

FortiOS – The foundation for Security Transformation

Filippo Cassini SVP WW CSE

SECURITYDAY



This document contains confidential material proprietary to Fortinet, Inc.

This document and information and ideas herein may not be disclosed, copied, reproduced or distributed to anyone outside Fortinet, Inc. without prior written consent of Fortinet, Inc.

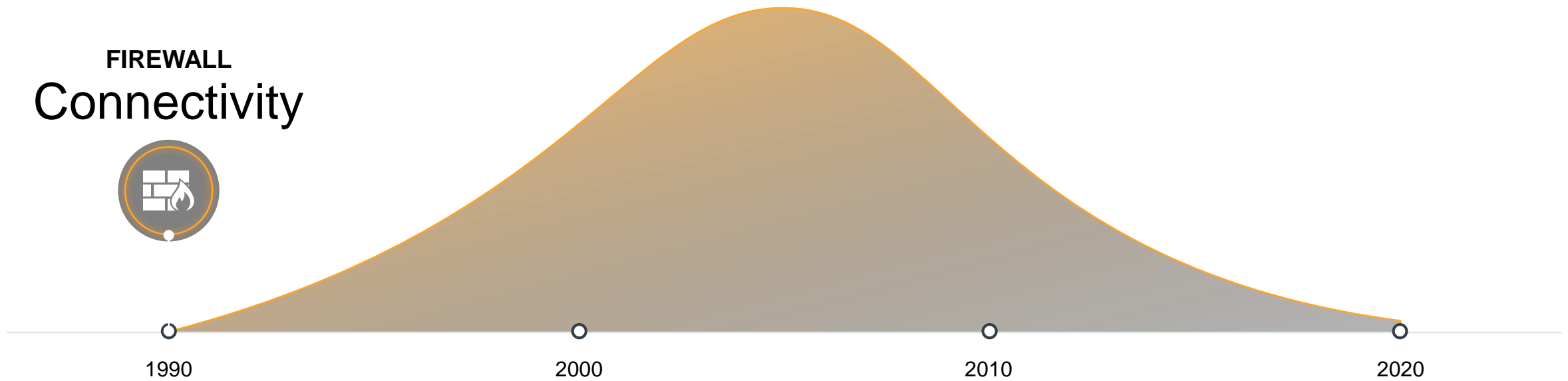
This information is pre-release and forward looking and therefore is subject to change without notice.

The purpose of this document is to provide a statement of the current direction of Fortinet's product strategy and product marketing efforts.

Please note that this Product Roadmap is neither intended to bind Fortinet to any particular course of product marketing and development nor to constitute a part of the license agreement or any contractual agreement with Fortinet or its subsidiaries or affiliates.

