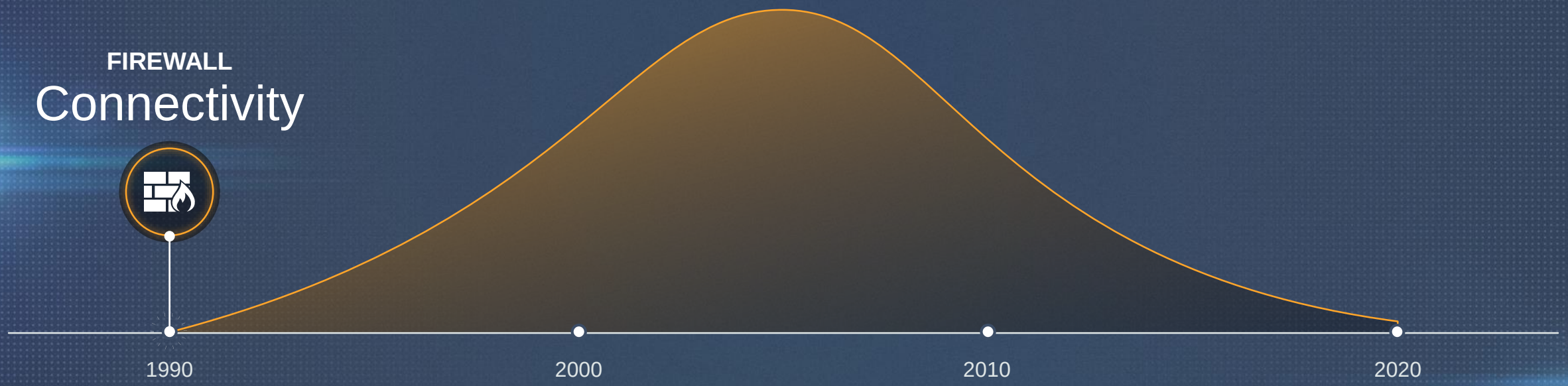
FORTINET SECURITY FABRIC

ALEJANDRO REYEROS

1st Generation

EVOLUTION OF NETWORK SECURITY



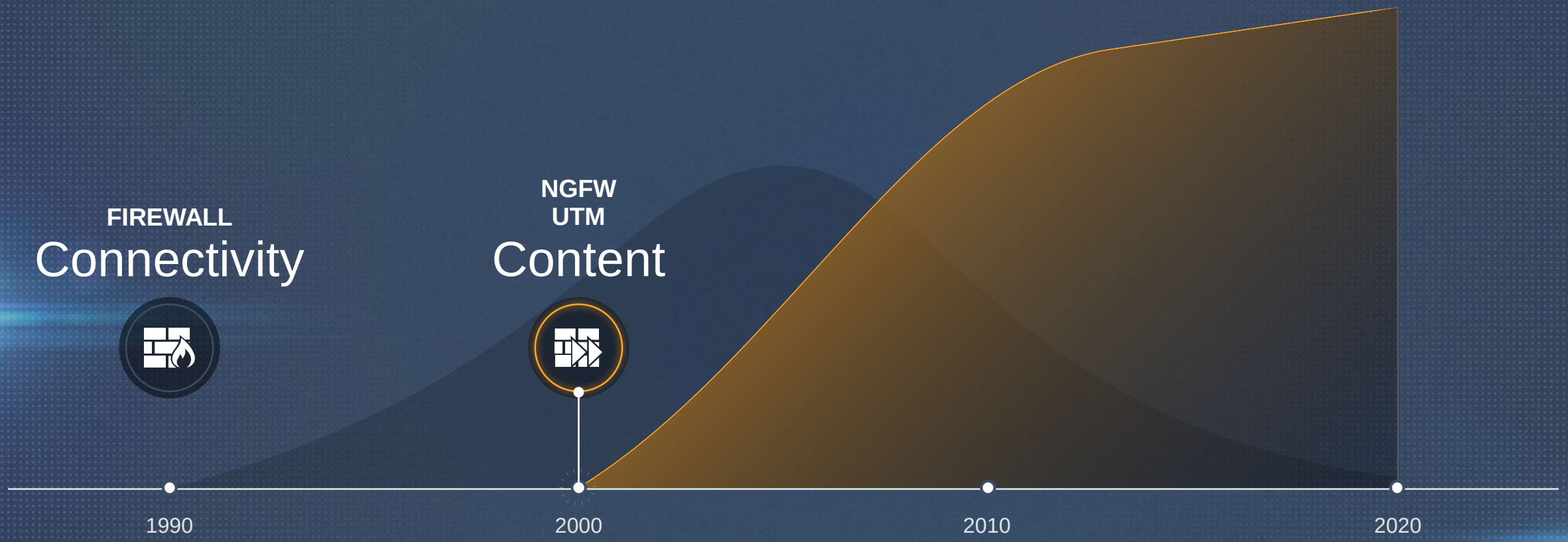
SOFTWARE

FORTINET

1st Generation | 2nd Generation

EVOLUTION OF NETWORK SECURITY

CONTINUED GROWTH IN THE SECOND GENERATION



SOFTWARE + SECURITY PROCESSORS

FORTINET

1st Generation | 2nd Generation | 3rd Generation

