnerability emulator is automatically pushed as a feed to the outbreak decoy without requiring a software update.

• **Rapid threat hunting** to identify indicators of compromise (IOCs): FortiDeceptor's integration with SOAR provides on-demand deception asset deployment, triggered by SOAR playbooks to help hunt and quarantine any malicious activity. When suspicious activity is detected, a SOAR playbook can automatically initiate the deployment of decoys and tokens in that specific segment to help detect an attack and capture intel.

In addition, FortiDeceptor offers integrations with leading security tools, as well as with the Fortinet Security Fabric, providing orchestrated threat mitigation and enriched attack intelligence.

Deception for OT and IoT environments

OT environments are diverse, with numerous, multi-vendor devices and systems often designed without built-in security. Hardening mostly legacy systems via monitoring agents or security patching to mitigate risks is not always an option due to continuity, costs, patch availability, and more. FortiDeceptor's decoys simulate various types of IT, OT, ICS, and IoT devices, as well as critical applications such as SAP and ERP that can be deployed across all levels of the Purdue model.

FortiDeceptor works by automatically running active and passive asset discovery, creating asset inventory, and recommending optimized decoy placement across the IT and OT network. It can operate in online or air-gapped modes, and is also available as an industrially-hardened rugged appliance: the FortiDeceptor Rugged 100G, designed specifically for harsh industrial environments.
FortiDeceptor Benefits at a Glance

Accurate, Early Detection and Fast Response
• Reduces dwell time and false-positives
• Detects early reconnaissance and lateral movements
• Built-in, automated attack quarantine capabilities stop attacks before they spread
• Automatically scales as risk level rises
• Helps mitigate ransomware by leading malware to encrypt fake files, triggering automatic blocking of the infected endpoint
• Automatically deploys vulnerable decoys based on FortiGuard Labs latest outbreak alerts
• Integrates with the Fortinet Security Fabric and third-party security controls

Enrich Actionable Insights, Increase SOC Effectiveness
• Generates high-fidelity, actionable alerts based on real-time interactions with adversaries
• Correlates malicious activities using eight different forensic engines to help analysts investigate, gather forensic evidence, monitor, and automatically stop attacks in progress
• Closes visibility gaps with in-progress attack intel and detailed forensics
• Provides attack replays and attack visualizations
• Low-friction deployment and maintenance via automation

Extend Support to Challenging Areas
• Optimized OT, IoT, and IoMT decoys designed to expose and block threats to industrial systems, IoT, and IoMT devices
• Agentless and non-intrusive, with zero impact on mission-critical operations
• Ease of installation (one-day operation) and use; does not require any network topology changes
• Detects threats to assets that cannot provide their own telemetry
• Available across every attack surface, including on-premise, cloud, and IT, OT, IoT, and IoMT environments
• Operates in both online and air-gapped modes
Specifications

**FORTIDECEPTOR RUGGED 100G**

**Size RAM**
- DDR4-2400 48 GB ECC RDIMM (16GBx1 + 32GBx1)

**On Board Flash**
- 16 GB (M.2 2242)

**Decoy VM Support**
- Combination of Windows 7, Windows 10, Windows 10 (customizable BYOL), Linux (Ubuntu, CentOS, Redhat), macOS, SSL-VPN Server, Medical (FACS, Infusion pump), POS, ERP, IoT (Router, Switch, Printer and IP Camera), OT (PLC, HMI, MNO), SAP, SCADA, Outbreak, VOIP (4G/5G), TOMCAT, Webmin, Citrix, ESXI, Elastic-Search, SWIFT.

**Decoy Services**
- SSL VPN, SSH, SMB, RDP, HTTP/S, SQL, GIT, DICOM, Teinet, FTP, TFTP, SNMP, MODBUS, S7COMM, BACNET, IPMI, TRICONEX, SRTP, MOXA, KANTRIP, GUARDIAN-AST, IEC104, EtherNet/IP, DNP3, JET-DIRECT, RTSP, UPnP, CDP, TCP port listener, SMTP, RADIUS, MySQL, MQTT, SIP, XMPP, 3GPP, CANbus, B.BRAUN and VNC.