Evolution of network security

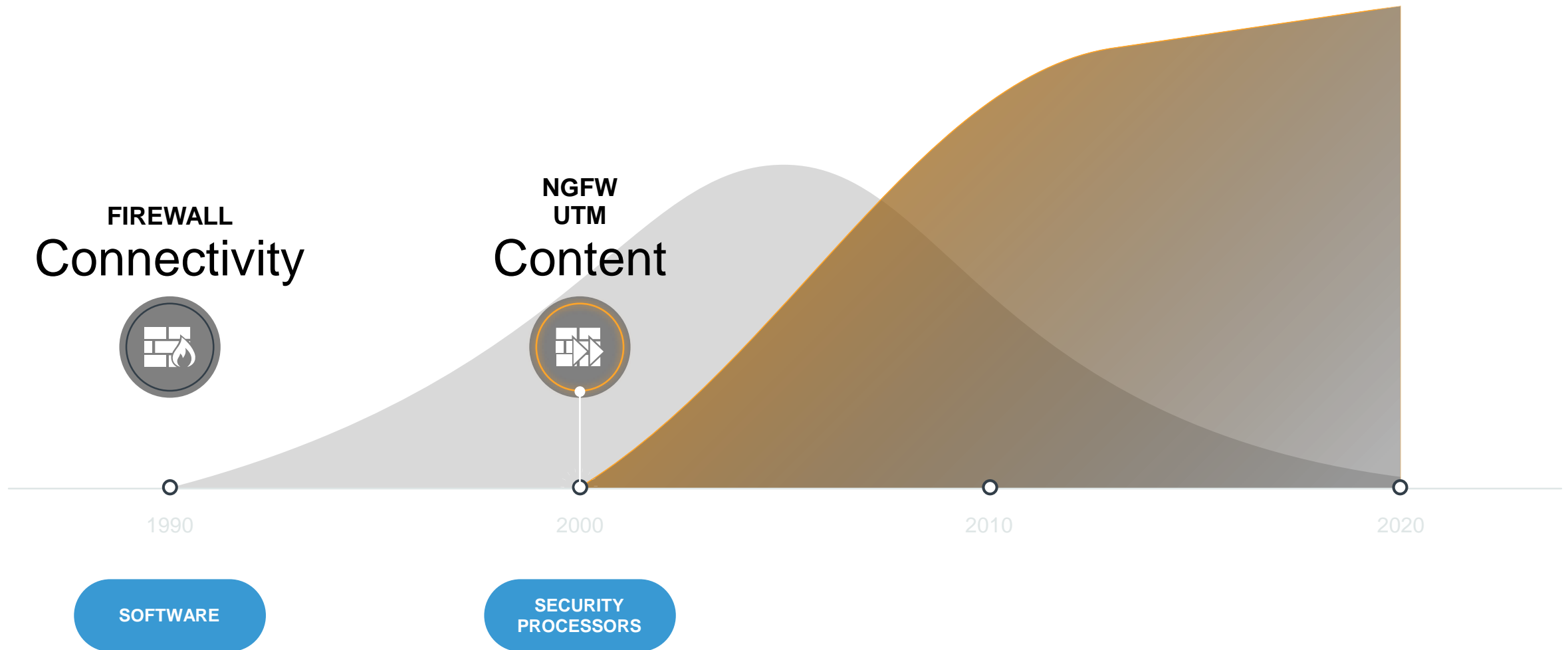
FIREWALL
Connectivity



SOFTWARE

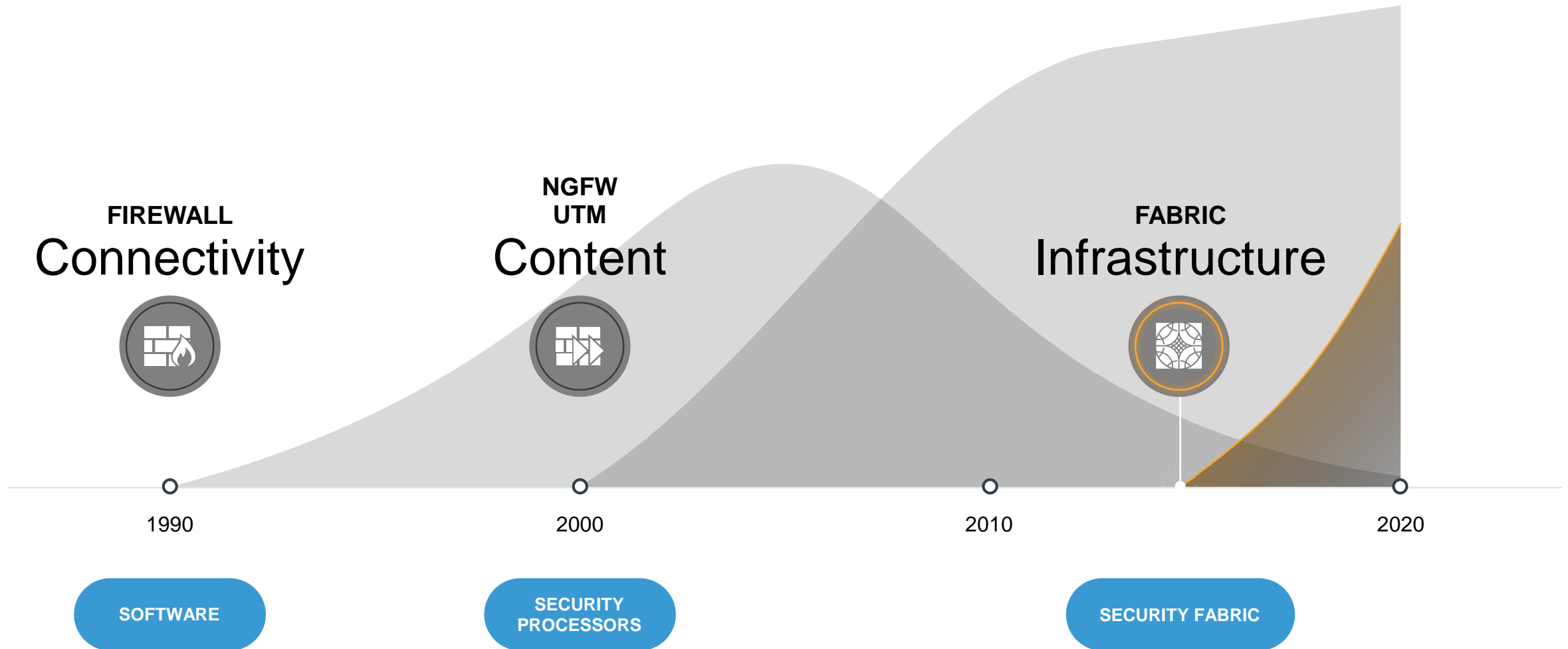
Evolution of network security

- CONTINUED GROWTH IN THE SECOND GENERATION



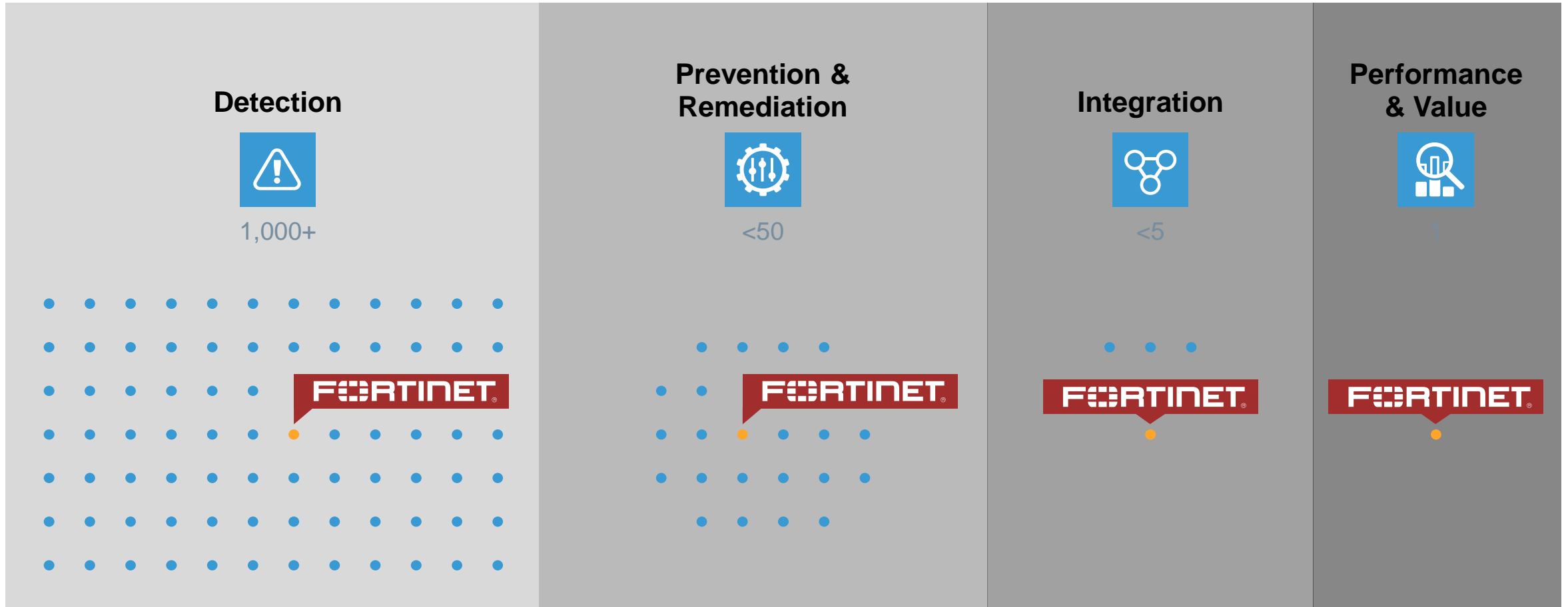
Evolution of network security

- WE ARE IN THE EARLY STAGES OF THE THIRD GENERATION



Only fortinet can reach the HIGHEST LEVELS of security

- SIGNIFICANT ENGINEERING INVESTMENT REQUIRED FOR PERFORMANCE AND VALUE

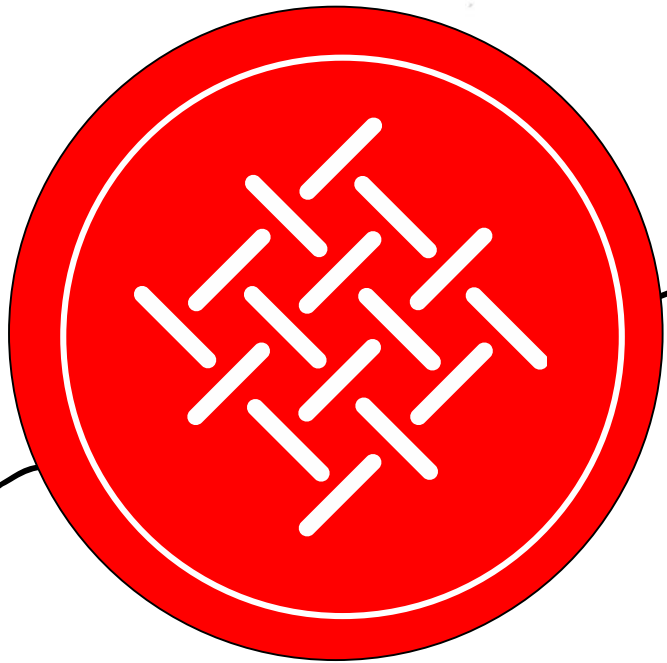


Hey, look at this news alert...

I'll ask IT



Board / C-Suite



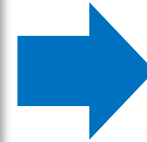
NOC / SOC





• **Expansion Roadblocks**

- Replicated Operations
- Disjointed Systems

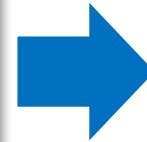


**Scalable
Expansion**



• **Business Disconnect**

- Communication
- Frustration

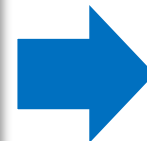


**Business
Alignment**



• **Inefficient Operations**

- Maintenance
- Security Operations
- Incident Response