EVOLUTION OF NETWORK SECURITY

WE ARE IN THE EARLY STAGES OF THE THIRD GENERATION

FIREWALL
Connectivity

NGFW
UTM
Content

FABRIC
Infrastructure

1990 | 2000 | 2010 | 2020

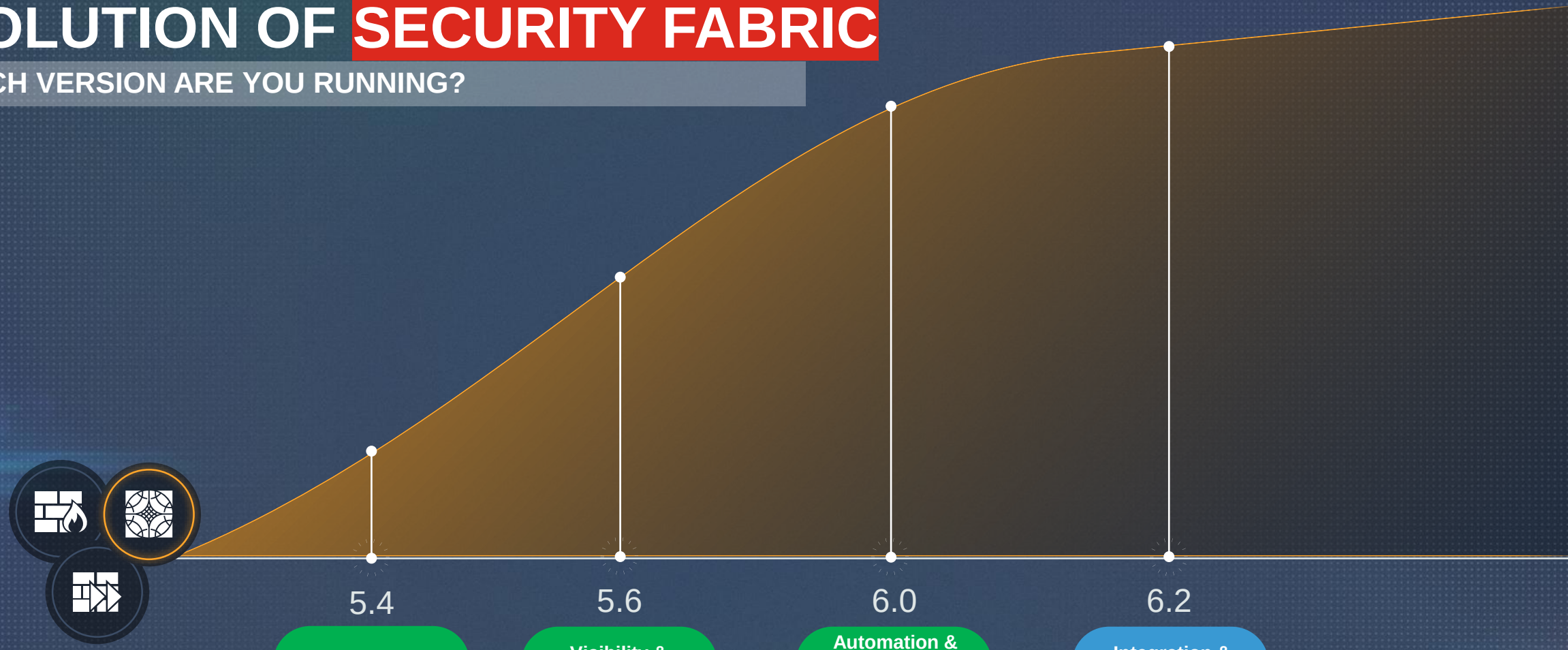
SOFTWARE + SECURITY PROCESSORS + SECURITY FABRIC

FORTINET

1st Generation | 2nd Generation | 3rd Generation

EVOLUTION OF SECURITY FABRIC

WHICH VERSION ARE YOU RUNNING?



