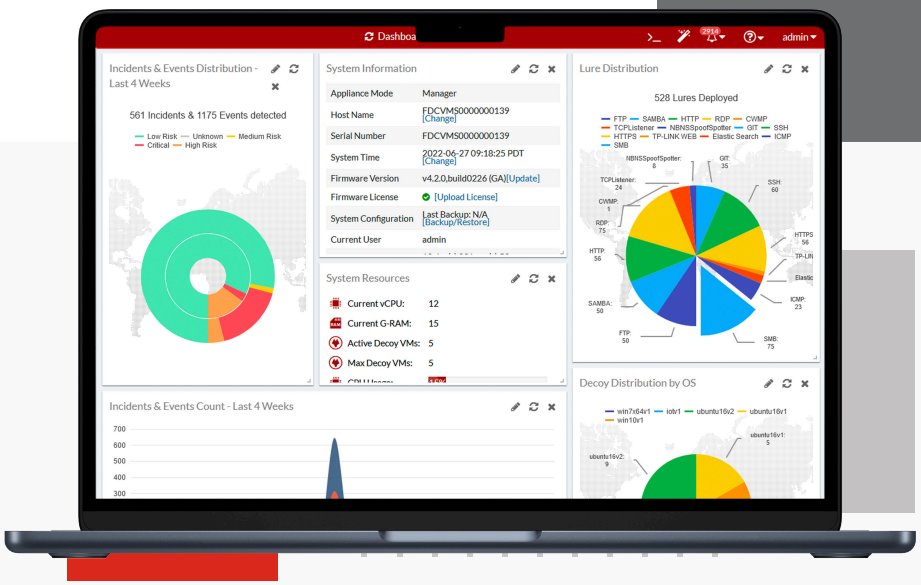
FortiDeceptor



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

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.

Available in

Appliance

Virtual

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

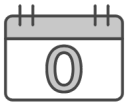
The solution generates high-fidelity, zero false-positive alerts, providing security teams with a unique advantage over malicious activity, and unparalleled visibility to detect and stop attacks, credential thefts, lateral movement, and malware activity. It also provides compensating security control 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-as-a-Service

FortiDeceptor-as-a-Service is a SaaS-based deception solution hosted in the Fortinet private cloud that detects and responds to in-network attacks, such as stolen credential usage, lateral movement, man in the middle (MITM), and ransomware. Deploying FortiDeceptor-as-a-Service transforms your entire network into a mirror maze with numerous authentic-seeming fake assets in minutes. When an attack is detected, high-fidelity zero-false-positive alerts are generated immediately. This activity enables your security team to detect human and automated attacks earlier in the kill chain and move them to the FortiDeceptor-as-a-Service cloud to avoid damage.

Simple deployment of deception assets

FortiDeceptor-as-a-Service provides many IT, OT, and IoT decoys. Decoys can also generate limited fake network traffic to ensure they appear in passive network scans the attacker runs. In addition, it generates deception tokens (fake cached credentials, data and configuration files, network share) placed on real assets. Deception tokens are agentless technology that serves as attractive targets for attackers, designed to deceive them to laterally move to the decoys. Any interaction with deception assets redirects attackers away from the network to the decoy hosted in the cloud.

Decoys run in the Fortinet private cloud, using your available, unused IP addresses. The IP addresses do not correspond to any real host or device on your network nor impact network availability. FortiDeceptor-as-a-Service also includes a lightweight appliance, the FortiDeceptor 100G Edge, available as hardware or a virtual appliance. Deployed in your network, the FortiDeceptor 100G Edge uses a secure Layer 2 tunnel to connect the relevant decoys hosted in the Fortinet private cloud to the respective VLANs. The FortiDeceptor private Layer 2 tunnel is embedded with its own authentication and encryption methods and heartbeat checks on top of SSL and TLS encryption.