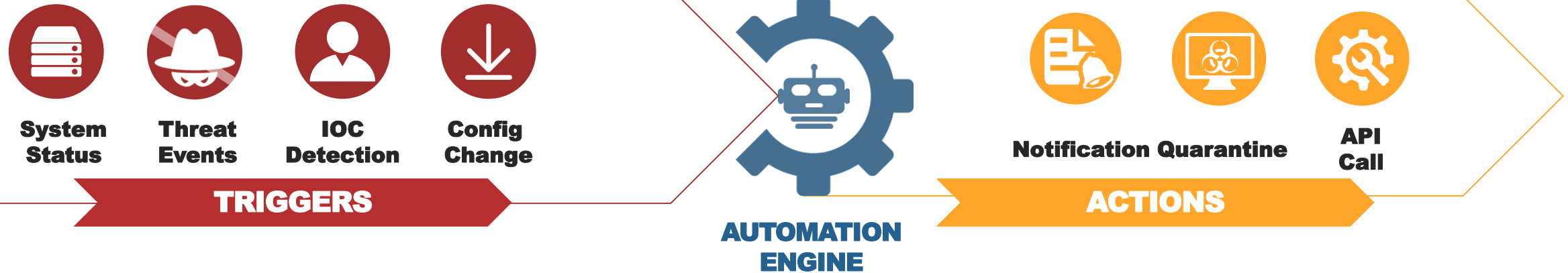
**Streamlined
Operations**



**A CLOSER
LOOK AT
SECURITY
FABRIC ...**

SECURITY FABRIC

Automation



**AUTOMATED WORKFLOWS
(STITCHES) USING
TRIGGERS TO DELIVER
APPROPRIATE ACTIONS**

- ✓ Easy creation using wizards
- ✓ Covers components within a security fabric

SECURITY FABRIC

Automation



STITCHES

Wizard that assist admin to easily setup automation via predefined components

Name	FortiGate	Action	Status
Compromised Host 2			
1_Fabric_Compromised_Quarantine	All FortiGates	Access Layer Quarantine Quarantine FortiClient via EMS	Disabled
4c_IOT_Compromised_TechExpo	All FortiGates	Webhook	Disabled
Configuration Change 1			
5_Cloud_ConfigChange_Breakout	All FortiGates	AWS Lambda	Disabled
Event Log 4			
2_Fabric_Login_Notification	All FortiGates	FortiExplorer Notification	Disabled
3_Fabric_Security_Event_Push	All FortiGates	FortiExplorer Notification	Disabled
4a_IOT_Login_Failure_Breakout	All FortiGates	Webhook	Disabled
4b_IOT_Login_Failure_TechExpo	All FortiGates	Webhook	Disabled

