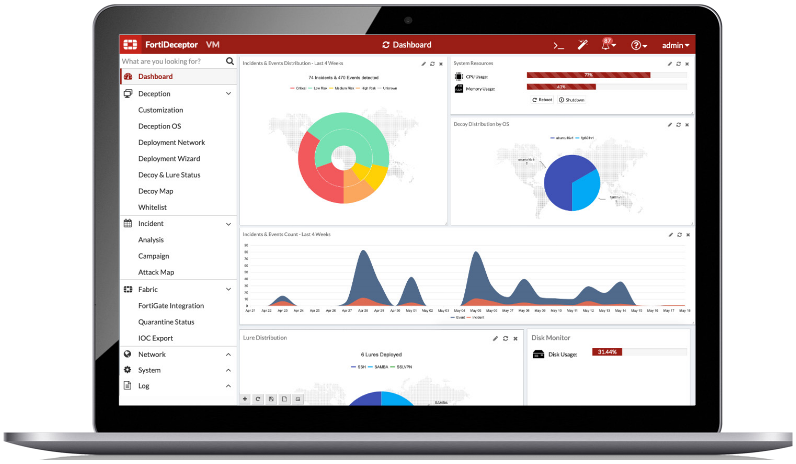
FORTINET

DATA SHEET

FortiDeceptor

DECEIVE | EXPOSE | ELIMINATE



FortiDeceptor is designed to **DECEIVE**, **EXPOSE**, and **ELIMINATE** advanced attacks by breaking the kill chain at the earliest opportunity and discovering intruders that may have slipped past traditional security controls. It automates the creation of decoys to provide an internal layer of protection to lure, expose, and stop attackers before any damage is done.

Fortinet Security Fabric provides unified, end-to-end protection with Fortinet Enterprise Firewalls to tackle advanced persistent threats. Adding FortiDeceptor as part of a Breach Protection strategy expands your defenses from reactive to proactive with intrusion-based detection and robust security alerts that are both actionable and automated. FortiDeceptor 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 and decoys, managed from a centralized location. Deploy a Deception Surface of real Windows, Linux, VPN, and SCADA VMs that are indistinguishable from real assets, e.g. production servers, to lure attackers into revealing themselves.

EXPOSE hacker activity with early and accurate detection and actionable alerts. Trace and correlate hackers' lateral movement and notify Security Administrators through Web UI, Email, SNMP traps, logs, and events via FortiSIEM and FortiAnalyzer. Analyze detailed forensic information of hackers' lateral movements and activities. Correlate incident and campaign information of attackers' traffic.

ELIMINATE threats by quarantining attackers with FortiGates in Fortinet Security Fabric. Identify intrusions and malware infection on the network.

Feature Highlights

Wizard-based deployment of Decoy VMs and Tokens in both IT and OT networks to lure hackers to engage with decoy VMs.

Monitor and Correlate Incidents and Campaigns with information about logins/logouts to hosts, tracking lateral movements, file added/modified/deleted/executed on decoy VMs.

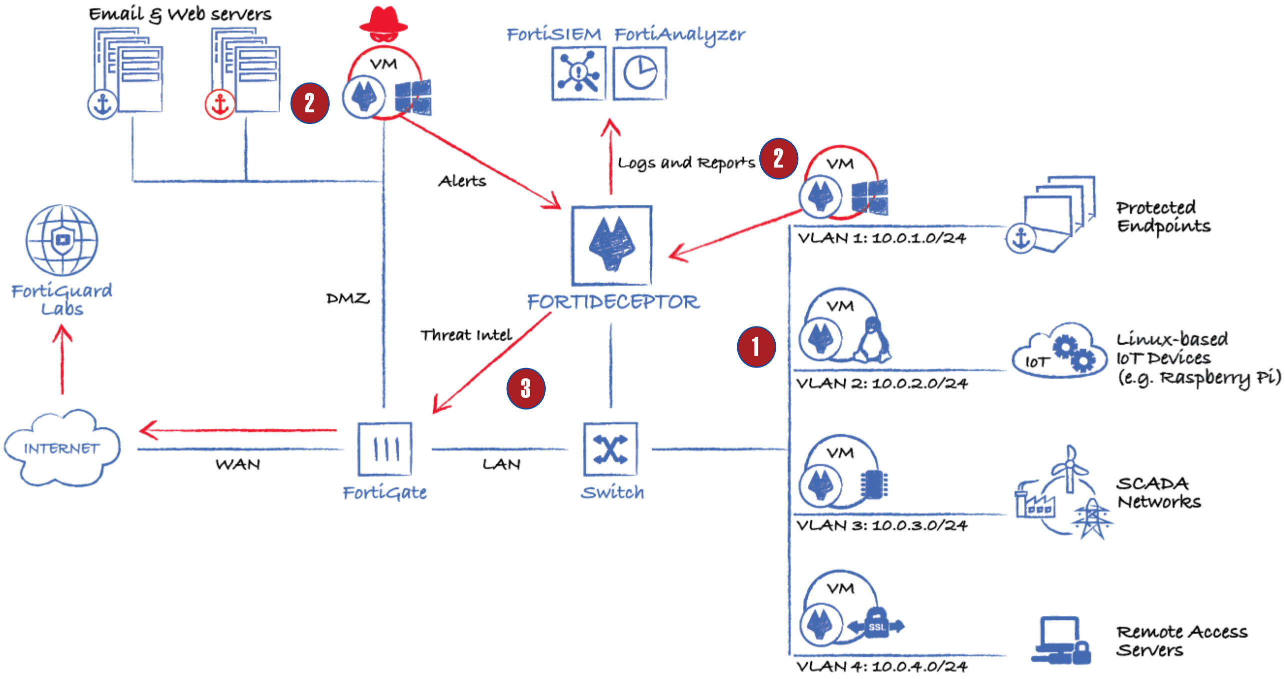
Eliminate External and Internal Attacks to/from decoys by identifying intrusions, malware, and website visits.

