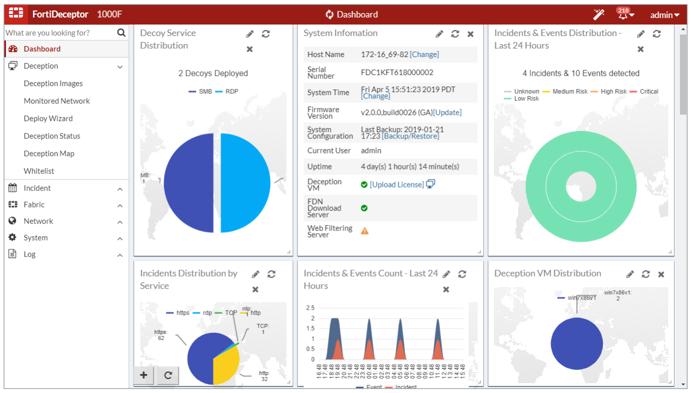
DATA SHEET

FortiDeceptor

FortiDeceptor is designed to deceive, expose and eliminate advanced attacks by breaking the kill chain and stopping malware from spreading and provide visibility to malicious activity that may have slipped past traditional security controls. It automates the creation of decoys Deception VMs or decoys to provide an internal layer of protection to lure and expose stop attackers that have penetrated the network.

Fortinet Security Fabric provides unified, end-to-end protection with Fortinet Enterprise Firewalls to battle advanced persistent threats. Adding FortiDeceptor as Breach Prevention suite expands your defenses with deception based detection and robust security alert information that is both actionable and automated. FortiDeceptor lays out a layer of Decoys and lures, helping you conceal your valuable network assets behind a fabricated **Deception Surface** to confuse and redirect attackers while revealing their presence on your network.



Host Name	172-16_69-82 [Change]
Serial Number	FDC1KFT618000002
System Time	Fri Apr 5 15:51:23 2019 PDT [Change]
Firmware Version	v2.0.0,build0026 (GA)[Update]
System Configuration	Last Backup: 2019-01-21 17:23 [Backup/Restore]
Current User	admin
Uptime	4 day(s) 1 hour(s) 14 minute(s)
Deception VM	✓ [Upload License]
FDN Download Server	✓
Web Filtering Server	⚠

FortiDeceptor Dashboard

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 and SCADA VMs that are indistinguishable from real assets, to lure attackers into revealing themselves.

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

Eliminate threats by redirecting attackers to deception hosts from production servers. Quarantine attackers with FortiGates in Fortinet Security Fabric to and stop connections to C&C servers to break the kill chain. Stop intrusions and malware infection on network.

Feature Highlights

Deploy Decoy VMs and Setup Lures in both Enterprise and SCADA 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 on Decoy VMs.

Eliminate Attacks to/from Decoys by identifying intrusions, websites visits and malware planted during attacks.

Security Fabric Integration with FortiGate by automated quarantine source of attack.

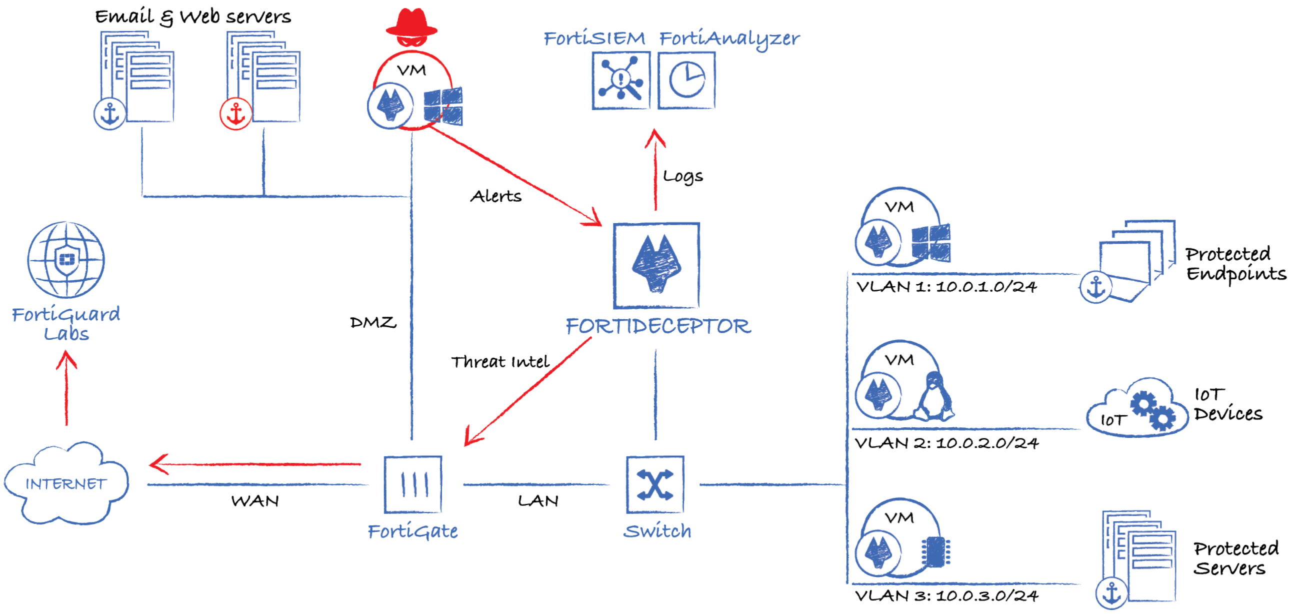
Generate Custom and Comprehensive Reports from incident tables from the GUI in PDF format.