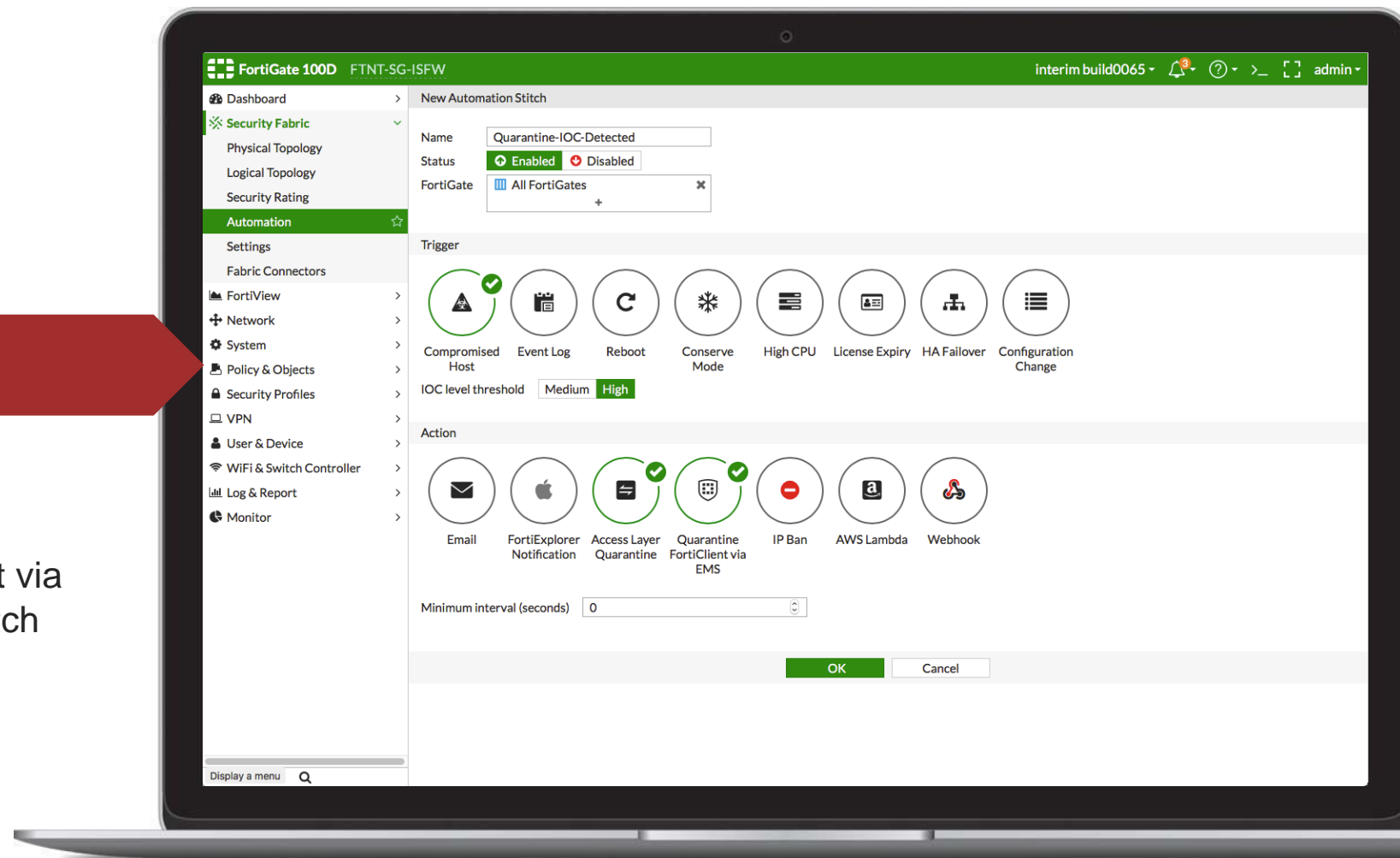
SECURITY FABRIC

Automation



QUARANTINE

- Automatically quarantine compromised hosts via Stitch
- Option to do so using FortiClient via EMS or connection via FortiSwitch and FortiAP