Security Fabric Integration with FortiGate by automated quarantine source of the attack, and with FortiSIEM and FortiAnalyzer for comprehensive incident visibility and management.

Comprehensive Reports from incident tables of incidents and campaigns in PDF format.

Configure Alerts and send Alert Notifications via email, SNMP TRAPs, Common Event Format, and SYSLOG.

Deception Workflow



1 FortiDeceptor deploys decoys with different OS types equipped with lures (e.g. SMB/SQL/SSH service) 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 to a consolidated set of security events and correlates them to the campaigns with timeline of activities.

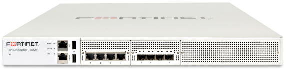
3 FortiDeceptor allows security analyst to manually investigate and apply manual remediation or automatically block these attacks based on severity before actual damage occurs via integration with FortiGate to quarantine IP address of the threat actor.

Specifications

FORTIDECEPTOR VM	
Capacity	
Deception VM OS	Windows, Ubuntu, and SCADA
Decoy Support	Combination of Windows 7, Windows 10, Windows 10 (customizable BYOL), Windows Server 2016 and 2019 (customizable BYOL), and/or SCADA, up to 16 Decoys
Decoy Services	SSL VPN, SSH, SAMBA, SMB, RDP, HTTP, FTP, TFTP, SNMP, MODBUS, S7COMM, BACNET, IPMI, TRICONEX, GUARDIAN-AST, IEC104, Microsoft SQL, TCP port listener
VLANs Support (Maximum)	32
Deception VMs Shipped	0 Upgradable to max.16
Virtual Machine	
Hypervisor Support	VMWare vSphere ESXi 5.1, 5.5 or 6.0 and later, KVM
Virtual CPUs (Min / Max)	4 / Unlimited* Intel Virtualization Technology (VT-x/EPT) or AMD Virtualization (AMD-V/RVI)
Virtual Network Interfaces	6
Virtual Memory (Min / Max)	4GB / Unlimited**
Virtual Storage (Min / Max)	200GB / 16TB***

* Fortinet recommends that the number of virtual CPUs is one plus the number of VM instance.
** Fortinet recommends that the size of virtual memory is 4GB plus 2 GB for every VM instance.
*** Fortinet recommends that the size of virtual storage is 1TB for production environment.

Specifications



	FORTIDECEPTOR 1000F
Capacity and Performance	
Size RAM	DDR4-2400 48GB ECC RDIMM (16GB*3)
On Board Flash	2 GB USB
Deception VM OS	Windows, Ubuntu, and SCADA
Decoy Support	Combination of Windows 7, Windows 10, Windows 10 (customizable BYOL), Windows Server 2016 and 2019 (customizable BYOL), and/or SCADA, up to 16 Decoys
Decoy Services	SSL VPN, SSH, SAMBA, SMB, RDP, HTTP, FTP, TFTP, SNMP, MODBUS, S7COMM, BACNET, IPMI, TRICONEX, GUARDIAN-AST, IEC104, Microsoft SQL, TCP port listener
VLANs Support (Maximum)	32
Decoys Shipped *	2 Win (1 x Win7 & 1 x Win10) and 8 Linux; Upgradable to max.16
Hardware Specifications	
Form Factor	1 RU Rackmount
Total Interfaces	4 x GE (RJ45), 4 x GE (SFP)
Storage Capacity	2TB (2 x 1TB HDD)
Usable Storage (After RAID)	1 TB
Removable Hard Drives	No
RAID Levels Supported	RAID 0/1
Default RAID Level	1
Optional (SKU: SP-FSA1000F-PS)	
Power Supply	Dual PSU Support (Shipped with single PSU)
	Additional PSU (SKU: SP-FSA1000F-PS)
Dimensions	
Height x Width x Length (inches)	1.73 x 17.24 x 22.83
Height x Width x Length (cm)	4.4 x 43.8 x 58.0
Weight	24 lbs (10.9 kg)
Environment	
AC Power Supply	100-240 VAC, 50-60 Hz
Power Consumption (Max / Average)	116.58 W / 66.93 W
Heat Dissipation	397.77 (BTU/h)
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 90% (non-condensing)
Operating Altitude	Up to 7,400 ft (2,250 m)
Compliance	
Safety Certifications	FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB