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	FORTIDECEPTOR 100G (EDGE)	FORTIDECEPTOR 1000G
Capacity and Performance			
Size RAM	DDR4-2400 48 GB ECC RDIMM (16GBx1 + 32GBx1)	4G	DDR4-2400 48 GB ECC RDIMM (16 GB*3)
On Board Flash	16GB (M.2 2242)	8G	2 GB USB
Decoy VM Support	Windows 7 / 10 / 11, Win 10 / 11 (customizable, BYOL), Win Server 2016/2019/2022 (customizable, BYOL), Ubuntu 16.04 / 18.04, Redhat (customizable, BYOL), CentOS 7.9, SSL-VPN, ESXI Decoy, FortiGate, IoT (Routers, Switch, Printers and IP-Camera), Medical devices, (PACS, Infusion pump), SWIFT, SCADA, ERP, POS, SAP, Elastic Search, Tomcat, MySql MariaDB, SIP, XMPP, MQTT, 4G/5G 3GPP, MacOS, Webmin, Citrix, Nginx, EV-CPO		
Decoy Services	ARP, BACNET, B.BRAUN (port 8080), CAN Bus Protocol, CDP, CoAP, CWMP, DICOM Server, DNP3, Elastic Search, ENIP, ERP-WEB, FTP, GIT, GTP-U, Guardian-AST, HoneyDoc, HTTP, HTTP (APACHE), HTTPS, ICMP, IEC104, IIS (HTTP), IIS (HTTPS), Infusion Pump (FTP), Infusion Pump (Telnet), IP Camera-WEB, IPMI, Jetdirect, KAMSTRUP, Lantronix Discovery Protocol, LOGON, MariaDB, MODBUS, MOXA, MQTT WEB, MSSQL, MYSQL, NBNSSpoofSpotter, NextEPC WEB, PACS, PACS-WEB, POS-WEB, Printer-WEB, PROFINET, RADIUS, RARP, RDP, RTSP, S7COMM, SAMBA, SAP DISPATCHER, SAP ROUTER, SAP WEB, SAP WEB HTTPS, ScadaBR, SCTP and GTP-C, SIP, SMB, SMTP, SNMP, SRTP, SSH, SSLVPN, SWIFT Lite2, TCPListener, Telnet, TFTP, TOMCAT (HTTP), TOMCAT (HTTPS), TP-LINK WEB, TRICONEX, UPnP, vnc, XMPP, XMPP WEB		
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	FortiDeceptor 100G Appliance, support both Local FDC manager and DAAS* platform and up to 128 VLANS. *DAAS (Deception-as-a-Service)	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	Desktop	1 RU Rackmount
Total Interfaces	6× 1GbE RJ-45 ports	10	4 x GE (RJ45), 4 x GE (SFP)
Storage Capacity	2.5 inch SATA SSD 1TB (1TBx1)		2 TB (2 × 1 TB HDD)
Usable Storage (After RAID)	2GB USB DOM, SATA-DOM or M.2 (SATA)		1 TB
Removable Hard Drives	No		No
RAID 1	No		RAID 1
Default RAID Level	No		1
Power Supply	Powered by External DC Power Adapter, 100-240V, 1.8A, 50-60Hz	12VDC, 3A	650W Redundant PSU (1+0) Additional/optional PSU (SKU: SP-FSA1000G-PS)
Dimensions			
Height x Width x Length (inches)	3.85 × 10.83 × 8.86	1.5 × 8.5 × 6.3	1.73 × 17.24 × 23.62
Height x Width x Length (mm)	98 × 275 × 225	38.5 × 216 × 160	44 × 438 × 600
Weight	12.63 lbs (5.73 kg)	2.1 lbs (0.95 kg)	27.56 lbs (12.5 kg)
Environments			
AC Power Supply	N/A	External DC Power Adapter, 100–240V AC, 50/60 Hz	100-240 VAC, 60-50 Hz, 650W Redundant PSU (1+0)
DC Power Supply	Input: 24-48Vdc 3.45-1.77A		
Power Consumption (Max)	+24V (66.11W), +48V (73.92W)	18.7 W	253.2 W
Power Consumption (Average)	+24V (54.1W), +48V (60.5W)	17.2 W	202.56 W
Maximum Current	+24V (3.45A), +48V (1.77A)	100VAC/1.0A, 240VAC/0.6A	
Heat Dissipation	+24V (259.69 BTU/h), +48V (286.34 BTU/h)	63.8 BTU/hr	863.92 (BTU/h)
Operating Temperature	32°F to 104°F (0°C to 40°C)	32°F to 104°F (0°C to 40°C)	32°F to 104°F (0°C to 40°C)
Storage Temperature	-40°F to 158°F (-40°C to 70°C)	31°F to 158°F (-35°C to 70°C)	-13°F to 158°F (-25°C to 70°C)
Humidity	5% to 95% (non-condensing)	10%–90% non-condensing	10% to 90% (non-condensing)
Operating Altitude	Up to 13 123 ft (4000 m)	Up to 7400 ft (2250 m)	Up to 7400 ft (2250 m) *
IP Rating	IP40		—
Compliance			
Safety Certifications	Onboard flash is 8GB FCC, ICES, 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	FCC, ICES, CE, RCM, VCCI, BSMI, UL/cUL, CB, USGv6/IPv6	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB

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

FortiDeceptor Rugged 100G

FortiDeceptor 100G

FortiDeceptor 1000G

Specifications

FORTIDECEPTOR VM	
Capacity	
Decoy VM Support	Combination of Windows 7, Windows 10, Windows 10 (customizable BYOL), Windows Server 2016, 2019 and 2022 (customizable BYOL), Linux (Ubuntu, CentOS, Redhat), macOS, SSL-VPN Server, Medical (PACS, Infusion pump), POS, ERP, IoT (Router, Switch, Printer and IP-Camera), OT (PLC, HMI, MNG), SAP, SCADA, Outbreak,VOIP (4G/5G), TOMCAT, Webmin, Citrix, ESXi, Elastic-Search, SWIFT.
Decoy Services	SSL VPN, SSH, SAMBA, SMB, RDP, HTTP/S, SQL, GIT, DICOM, Telnet, FTP, TFTP, SNMP, MODBUS, S7COMM, BACNET, IPMI, TRICONEX, SRTP, MOXA, KAMSTRUP, 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	VM model 24×7 FortiCare, Deceptor Bundle Contract included license for Deception Decoys, Deception Lures plus FortiGuard Services Subscriptions (AREA, AV, IPS, and Web Filtering). One network VLAN unit price, minimum order of two VLANs. Support up to 20 Deception VMs and up to 128 network VLANS.
Virtual Machine	
Hypervisor Support	VMWare vSphere ESXi 5.1, 5.5, 6.0 or 7.0 and later, KVM, Hyper-V, AWS. AZURE, GCP
Virtual CPUs (Min / Max)	12 / Unlimited* Intel Virtualization Technology (VT-x/EPT) or AMD Virtualization (AMD-V/RVI)
Virtual Network Interfaces	6
Virtual Memory (Min / Max)	16 GB / Unlimited**
Virtual Storage (Min / Max)	200 GB / 16 TB***

* 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 2 GB for every Deception VM clone.

