DATA SHEET

FortiDeceptor

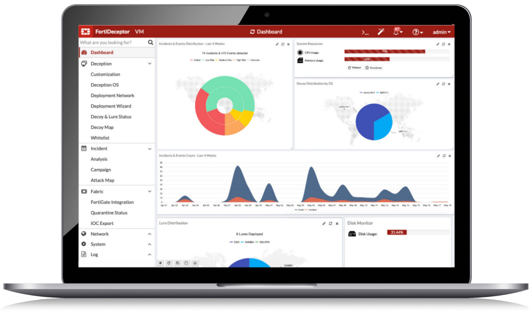
Available in:

Appliance

Virtual Machine

Deceive | Expose | Eliminate

FortiDeceptor is designed to **deceive, expose,** and **eliminate** external and internal threats early in the attack kill chain and proactively block these threats before any significant damage occurs.



Fortinet Security Fabric provides unified, end-to-end protection with Fortinet Next Generation Firewalls to tackle advanced persistent threats. Adding FortiDeceptor as part of a Breach Protection strategy helps evolve your defenses from reactive to proactive with intrusion-based detection layered with contextual intelligence. It automates the blocking of attackers targeting IT devices and OT system controls. FortiDeceptor automatically lays out a layer of decoys and lures, helping you conceal your sensitive and critical assets behind a fabricated Deception Surface to confuse and redirect attackers while revealing their presence on your network.

Advanced Threat Deception

DECEIVE external and internal threats with deceptive VM instances aka decoys managed from a centralized location. Deploy a Deception Surface of real Windows, Linux, VPN, Medical, IoT/OT, SCADA, and SAP VMs with services that are indistinguishable from real assets, e.g. production servers and lures embedded into devices designed to uncover the attackers.

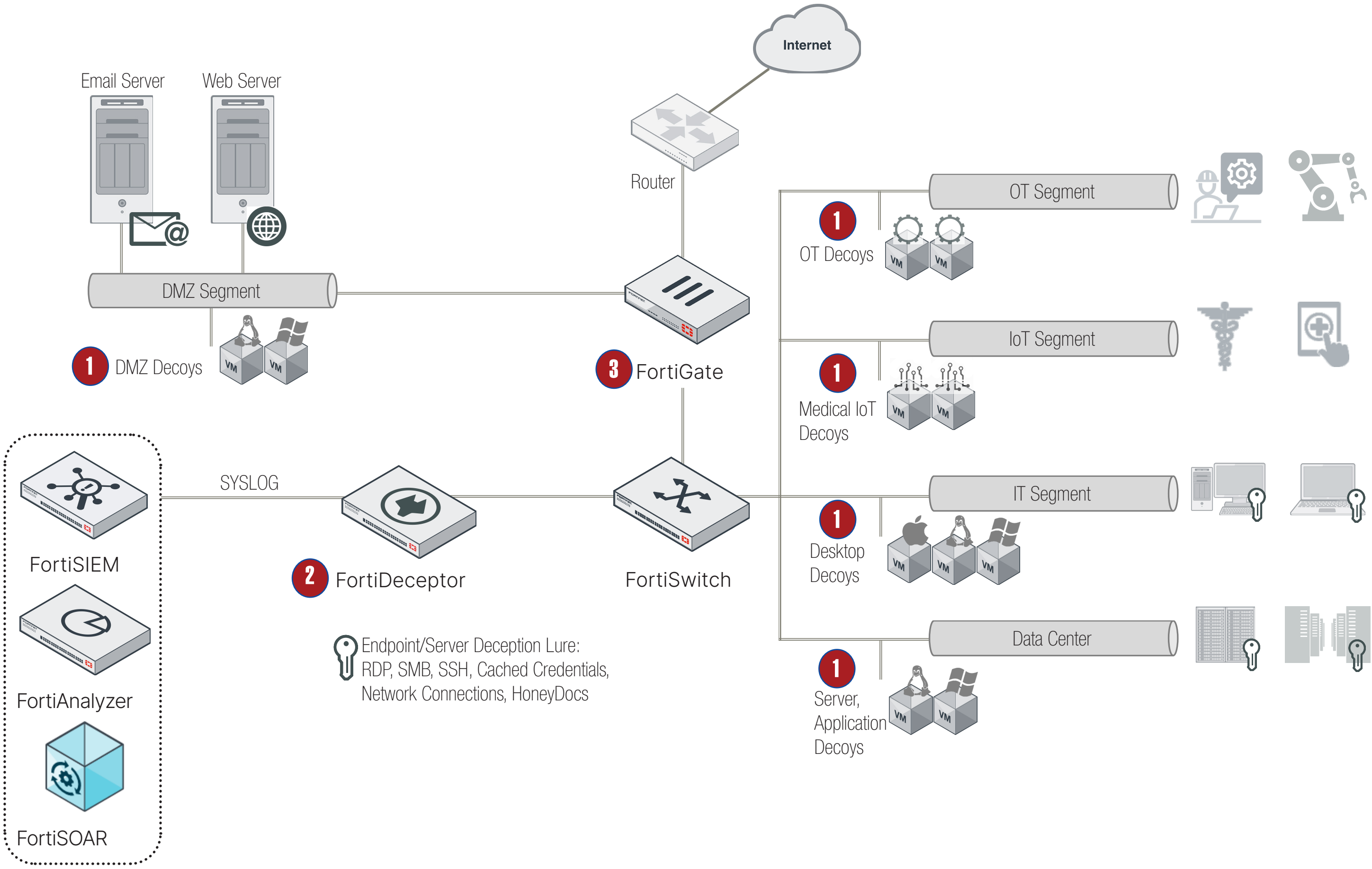
EXPOSE hacker activity with early and accurate detection and actionable alerts enabled through tracing and correlation of an attacker's Tactics, Tools, and Procedures (TTPs) and active notification via Web UI, Email, SNMP traps, logs, and events via FortiSIEM and FortiAnalyzer.