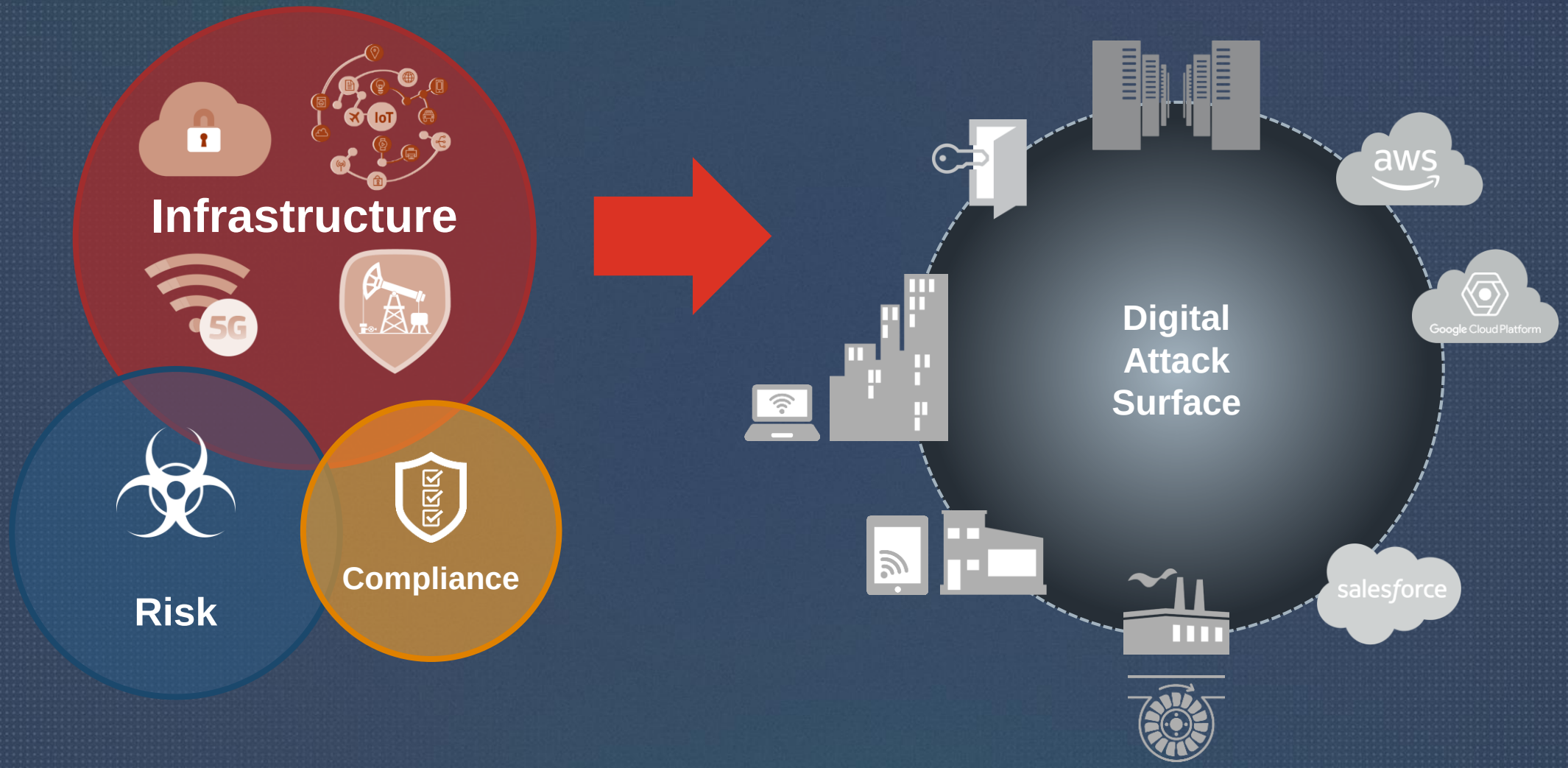
FEATURES	5.4 Telemetry	5.6 Visibility & Control	6.0 Automation & Incident Management	6.2 Integration & Connectors
CISO	Advanced Malware	Policy Awareness & Control	Dynamic Data Protection	Extended Trust & Assurance
FORTINET	1st Gen. Co-ordinated Operations	Reduced time of visibility & management	Self-assessment and automated ops	Managed security state across the topology

SX

[Security Transformation]

is the integration of security into all areas of digital technology resulting in fundamental changes to how security is architected, deployed and operated.