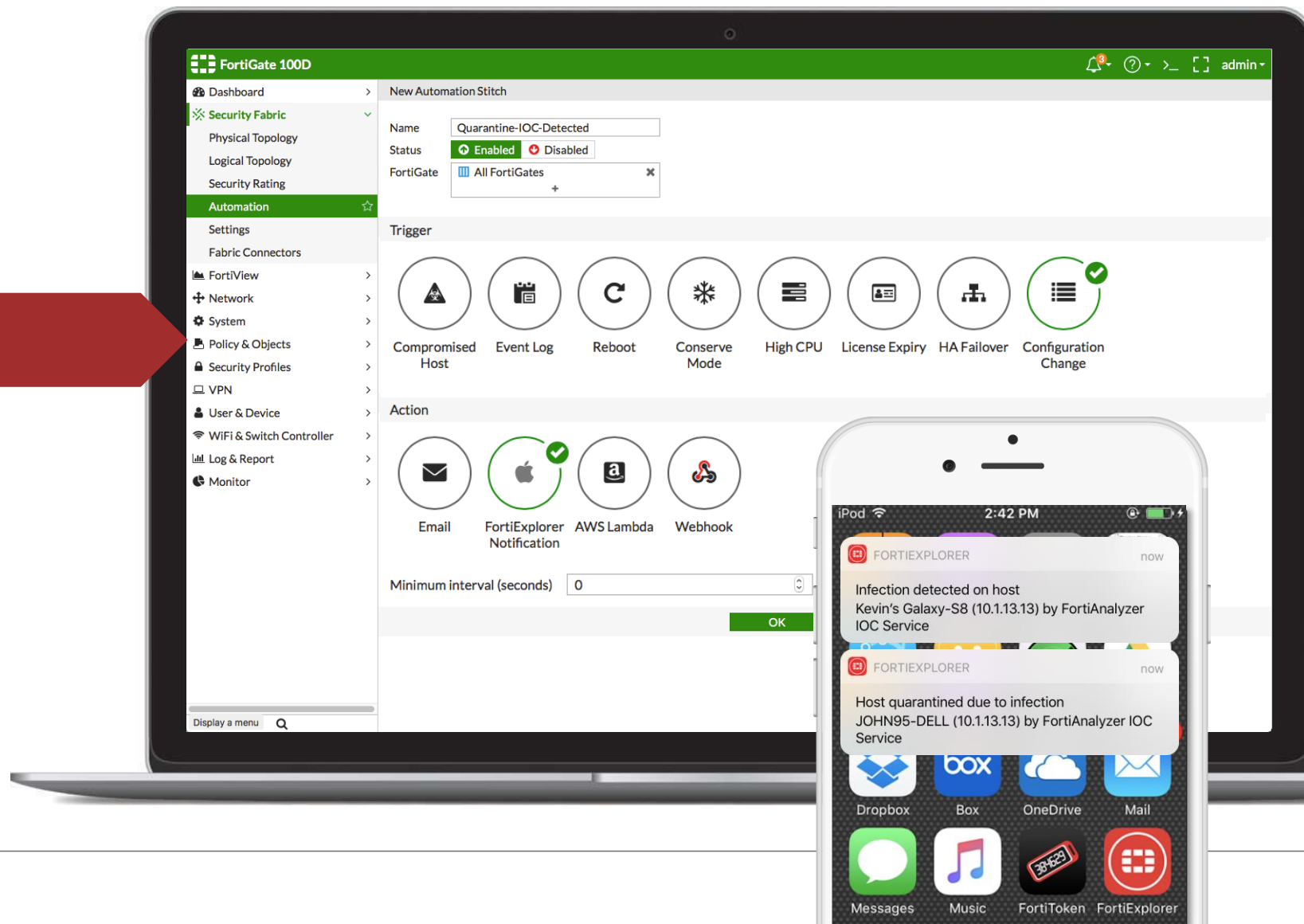
SECURITY FABRIC

Automation



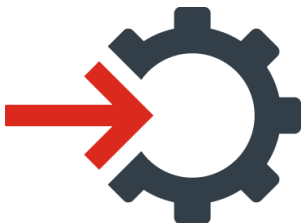
NOTIFICATIONS

- New iOS Push notification via FortiExplorer



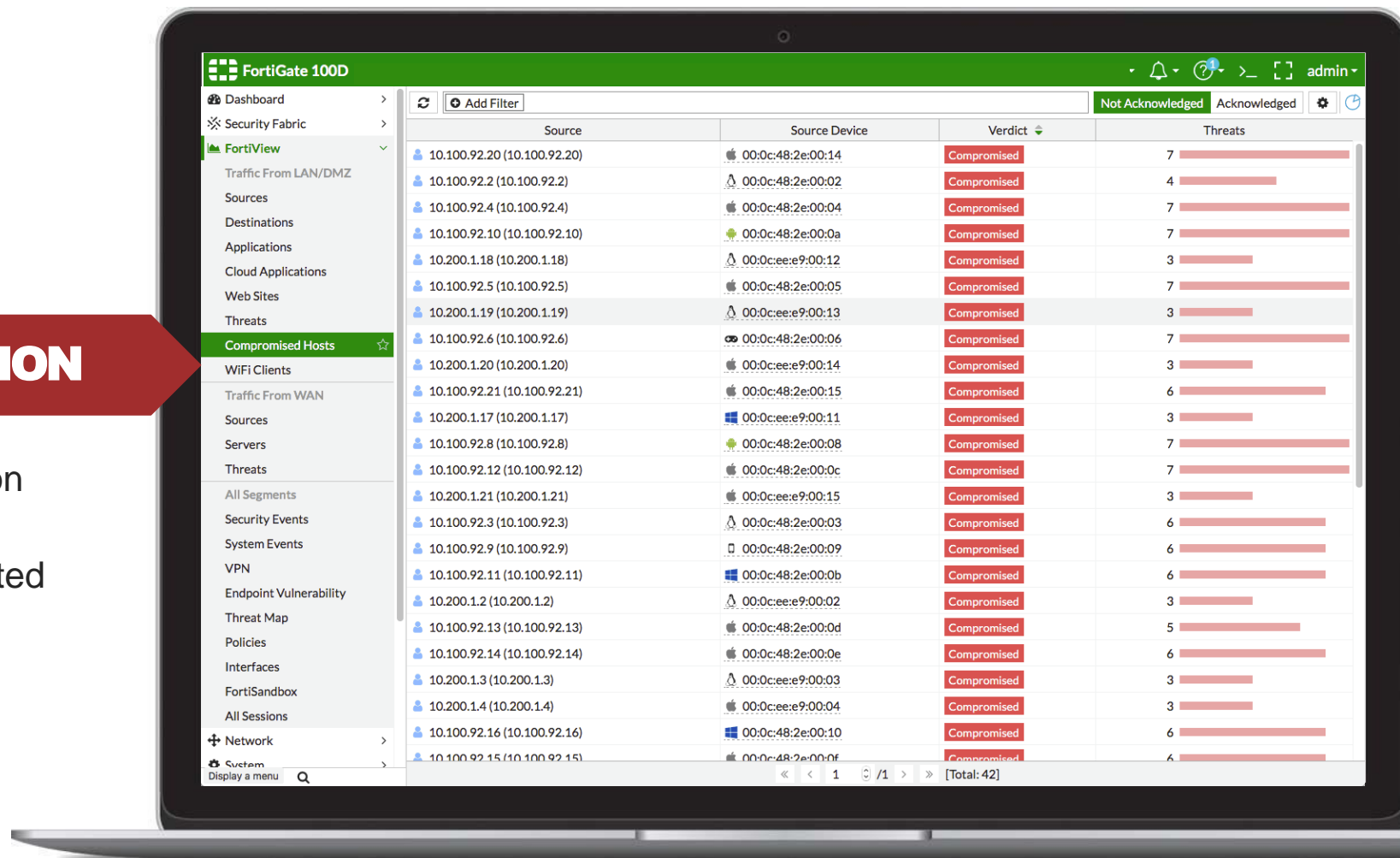
SECURITY FABRIC

New Solution and Service Integration



IOC SERVICE INTEGRATION

- Presenting IOC data from FAZ on FortiView and topology maps
 - » Retrieve data and show affected hosts on FortiGate
 - » Allow admin to quarantine affected hosts



FortiCloud – Fortinet SaaS Cloud

- FortiCloud Key
- FortiDeploy
- Assign to FortiCloud or FortiManager

- Easy to use Interface
- Multi-Tenancy
- Deploy Templates and Scripts
- Role Privilege Assignment

ZERO TOUCH DEPLOYMENT



MANAGEMENT

1 Year
FortiCloud Sandbox inspection



- Indicators of Compromise
- FortiView & Reporting

SANDBOX

- Free 100 Files a day submission
- On Demand Upload Service

SECURITY ANALYTICS

7 Day
free log retention & analysis

1 Year
Log Retention & Analysis Subscription
(unlimited Log volume)

FortiCloud Security Analytics



GLOBAL THREAT INTELLIGENCE

Detect and mitigate all **known** threats including post infection with IoC



LOCAL THREAT INTELLIGENCE

Discover and mitigate **unknown** threats using FortiCloud FortiView and Sandbox



COOPERATION/ ACTION

Rank	Severity	Recommendation
5	CRITICAL	Zero-Day Vulnerability
4	MEDIUM	Not Connected to Fabric
3	ADVISORY	Logging Disabled