Order Information

Product	SKU	Description
FortiDeceptor-VM	FDC-VM	FortiDeceptor-VM virtual appliance with 0 Decoy upgradable to max 16 Decoys
	FC1-10-FDCVM-291-02-DD	FortiDeceptor Anti-Reconnaissance & Anti-Exploit (ARAE) Service for ARAE engine, includes FortiGuard AV, IPS, Web Filtering updates, up to 2 Decoys
	FC2-10-FDCVM-291-02-DD	FortiDeceptor Anti-Reconnaissance & Anti-Exploit (ARAE) Service for ARAE engine, includes FortiGuard AV, IPS, Web Filtering updates, up to 4 Decoys
	FC3-10-FDCVM-291-02-DD	FortiDeceptor Anti-Reconnaissance & Anti-Exploit (ARAE) Service for ARAE engine, includes FortiGuard AV, IPS, Web Filtering updates, up to 8 Decoys
	FC4-10-FDCVM-291-02-DD	FortiDeceptor Anti-Reconnaissance & Anti-Exploit (ARAE) Service for ARAE engine, includes FortiGuard AV, IPS, Web Filtering updates, up to 16 Decoys

Product	SKU	Description
FortiDeceptor-VM Support	FC1-10-FDCVM-248-02-DD	24x7 FortiCare Contract for (up to) 2 Decoys for FDC-VM
	FC2-10-FDCVM-248-02-DD	24x7 FortiCare Contract for (up to) 4 Decoys for FDC-VM
	FC3-10-FDCVM-248-02-DD	24x7 FortiCare Contract for (up to) 8 Decoys for FDC-VM
	FC4-10-FDCVM-248-02-DD	24x7 FortiCare Contract for (up to) 16 Decoys for FDC-VM

Product	SKU	Description
FortiDeceptor-1000F	FDC-1000F	FortiDeceptor 1000F Appliance with 2 Windows Decoys (include 1 x Win7 and 1 x Win10 licenses) and 8 Linux Decoys, upgradable up to max 16 Decoys
	FC-10-FDC1K-247-02-DD	24x7 FortiCare Contract for (up to) 16 Decoys for FDC-1000F
	FC-10-FDC1K-291-02-DD	FortiDeceptor Anti-Reconnaissance & Anti-Exploit (ARAE) Service for ARAE engine, includes FortiGuard AV, IPS, Web Filtering updates

Product	SKU	Description
FortiDeceptor License Add-Ons*	FDC-UPG-LNX	Expands FortiDeceptor capacity by 2 Linux Decoys. This upgrade SKU can be applied to FortiDeceptor VM or Physical Appliance
	FDC-UPG-WIN7	Expands FortiDeceptor capacity by 2 Windows 7 Decoys. Include 2 x Windows 7 licenses. This upgrade SKU can be applied to FortiDeceptor VM or Physical Appliance
	FDC-UPG-WIN10	Expands FortiDeceptor capacity by 2 Windows 10 Decoys. Include 2 x Windows 10 licenses. This upgrade SKU can be applied to FortiDeceptor VM or Physical Appliance
	FDC-UPG-SCA	Expands FortiDeceptor capacity by 2 SCADA Decoys. Include 2 x SCADA licenses. This upgrade SKU can be applied to FortiDeceptor VM or Physical Appliance
	FC-10-FDCVM-292-02-DD	Expands FortiDeceptor VM capacity by 1 x customisable Win10 client OR server 2016/2019 decoy, offered as subscription service. Does not include Windows licenses i.e. BYOL
	FC-10-FDC1K-292-02-DD	Expands FortiDeceptor 1000F capacity by 1 x customisable Win10 client OR server 2016/2019 decoy, offered as subscription service. Does not include Windows licenses i.e. BYOL.
	FC-10-FDCVM-287-02-DD	Expands FortiDeceptor VM capacity by 1 x SSL VPN decoy, offered as subscription service.
	FC-10-FDC1K-287-02-DD	Expands FortiDeceptor 1000F capacity by 1 x SSL VPN decoy, offered as subscription service.

*FortiDeceptor license add-on SKUs apply to both FortiDeceptor hardware and VM.

www.fortinet.com