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

Threat Management

FortiDeceptor deploys Decoys VMs which inspect the behavior of the attacker and validate the malicious intent. Attackers are redirected to deception hosts and away from customers' real production servers, thus protecting high value company assets. When an attack has been detected, actionable intelligence (IoCs & TTPs) are subsequently generated and the information is shared across a broad set of in-line security controls through the integration with Fortinet's Security Fabric to proactively block these unknown threats in real-time. Companies can create automated response processes to shut down current attacks and to prevent or detect future attacks. Security operations teams are notified with alerts and counter intelligence so that the kill chain is broken and attacks can be shut down immediately.

Deployment



Specifications

FORTIDECEPTOR VM	
Capacity	
Deception VM OS	Windows and Ubuntu
VM Instance support	Combination of Windows 7, Windows 10, Linux and/or SCADA
VLANs support (maximum)	32
Deception VMs Shipped	0 Upgradable to max. 256
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 and Ubuntu
VM Instance support	Combination of Windows 7, Windows 10, Linux and/or SCADA
VLANs support (Maximum)	32
Deception VMs Shipped *	2 Win (1 x Win7 & 1 x Win10) and 8 Linux
Hardware Specifications	
Form Factor	1 RU Rackmount
Total Interfaces	4 x GbE (RJ45), 4 x GbE (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
Redundant Hot Swap Power Supplies	✓
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, 60-50 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 VMs, upgradable to max 16 VMs (256 decoys)
	FC1-10-FDCVM-291-02-DD	One year FortiDeceptor Anti-Reconnaissance & Anti-Exploit Service for (up to) 2 VMs (32 decoys)
	FC2-10-FDCVM-291-02-DD	One year FortiDeceptor Anti-Reconnaissance & Anti-Exploit Service for (up to) 4 VMs (64 decoys)
	FC3-10-FDCVM-291-02-DD	One year FortiDeceptor Anti-Reconnaissance & Anti-Exploit Service for (up to) 8 VMs (128 decoys)
	FC4-10-FDCVM-291-02-DD	One year FortiDeceptor Anti-Reconnaissance & Anti-Exploit Service for (up to) 16 VMs (256 decoys)

Product	SKU	Description
FortiDeceptor-VM Support	FC1-10-FDCVM-248-02-DD	24x7 FortiCare Contract for (up to) 2 VMs (32 decoys) for FDC-VM
	FC2-10-FDCVM-248-02-DD	24x7 FortiCare Contract for (up to) 4 VMs (64 decoys) for FDC-VM
	FC3-10-FDCVM-248-02-DD	24x7 FortiCare Contract for (up to) 8 VMs (128 decoys) for FDC-VM
	FC4-10-FDCVM-248-02-DD	24x7 FortiCare Contract for (up to) 16 VMs (256 decoys) for FDC-VM

Product	SKU	Description
FortiDeceptor-1000F	FDC-1000F	FortiDeceptor 1000F Appliance with 2 WIN VMs (include 1x Win7 and 1 x Win10 licenses) and 8 Linux VMs, upgradable up to max 16 VMs (256 decoys)
	FC-10-FDC1K-247-02-DD	24x7 FortiCare Contract for (up to) 16 VMs for FDC-1000F
	FC-10-FDC1K-291-02-DD	One year FortiDeceptor Anti-Reconnaissance & Anti-Exploit Service

Product	SKU	Description
FortiDeceptor-Licenses Add-Ons*	FDC-UPG-LNX	Expands FortiDeceptor capacity by 2 Linux VMs (32 decoys)
	FDC-UPG-WIN7	Expands FortiDeceptor capacity by 2 VMs running Windows 7. Include 2 x Windows 7 licenses
	FDC-UPG-WIN10	Expands FortiDeceptor capacity by 2 VMs running Windows 10. Include 2 x Windows 10 licenses
	FDC-UPG-SCA	Expands FortiDeceptor capacity by 2 VMs running SCADA VM Include 2 x SCADA VM licenses

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

www.fortinet.com