EXPANDING DIGITAL ATTACK SURFACE



MANY DIFFERENT CYBERSECURITY CONTROLS

Information Security

CSO

Analytics | SIEM | AI | Sandboxing | Threat Intelligence | Isolation | Deception | EUBA

Infrastructure Security

Endpoint | NAC | Email | OT | Switch | 5G | Mobile | IoT | Identity | WiFi

Network Security

SD WAN | VPN | FW | NGFW | SWG | ISFW | IPS

Cloud & Application Security

WAF | Cloud | CASB

CIO

CUSTOMER ISSUES

Complexity

Too many security vendors is costly and ineffective

Platform

Manual

Operations creates mistakes and a slow response

Automation

Hybrid

Multiple types of Networks, Clouds and Devices

Integration

Measurement

How well is my Security doing, How can I improve?

Visibility

The Fortinet Security Fabric

Third-Generation Network Security

BROAD

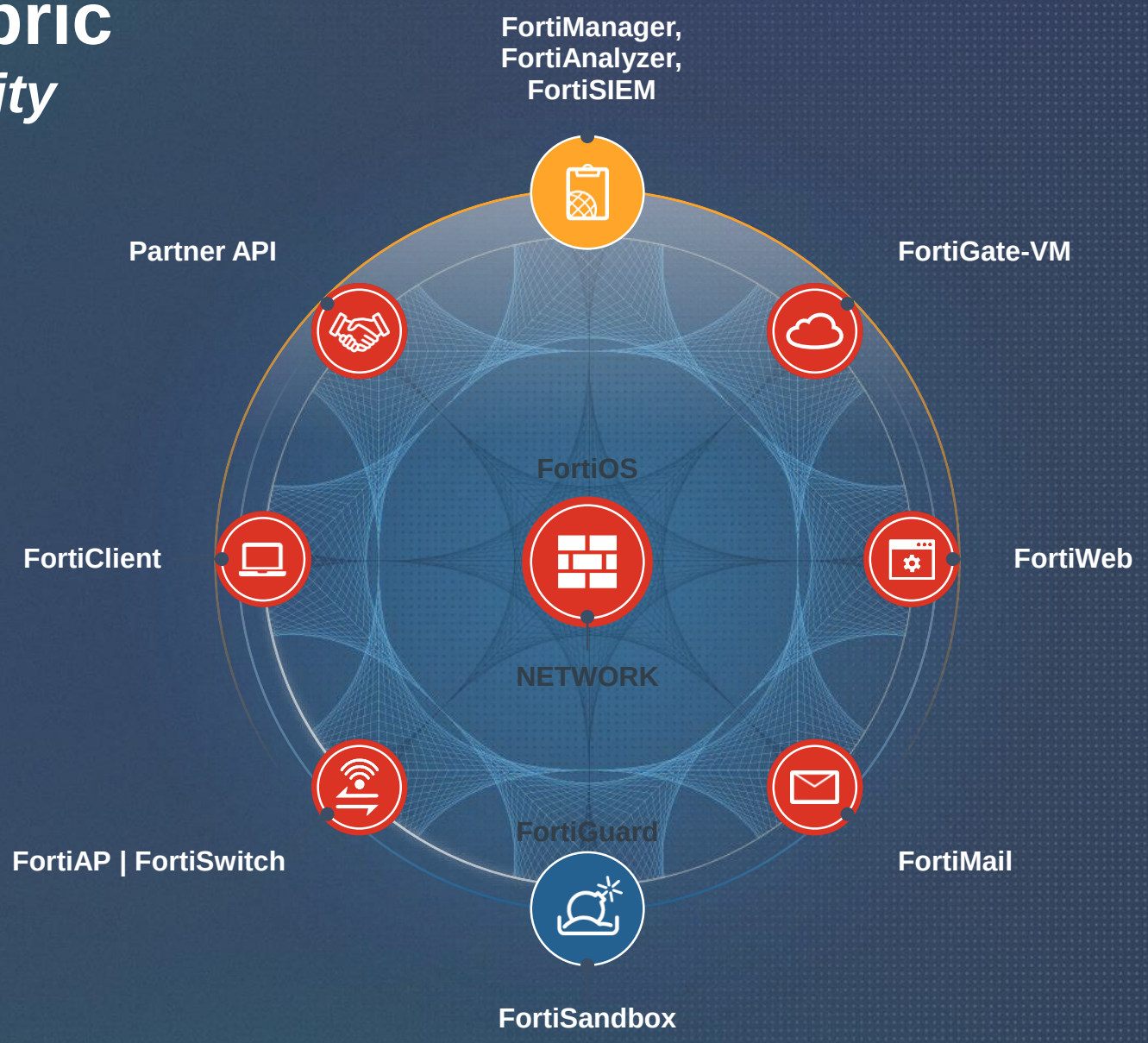
Visibility & Protection for the Digital Attack Surface