ELIMINATE threats by automating threat response with FortiGates, FortiNAC, FortiEDR, FortiSOAR, and third party security solutions via Fortinet Security Fabric.

Feature Benefits

- **Simple and Easy to Use** with a wizard-based setup of IT/ OT/ IoT decoys and lures fine-tuned to your environment and centrally manage a distributed deception deployment across your IT and OT environments
- **Rapid investigation** with intelligent incident correlation into a campaign timeline of all activities including access, tools used, lateral movement, and more, layered with contextual threat intelligence from FortiGuard Labs
- **Eliminate Early Stage Attacks** with Security Fabric integration including FortiGate, FortiNAC, FortiEDR, FortiSOAR, and third-party. Elevate threat visibility and hunting with FortiSIEM and FortiAnalyzer

DECEPTION WORKFLOW



1. FortiDeceptor deploys decoys with different OS types equipped with lures (e.g. RDP/ SMB/ Credentials/ HoneyDocs) that appear indistinguishable from real IT and OT assets and are highly interactive.

2. FortiDeceptor acts as an early warning system that exposes attacker's malicious intent and tracks lateral movement, which translates to real-time alerts sent to FortiDeceptor, as well as FortiAnalyzer and FortiSIEM for review and validation. FortiDeceptor applies analytics powered by FortiGuard Labs, FortiSandbox, and VirusTotal intelligence, to a consolidated set of security events and correlates them to the campaigns with timeline of activities.

3. FortiDeceptor allows security analyst to manually investigate and apply manual remediation or automatically block these attacks based on severity before actual damage occurs via integration with FortiGate, FortiNAC, FortiEDR and FortiSIEM/ FortiSOAR.

Feature Integration

FortiGate: FortiDeceptor shown prominently in FortiGate's network topology map as a widget detailing system info, status, and deception servers list.