**Deception VMs Shipped**
- Deceptor Bundle Contract included license for Deception Decoys, Deception Lure plus FortiGuard Services Subscriptions (AREA, AV, IPS, and Web Filtering). 1 VLAN unit price. Minimum order of 2 VLANs.

**Hardware Specifications**

**Form Factor**
- Desktop - fanless

**Total Interfaces**
- 6x 1GbE RJ-45 ports

**Storage Capacity**
- 2.5 inch SATA SSD 1TB (1TBx1)

**Usable Storage (After RAID)**
- 2GB USB DOM, SATA-DOM or M.2 (SATA)

**Removable Hard Drives**
- No

**RAID 1**
- No

**Default RAID Level**
- 1

**Power Supply**
- Powered by External DC Power Adapter, 100-240V, 1.8A, 50-60Hz

**Dimensions**
- Height x Width x Length (inches) 3.85 x 10.82 x 8.86

**Weight**
- 16.63 lbs (5.73 kg)

**Operating Temperature**
- 32°F to 104°F (0°C to 40°C)

**Storage Temperature**
- -40°F to 158°F (-40°C to 70°C)

**Humidity**
- 5% to 95% (non-condensing)

**Operating Altitude**
- Up to 13 123 ft (4000 m)

**IP Rating**
- IP40

**Compliance**
- Safety Certifications – FCC, IEC, CE, RCM, VCCI class A
- CB: Low Voltage Directive (LVD) 2014/35/EU
- IEC 62368-1 2nd Edition
- IEC 62368-1 3rd Edition
- UL/CSA: UL 62368-1 3rd Edition

---

* Operating at maximum temperature derates 1.5°C per 1000 ft (305 m)
Specifications

<table>
<thead>
<tr>
<th>FORTIDECEPTOR VM</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Capacity</strong></td>
</tr>
<tr>
<td>Decoy VM Support</td>
</tr>
<tr>
<td>Decoy Services</td>
</tr>
<tr>
<td>Deception VMs Shipped</td>
</tr>
<tr>
<td>Virtual Machine</td>
</tr>
<tr>
<td>Hypervisor Support</td>
</tr>
<tr>
<td>Virtual CPUs (Min / Max)</td>
</tr>
<tr>
<td>Virtual Network Interfaces</td>
</tr>
<tr>
<td>Virtual Memory (Min / Max)</td>
</tr>
<tr>
<td>Virtual Storage (Min / Max)</td>
</tr>
</tbody>
</table>

* Fortinet recommends that the number of virtual CPUs is two plus the number of Deception VMs when each Deception VM requires 2vCPU.
** Fortinet recommends that the size of virtual memory is 4GB plus 2GB for every Deception VM clone.
*** Fortinet recommends that the size of virtual storage is 1TB for production environment.
### Ordering Information

#### FORTIDECEPTOR VM

<table>
<thead>
<tr>
<th>Product</th>
<th>SKU</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FortiDeceptor-VM Subscription License</td>
<td>FC1-10-DCVMYS-496-02-DD</td>
<td>VM model 24x7 FortiCare, Deceptor Bundle Contract included license for Deception Decoys, Deception Lures plus FortiGuard Services Subscriptions (AREA, AV, IPS, and Web Filtering). 1 network VLAN unit price, minimum order of 2 VLANs. Support up to 20 Deception VMs and up to 128 network VLANs</td>
</tr>
</tbody>
</table>