FortiCloud FortiDeploy

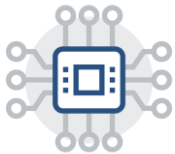
Retail Use Case



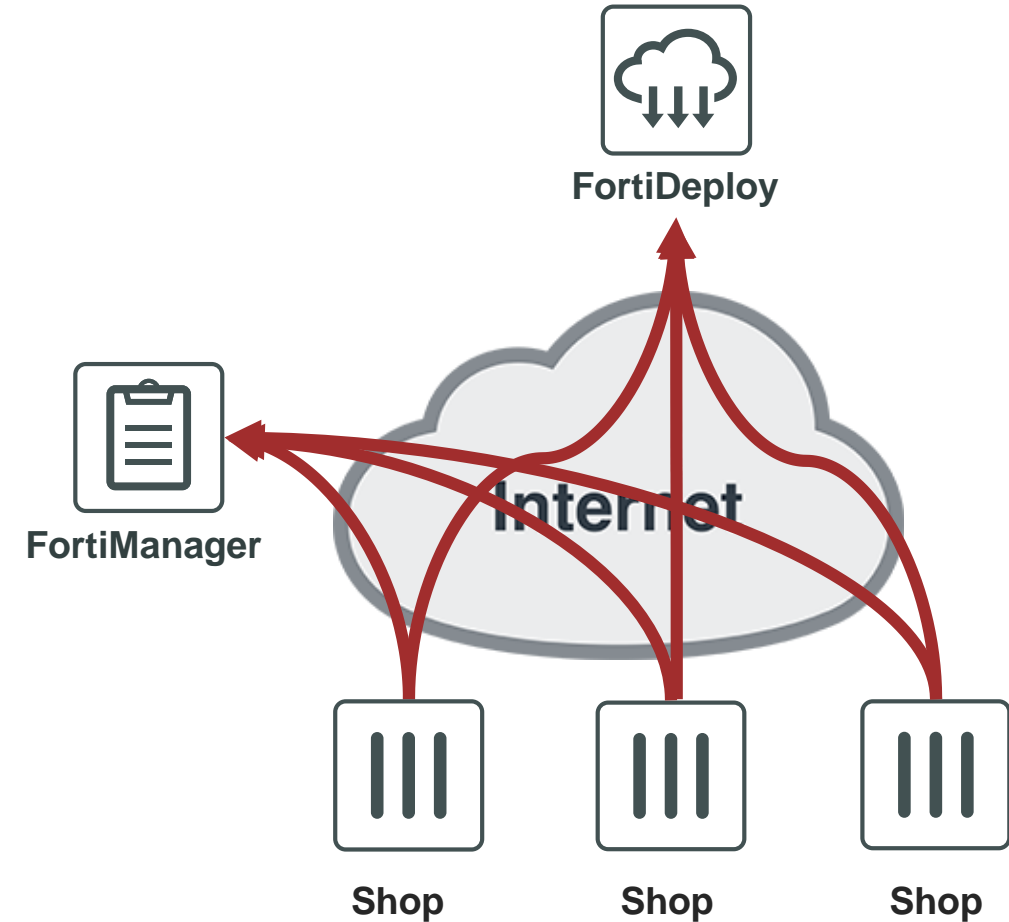
Zero – touch deployment



Includes FMG onboarding automation



Scales to 10K's devices in different countries





A CLOSER LOOK AT SOC FUNCTIONS

BUILT IN CORRELATION (IOC)

Event Management
ADOM: DB_FortiDemo_FGT
admin


- Incident Response
- CIO Dashboard
- Incidents
- Event Monitor
- All Events
- Custom View
- Event Handler List
- Calendar View

Refresh
Last 7 Days
Event Handler List

Recent Events (266) Show Acknowledged

#	Event Name	Count	Severity	Event Type	Last Update	Handler	Additional Info
1	Spyware CnC	7	Critical	IOC	2017-08-22 12:25:13	IOC Infected	Indicators of Compromise
2	Malicious File Detected	100	Critical	FortiSandbox	2017-08-22 12:18:29	Malicious File Detected	FortiSandbox Detection
3	Domain belongs to a denied category in policy	100	High	DNS	2017-08-22 12:18:05	DNS Botnet C-and-C - High Severity	Domain belongs to a denied category in policy
4	Illegal or Unethical	2	Medium	Web Filter	2017-08-22 12:13:23	UTM Web Filter Event	Potentially Liable
5	FSA/RISK_MALICIOUS	1	High	Antivirus	2017-08-22 12:13:08	UTM Antivirus Event	Virus (FortiGuard ID: 7)
6	Fareit	20	High	Antivirus	2017-08-22 12:21:03	UTM Antivirus Event	Virus (FortiGuard ID: 4318)

#	Date/Time	Device ID	User	Source	Destination IP	Service	Host Name	Action
1	08-22 12:25	FG1K5D3115804...	Peter Smith	10.100.1.100	184.168.221.43	HTTP	blakelieberman.me	pass
2	08-15 08:25	FG1K5D3115804...	Peter Smith	10.100.1.100	184.168.221.35	HTTP	blakelieberman.me	pass
3	08-15 08:25	FG1K5D3115804...	Peter Smith	10.100.1.100	184.168.221.33	HTTP	blakelieberman.me	pass
4	08-15 08:25	FG1K5D3115804...	Peter Smith	10.100.1.100	184.168.221.35	HTTP	blakelieberman.me	pass
5	08-15 08:25	FG1K5D3115804...	Peter Smith	10.100.1.100	50.63.202.48	HTTP	blakelieberman.me	pass
6	08-15 08:25	FG1K5D3115804...	Peter Smith	10.100.1.100	50.63.202.48	HTTP	blakelieberman.me	pass
7	08-15 08:25	FG1K5D3115804...	Peter Smith	10.100.1.100	184.168.221.43	HTTP	blakelieberman.me	pass



Peter Smith
10.100.1.100

OS	Linux 3.16.0
Verdict	Infected
Malware Type	Spyware CnC
Policy ID/UUID	28/99e33412-7263-51e7-af7e-2cb499ec896c
Policy Action	Passthrough
Time Period	12:25:13 08/22/2017

Event Timeline >

Event	Spyware CnC
Severity	Critical
Type	IOC
Count	7
Additional Info	Indicators of Compromise
Last Update	2017-08-22 12:35:13
Event Handler	IOC Infected
Comment	<div style="border: 1px solid #ccc; height: 20px; width: 100%;"></div>

Incidents										
+ Create New Edit Delete Clone More										
All Incidents	#	Incident Number	Incident Date/Time	Incident Reporter	Incident Category	Severity	Status	Affected Endpoint(s)		
Event Monitor	<input checked="" type="checkbox"/>	1	IN000000001	2017-12-11 15:55:16	Josh Choi	Intrusion	Medium	Draft	Wed_Srv_2	
All Events	<input type="checkbox"/>	2	IN000000002	2017-12-11 15:26:32	Admin	Malicious Content	High	Analysis	172.18.45.100	
Custom View	<input type="checkbox"/>	3	IN000000003	2017-12-11 11:12:12	Lucy Tam	DDOS Attack	Medium	Response	Email_Srv_1	

Analysis Page

Right Click

Affected Endpoint and User



Colin Freeman

Van_Office_FW2_Master
CFREEMAN-PC

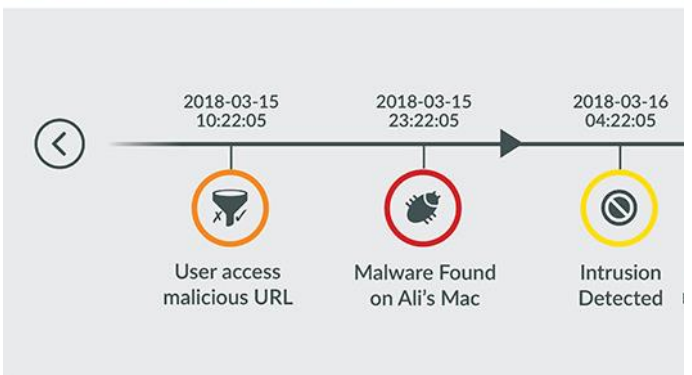
Topology

Zone & Interface: 75_HW_lab (S548DF4K16000343: port44)