SPECIFICATIONS

FORTIDECEPTOR 1000G	
Capacity and Performance	
Size RAM	DDR4-2400 48 GB ECC RDIMM (16 GB*3)
On Board Flash	2 GB USB
Decoy VM Support	Combination of Windows 7, Windows 10, Windows 10 (customizable BYOL), Windows Server 2016 and 2019 (customizable BYOL), Linux, VPN Server, Medical (PACS, Infusion pump), POS, ERP, IoT (Router, Printer and Camera), SAP and/or SCADA, up to 20 Deception VMs and 128 VLANs
Decoy Services	SSL VPN, SSH, SAMBA, SMB, RDP, HTTP/S, SQL, GIT, DICOM, Telnet, FTP, TFTP, SNMP, MODBUS, S7COMM, BACNET, IPMI, TRICONEX, GUARDIAN-AST, IEC104, EtherNet/IP, DNP3, JET-DIRECT, RTSP, UPnP, CDP and TCP port listener
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	1 RU Rackmount
Total Interfaces	4 x GE (RJ45), 4 x GE (SFP)
Storage Capacity	2 TB (2 × 1 TB HDD)
Usable Storage (After RAID)	1 TB
Removable Hard Drives	No
RAID 1	RAID 1
Default RAID Level	1
Optional (SKU: SP-FSA1000G-PS)	
Power Supply	650W Redundant PSU (1+0)
	Additional PSU (SKU: SP-FSA1000G-PS)
Dimensions	
Height x Width x Length (inches)	1.73 × 17.24 × 23.62
Height x Width x Length (cm)	44 × 438 × 600
Weight	27.56 lbs (12.5 kg)
Environments	
AC Power Supply	100-240 VAC, 60-50 Hz, 650W Redundant PSU (1+0)
Power Consumption (Max / Average)	253.2 W / 202.56 W
Heat Dissipation	863.92 (BTU/h)
Operating Temperature	32°F to 104°F (0°C to 40°C)
Storage Temperature	-13°F to 158°F (-25°C to 70°C)
Humidity	10% to 90% (non-condensing)
Operating Altitude	Up to 7400 ft (2250 m) *
Compliance	
Safety Certifications	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB

* Operating at maximum temperature derates 1.5°C per 1,000 ft (305 m)

FORTIDECEPTOR VM	
Capacity	
Decoy VM Support	Combination of Windows 7, Windows 10, Windows 10 (customizable BYOL), Windows Server 2016 and 2019 (customizable BYOL), Linux, VPN Server, Medical (PACS, Infusion pump), POS, ERP, IoT (Router, Printer and Camera), SAP and/or SCADA, up to 20 Decoys
Decoy Services	SSL VPN, SSH, SAMBA, SMB, RDP, HTTP/S, SQL, GIT, DICOM, Telnet, FTP, TFTP, SNMP, MODBUS, S7COMM, BACNET, IPMI, TRICONEX, GUARDIAN-AST, IEC104, EtherNet/IP, DNP3, JET-DIRECT, RTSP, UPnP, CDP and TCP port listener
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). 1 network VLAN unit price, minimum order of 2 VLANs. Support up to 20 Deception VMs and up to 128 network VLANS
Virtual Machine	
Hypervisor Support	VMWare vSphere ESXi 5.1, 5.5 or 6.0 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.

ORDER 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). 1 network VLAN unit price, minimum order of 2 VLANs. Support up to 20 Deception VMs and up to 128 network VLANS.

FORTIDECEPTOR HARDWARE

Product	SKU	Description
FortiDeceptor-1000G	FDC-1000G	FortiDeceptor 1000G Appliance. Support 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).1 VLAN unit price, minimum order of 2 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	4-Hour Hardware Delivery Premium RMA Service (requires 24×7 support).
	FC-10-DC1KG-212-02-DD	4-Hour Hardware and Onsite Engineer Premium RMA Service (requires 24×7 support).
	FC-10-DC1KG-301-02-DD	Secure RMA Service.

FORTIDECEPTOR LICENSES ADD-ONS

Product	SKU	Description
FortiDeceptor Central Management License	FC-10-FDCCM-497-02-DD	Central Management license for up to 50 FortiDeceptor devices.
FortiDeceptor Windows License*	LIC-FDC-WIN	Expands FortiDeceptor Licensed Windows VM capacity by 2. (1) Win7 and (1) Win10 license added.

* This Windows License applies to FDC-VMS and FDC-1000G only.

www.fortinet.com

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 censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the Fortinet EULA (https://www.fortinet.com/content/dam/fortinet/assets/legal/EULA.pdf) and report any suspected violations of the EULA via the procedures outlined in the Fortinet Whistleblower Policy (https://secure.ethicspoint.com/domain/media/en/gui/19775/Whistleblower_Policy.pdf).