#### FORTIDECEPTOR HARDWARE

<table>
<thead>
<tr>
<th>Product</th>
<th>SKU</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FortiDeceptor-1000G</td>
<td>FDC-1000G</td>
<td>FortiDeceptor 1000G Appliance. Support up to 20 Deception VMs and 128 VLANS</td>
</tr>
<tr>
<td></td>
<td>FC1-10-DC1KG-495-02-DD</td>
<td>Deceptor Bundle Contract included license for Deception Decoys, Deception Lure plus FortiGuard Services Subscriptions (AREA, AV, IPS, and Web Filtering). 1 VLAN unit price, minimum order of 2 VLANs</td>
</tr>
<tr>
<td></td>
<td>FC-10-DC1KG-247-02-DD</td>
<td>24x7 FortiCare Contract</td>
</tr>
<tr>
<td></td>
<td>FC-10-DC1KG-210-02-DD</td>
<td>Next Day Delivery Premium RMA Service (requires 24x7 support)</td>
</tr>
<tr>
<td></td>
<td>FC-10-DC1KG-211-02-DD</td>
<td>4-Hour Hardware Delivery Premium RMA Service (requires 24x7 support)</td>
</tr>
<tr>
<td></td>
<td>FC-10-DC1KG-212-02-DD</td>
<td>4-Hour Hardware and Onsite Engineer Premium RMA Service (requires 24x7 support)</td>
</tr>
<tr>
<td></td>
<td>FC-10-DC1KG-301-02-DD</td>
<td>Secure RMA Service</td>
</tr>
<tr>
<td>FortiDeceptor Rugged 100G</td>
<td>FDR-100G</td>
<td>FortiDeceptor-100G Rugged Appliance, Support up to 8 Deception VMs and 48 VLANS</td>
</tr>
<tr>
<td></td>
<td>FC1-10-DR1HG-495-02-DD</td>
<td>Deceptor Bundle Contract included license for Deception Decoys, Deception Lure plus FortiGuard Services Subscriptions (AREA, AV, IPS, and Web Filtering). One VLAN unit price, minimum order of two VLANs</td>
</tr>
<tr>
<td></td>
<td>FC-10-DR1HG-247-02-DD</td>
<td>FortiCare Premium Support</td>
</tr>
<tr>
<td></td>
<td>FC-10-DR1HG-210-02-DD</td>
<td>Next Day Delivery Premium RMA Service (Requires FortiCare Premium or FortiCare Elite)</td>
</tr>
<tr>
<td></td>
<td>FC-10-DR1HG-211-02-DD</td>
<td>4-Hour Hardware Delivery Premium RMA Service (Requires FortiCare Premium or FortiCare Elite)</td>
</tr>
<tr>
<td></td>
<td>FC-10-DR1HG-212-02-DD</td>
<td>4-Hour Hardware and Onsite Engineer Premium RMA Service (Requires FortiCare Premium or FortiCare Elite)</td>
</tr>
<tr>
<td></td>
<td>FC-10-DR1HG-301-02-DD</td>
<td>Secure RMA Service</td>
</tr>
</tbody>
</table>

#### FORTIDECEPTOR LICENSES ADD-ONS

<table>
<thead>
<tr>
<th>Product</th>
<th>SKU</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FortiDeceptor Central Management License</td>
<td>FC1-10-FDCCM-497-02-DD</td>
<td>Central Management seat license per FortiDeceptor device. One manageable appliance unit price, minimum order of two manageable appliances.</td>
</tr>
<tr>
<td>FortiDeceptor Windows License*</td>
<td>LIC-FDC-WIN</td>
<td>Expands FortiDeceptor Licensed Windows VM capacity by 2. (1) Win7 and (1) Win10 license added</td>
</tr>
</tbody>
</table>

* This Windows License applies to FDC-VMS, FDC-1000G, and FDR-100G.

Note: The network VLAN license cost is per class C network (/24), one VLAN per network. For subnet networks greater than class C (/23,/22), the cost is two VLANs per network.

---

### Fortinet Corporate Social Responsibility Policy

Fortinet is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you will not use Fortinet’s products and services to engage in, or support in any way, violations or abuses of human rights, including those involving illegal censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the Fortinet EULA and report any suspected violations of the EULA via the procedures outlined in the Fortinet Whistleblower Policy.
copyright © 2023 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 general counsel, 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.

www.fortinet.com