Addresses: MAC: 9c-eb-e8-07-08-ef
IP: 192.168.6.10

FortiClient Version: 5.6.2.117 Updated on 2017.12.12

Operating System: Microsoft Windows 7 Professional Updated on 2017.12.10



Network Sessions

Process Name	Destination	Application	Sessions (Blocked/ Allowed)	Bytes (Sent/ Received)	Policy
wlmail.exe	208.91.113.80	UDP/161	10	2.45 kb	219
chrome.exe	172.16.100.117	UDP/161	6	3.51 kb	219
QQProtectUpd.exe	58.250.11.124	UDP/161	4	279 b	219
chrome.exe	216.58.193.74	UDP/161	4	1.23 kb	219
explorer.exe	104.92.141.253	UDP/161	4	3.43 kb	219

Events

Event Status	Event Info	Count	Severity	Event Type	Last Update	Additional Info
Contained	Byanga	22	Medium	IPS	2017-09-20 04:10:12	Buffer Errors (CVE-1999-0003,CVE-1999-0687,)
Open	Dynamic DNS	14	High	IPS	2017-09-20 01:32:06	Buffer Errors (CVE-1999-0003,CVE-1999-0687,C)
Contained	Byanga	6	High	IPS	2017-09-20 01:10:13	Permission/Privilege/Access Control (CVE-201
Mitigated	EICAR_TEST_FILE	6	High	IPS	2017-09-19 20:14:16	Permission/Privilege/Access Control (CVE-2017
Contained	Byanga	6	Medium	IPS	2017-09-19 20:10:13	Buffer Errors (CVE-1999-0003,CVE-1999-0687,)
Mitigated	EICAR_TEST_FILE	6	Medium	IPS	2017-09-19 19:03:37	Permission/Privilege/Access Control (CVE-201
Open	Phishing	6	Medium	IPS	2017-09-19 18:49:49	Permission/Privilege/Access Control (CVE-201
Contained	Domain was blocked by dns botnet C&C	6	Medium	Antivirus	2017-09-19 18:46:42	Virus (FortiGuard ID: 7630075)
Contained	Domain was blocked by dns botnet C&C	4	Medium	IPS	2017-09-19 16:34:18	General
Open	Phishing	4	Medium	IPS	2017-09-19 14:45:21	Permission/Privilege/Access Control (CVE-201
Contained	Domain was blocked by dns botnet C&C	3	Medium	IPS	2017-09-19 14:14:41	Anomaly (CVE-2012-2122)
Contained	Domain was blocked by dns botnet C&C	3	Medium	IPS	2017-09-19 11:55:09	
Contained	FortiDisco.Botnet	3	Medium	Antivirus	2017-09-19 11:39:47	Virus (FortiGuard ID: 7630240)
Open	Phishing	2	Medium	Antivirus	2017-09-19 11:40:03	Virus (FortiGuard ID: 7630240)
Contained	Domain was blocked by dns botnet C&C	3	High	IPS	2017-09-19 11:10:17	Buffer Errors (CVE-1999-0003,CVE-1999-0687
Mitigated	EICAR_TEST_FILE	3	High	IPS	2017-09-19 09:57:04	Buffer Errors (CVE-1999-0003,CVE-1999-0687,)



A CLOSER LOOK AT NETWORKING...

NETWORKING

SD-WAN Improvements

PATH SELECTION STRATEGY

Recommended Use Case

BEST QUALITY

Administrators who prefer simplistic path selection, relying on preferred quality criteria

MIN. QUALITY (SLA)

Administrators who desire granular threshold configurations per applications

Outgoing Interfaces

Strategy **Best Quality** Minimum Quality (SLA)

Interface preference wan1 wan2 +

Measured SLA salesforce.com

Quality criteria **Latency** Jitter Packet Loss Downstream Upstream Bandwidth custom-profile-1