*** Fortinet recommends that the size of virtual storage is 1TB for production environment.

Ordering Information

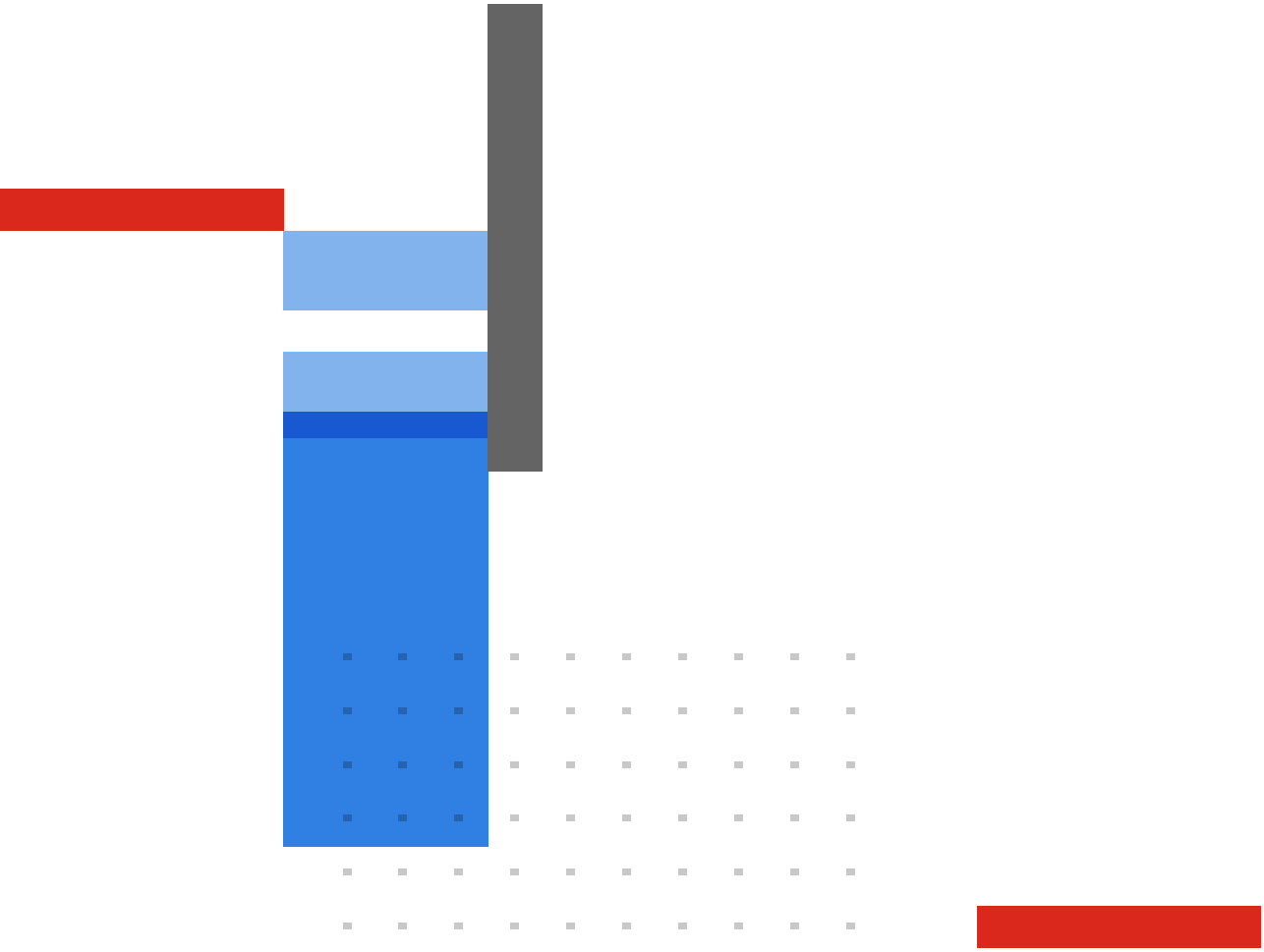
FORTIDECEPTOR VM		
Product	**SKU**	**Description**
FortiDeceptor-VM Subscription License	FC1-10-DCVMS-496-02-DD	VM model 24×7 FortiCare, Deceptor Bundle Contract included license for Deception Decoys, Deception Lures plus FortiGuard Services Subscriptions (AREA, AV, IPS, and Web Filtering). One network VLAN unit price, minimum order of two VLANs. Supports up to 20 Deception VMs and up to 128 network VLANS.
FORTIDECEPTOR HARDWARE		
Product	**SKU**	**Description**
FortiDeceptor-1000G	FDC-1000G	FortiDeceptor 1000G Appliance. Supports up to 20 Deception VMs and 128 VLANS.
	FC1-10-DC1KG-495-02-DD	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.
	FC-10-DC1KG-247-02-DD	24×7 FortiCare Contract.
	FC-10-DC1KG-210-02-DD	Next Day Delivery Premium RMA Service (requires 24×7 support).
	FC-10-DC1KG-211-02-DD	Four-Hour Hardware Delivery Premium RMA Service (requires 24×7 support).
	FC-10-DC1KG-212-02-DD	Four-Hour Hardware and Onsite Engineer Premium RMA Service (requires 24×7 support).
	FC-10-DC1KG-301-02-DD	Secure RMA Service.
FortiDeceptor-100G	FDC-100G	FortiDeceptor 100G Appliance, supports both Local FDC manager and DAAS platform and up to 128 VLANS.
	FC-10-DC1HG-247-02-DD	FortiCare Premium Support.
FortiDeceptor Rugged 100G	FDR-100G	FortiDeceptor-100G Rugged Appliance, Supports up to eight Deception VMs and 48 VLANS.
	FC1-10-DR1HG-495-02-DD	Deceptor Bundle Contract included license for Deception Decoys, Deception Lure plus FortiGuard Services Subscriptions (ARAE, AV, IPS, and Web Filtering). One VLAN unit price, minimum order of two VLANs.
	FC-10-DR1HG-247-02-DD	FortiCare Premium Support.
	FC-10-DR1HG-210-02-DD	Next Day Delivery Premium RMA Service (Requires FortiCare Premium or FortiCare Elite).
	FC-10-DR1HG-211-02-DD	Four-Hour Hardware Delivery Premium RMA Service (Requires FortiCare Premium or FortiCare Elite).
	FC-10-DR1HG-212-02-DD	Four-Hour Hardware and Onsite Engineer Premium RMA Service (Requires FortiCare Premium or FortiCare Elite).
	FC-10-DR1HG-301-02-DD	Secure RMA Service.
FORTIDECEPTOR DECEPTION AS A SERVICE (DAAS)		
Product	**SKU**	**Description**
FortiDeceptor-DAAS Premium Bundle	FC1-10-DCDAS-496-02-DD	DAAS FortiCare Premium Deceptor Bundle Contract included license for Deception Decoys, Deception Lures plus FortiGuard Services Subscriptions (ARAE, AV, IPS, and Web Filtering). One network VLAN unit price, minimum order of two VLANs.
FORTIDECEPTOR LICENSES ADD-ONS		
Product	**SKU**	**Description**
FortiDeceptor Central Management License	FC1-10-FDCCM-497-02-DD	Central Management seat license per FortiDeceptor device. One manageable appliance unit price, minimum order of two manageable appliances.
FortiDeceptor Windows License*	LIC-FDC-WIN	Expands FortiDeceptor Licensed Windows VM capacity by two. One Win7 and one Win10 license added.

* 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.



www.fortinet.com

Copyright © 2024 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 SVP Legal and above, 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.

June 21, 2024

FDC-DAT-R21-20240621