INTEGRATED

Detection of Advanced Threats

AUTOMATED

Response & Continuous Trust Assessment



FORTINET

What’s New in 6.0

FORTINET

VERSION 6.0 – WHAT'S NEW

EXPANDING IN 2 DIMENSIONS

1 Expanded **ATTACK SURFACE**

6.0

2 Expanded **SOC INTEGRATION**

1 Expanded **ATTACK SURFACE**

INTEGRATE

EXPAND

MEASURE

Telemetry

Access

Endpoint

Historical

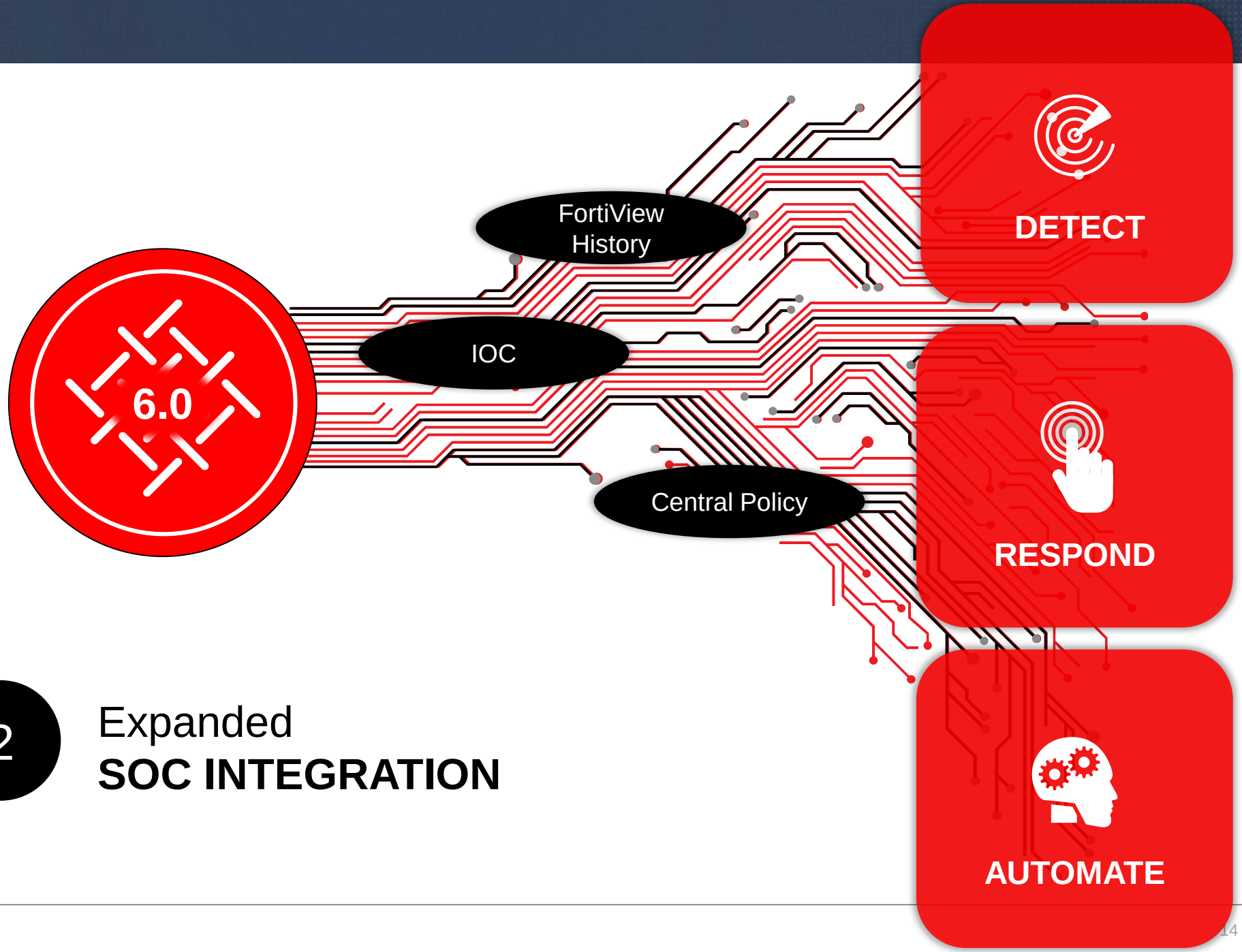
6.0

5.6
- visibility
- control

6.0
- integrate
- expand
- measure

5.6
- historical
- IOC

6.0
- detect
- respond