OK Cancel

Outgoing Interfaces

Strategy Best Quality **Minimum Quality (SLA)**

Interface preference wan1 wan2

Required SLA target salesforce.com#1 +

SLA salesforce.com#1
Criteria Jitter: 5ms

OK Cancel

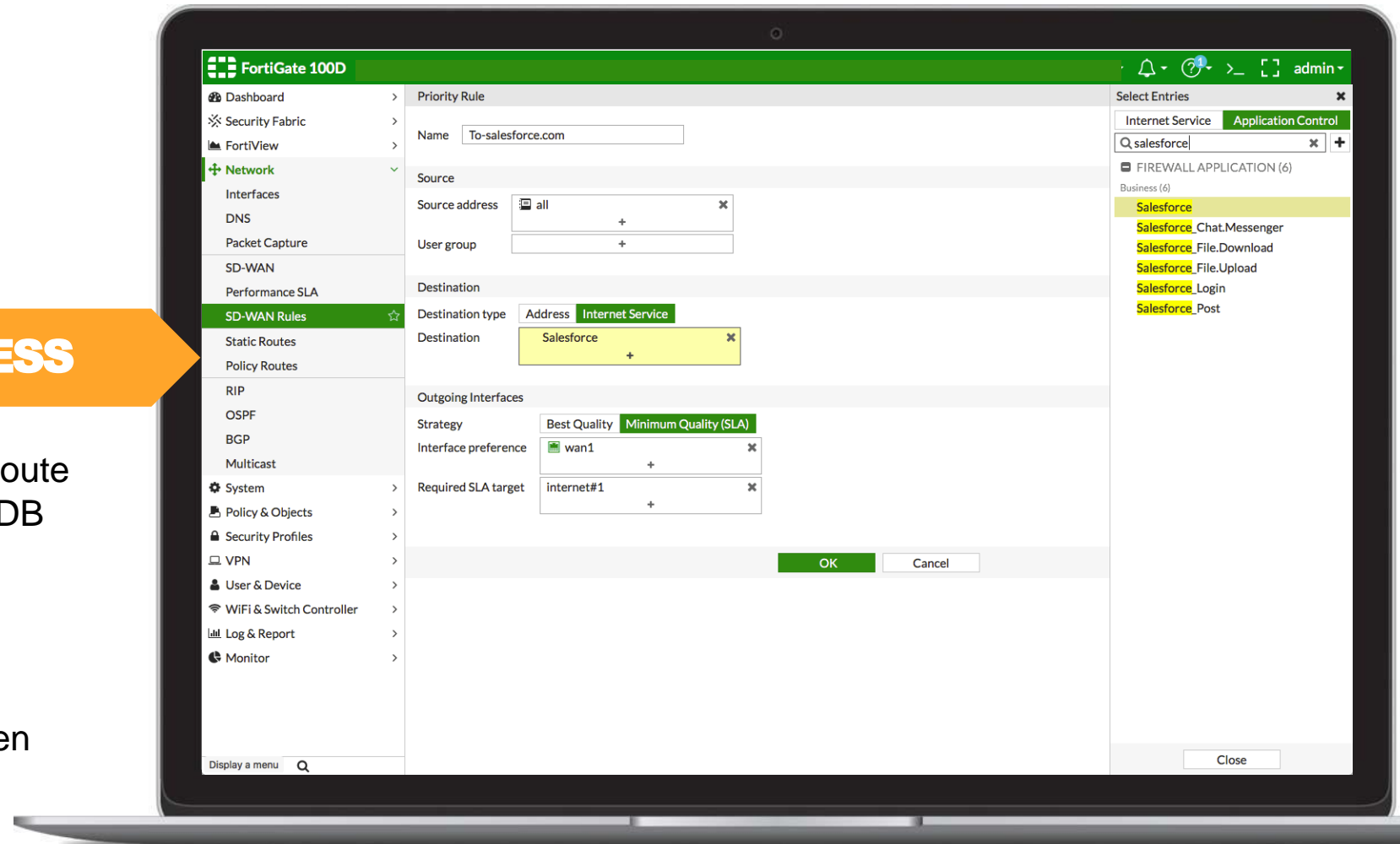
NETWORKING

SD-WAN Improvements



APPLICATION AWARENESS

- WAN Path Controller is able to route traffic using Application Control DB (with over 3,000 signatures), in addition to ISDB
- Once identified via application control, subsequent matching sessions are identified when seen next time on first packet



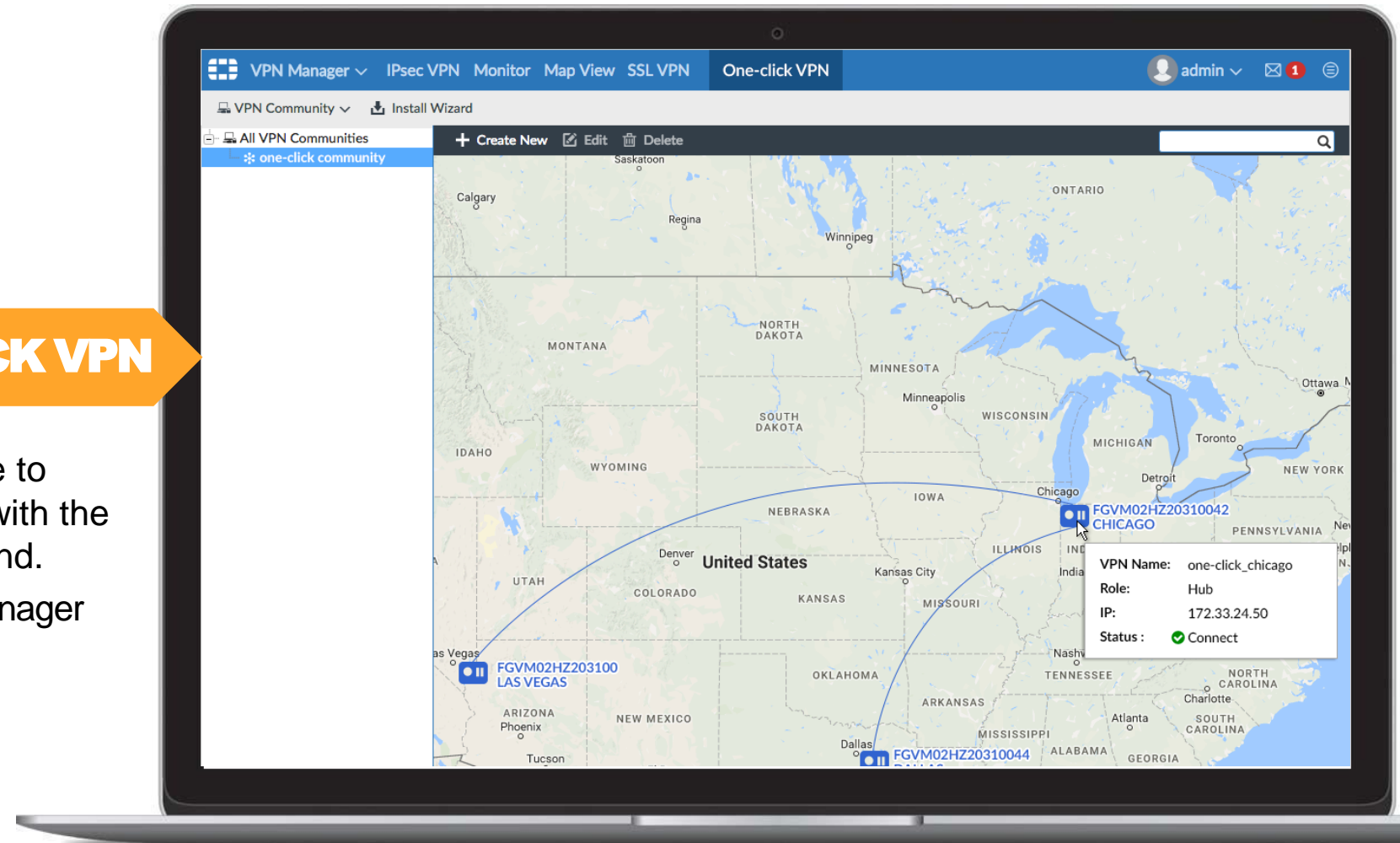
NETWORKING

VPN Configuration Enhancements



CLOUD-ASSISTED ONE-CLICK VPN

- Allows multiple sites of Fortigate to configure hub-and-spoke VPN with the help of FortiCloud on the backend.
- Can be implemented with FortiManager backup mode as another option



The logo for FERTINET is displayed in a bold, white, sans-serif font. The letter 'F' is stylized with three horizontal bars. The letters 'E', 'R', 'T', 'I', 'N', and 'E' are solid. The final 'T' is also solid. A registered trademark symbol (®) is located to the right of the final 'T'. The logo is centered horizontally on a dark blue background that features a complex, white, isometric wireframe pattern of overlapping rectangular and cubic shapes.

FERTINET®