- automate



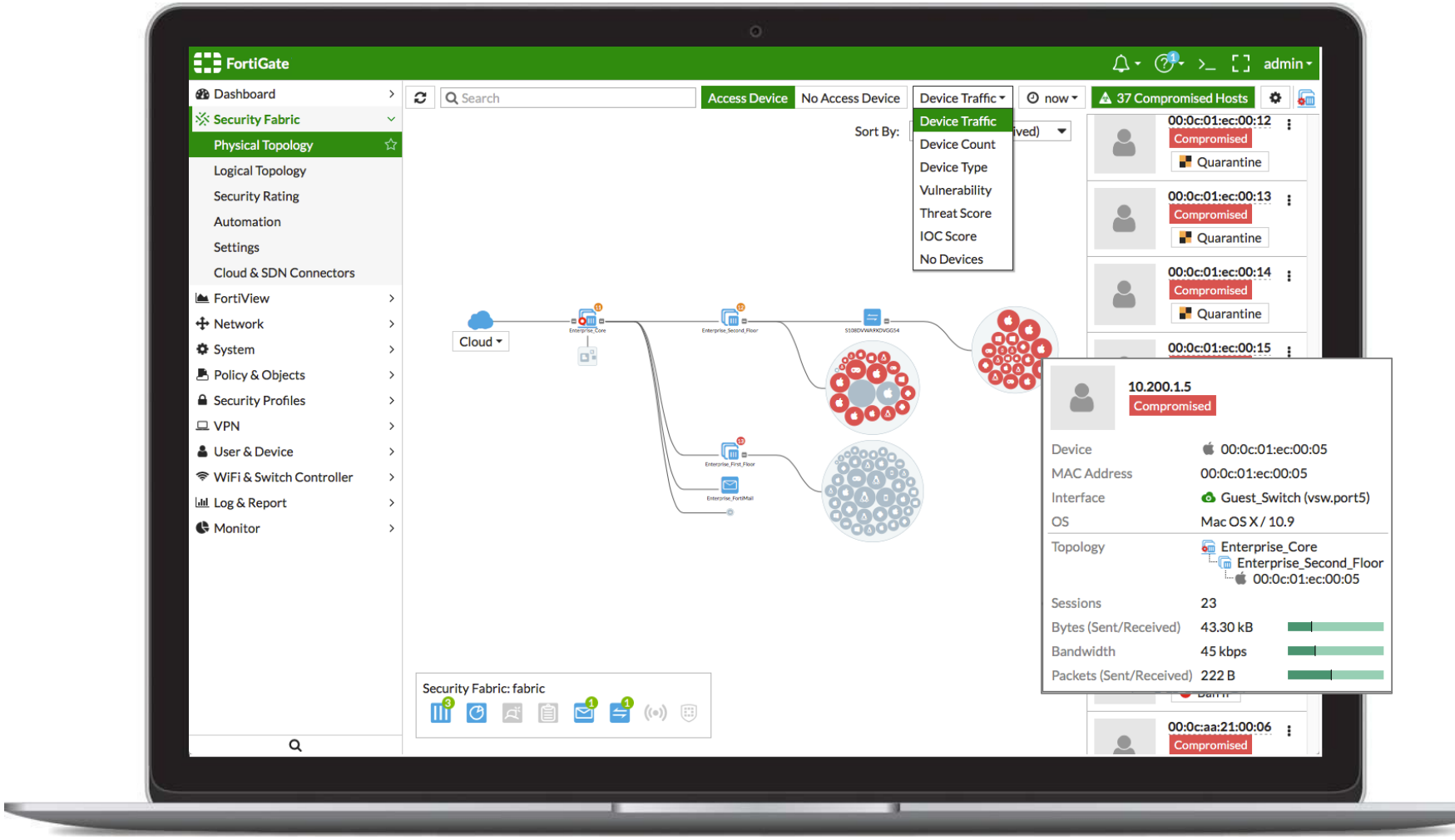
2

Expanded
SOC INTEGRATION

VISIBILITY

TOPOLOGY MAPS

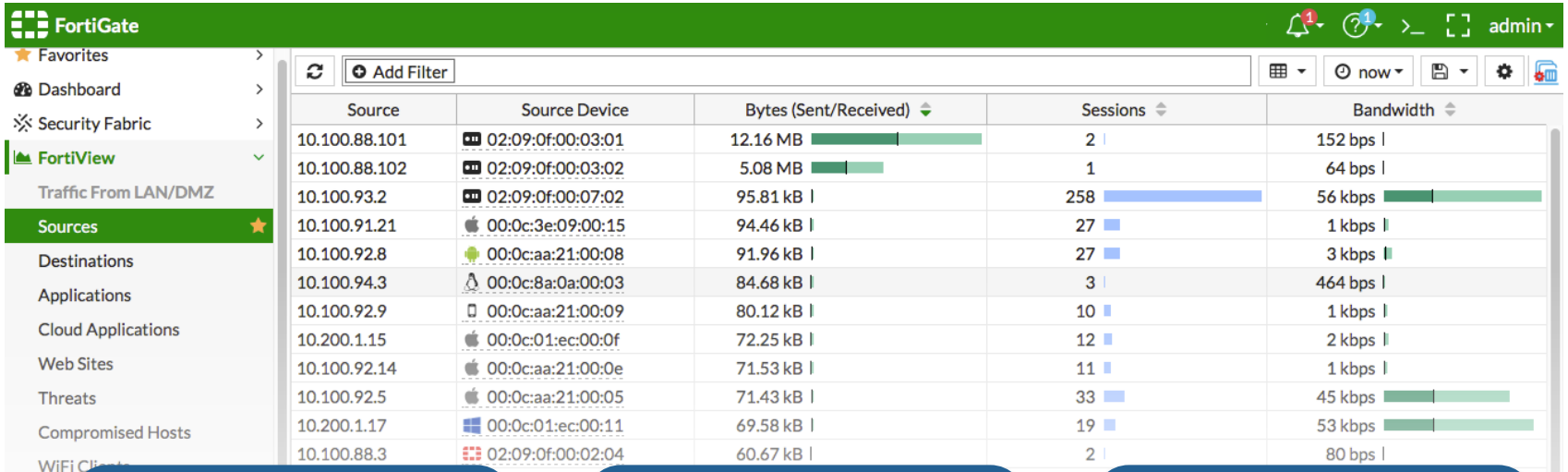
- Visualization of Security Fabric components from physical and logical connectivity perspective
- Mouse-over for endpoint contextual details
- Remote login to downstream FortiGates



VISIBILITY

FORTIVIEW

- Powerful on-demand query tool that provides contextual results with drill down capabilities
- Presents in various viewers
- Uses real-time or historical data from FortiAnalyzer or FortiCloud
- Aggregated data from downstream FortiGates within the Security Fabric



Is there an abnormality that needs further investigation?

Acquires proactive security knowledge

Supports proactive security management

Are my users abusing the network and how so?

Identifies network and threat status

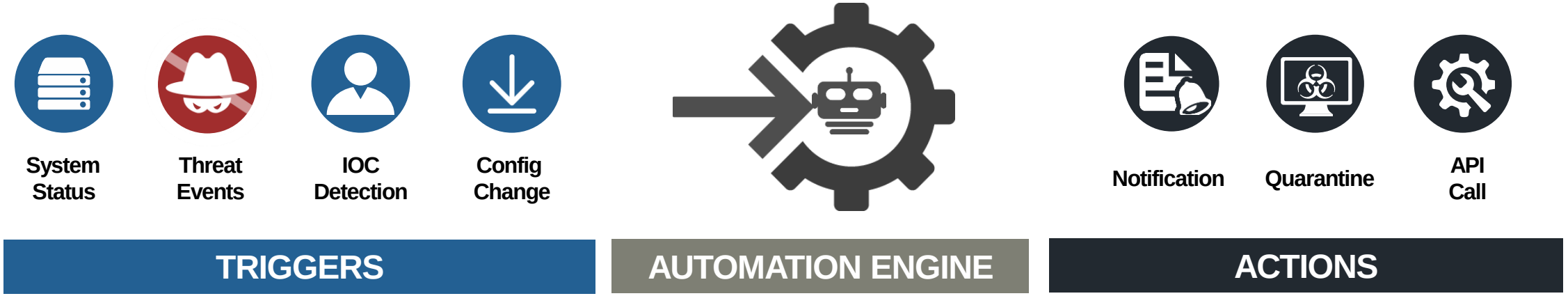
Resolves threats and networking problems quickly

Why is a particular group of users is having trouble using the cloud based ERP system?

Assists in network troubleshooting

Provides insights to optimizing networks & productivity

AUTOMATION

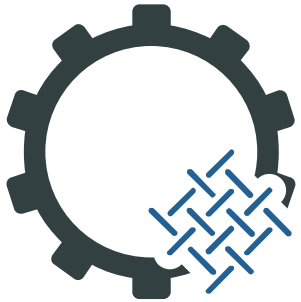


Automated workflows (stitches) using triggers to deliver appropriate actions

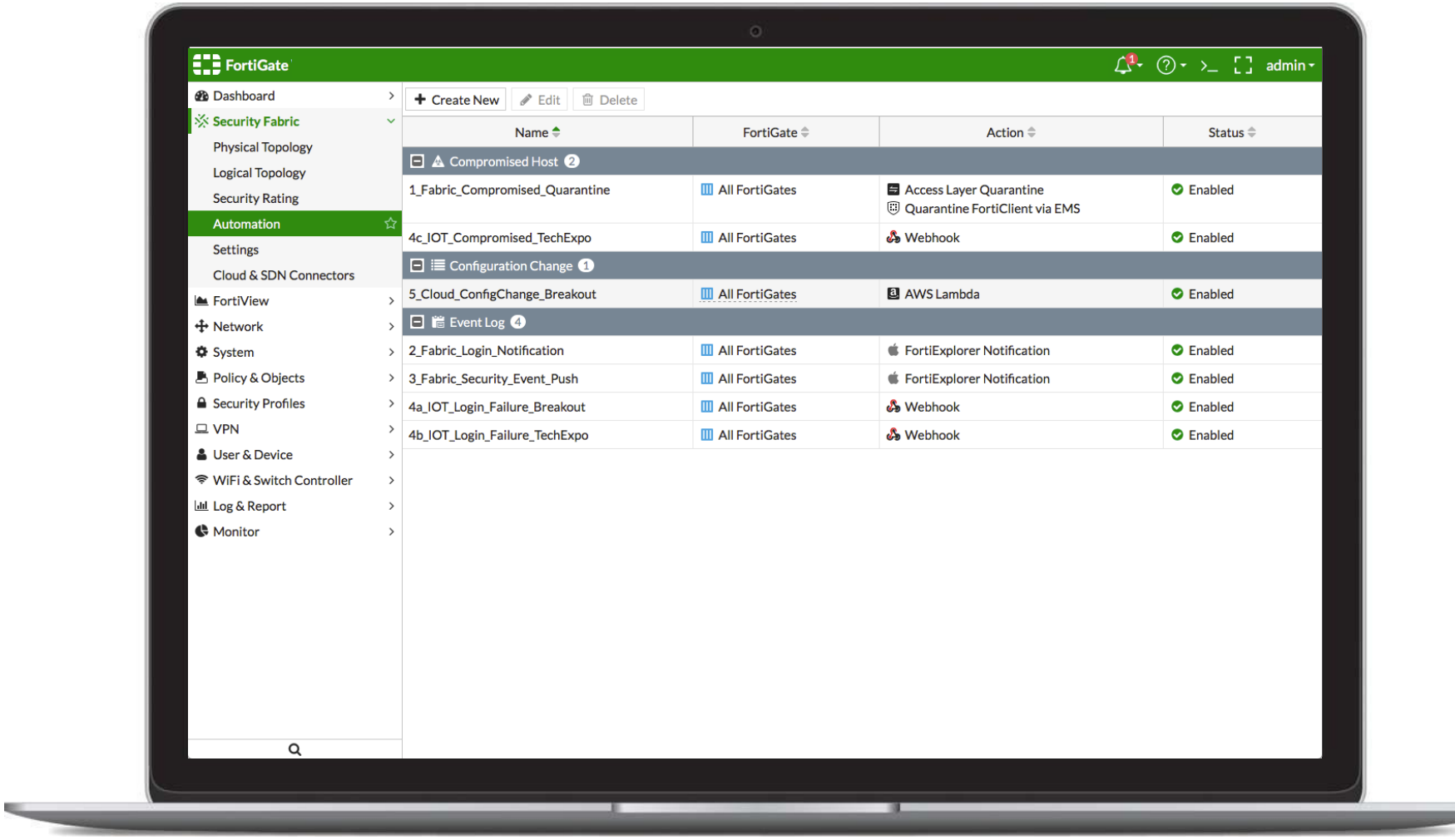
- ✅ Easy creation using wizards
- ✅ Covers components within a security fabric

AUTOMATION

STITCHES

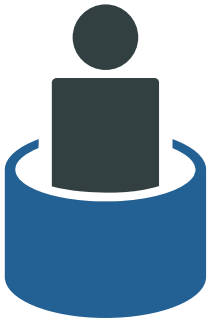


- Wizard that assist admin to easily setup automation via predefined components

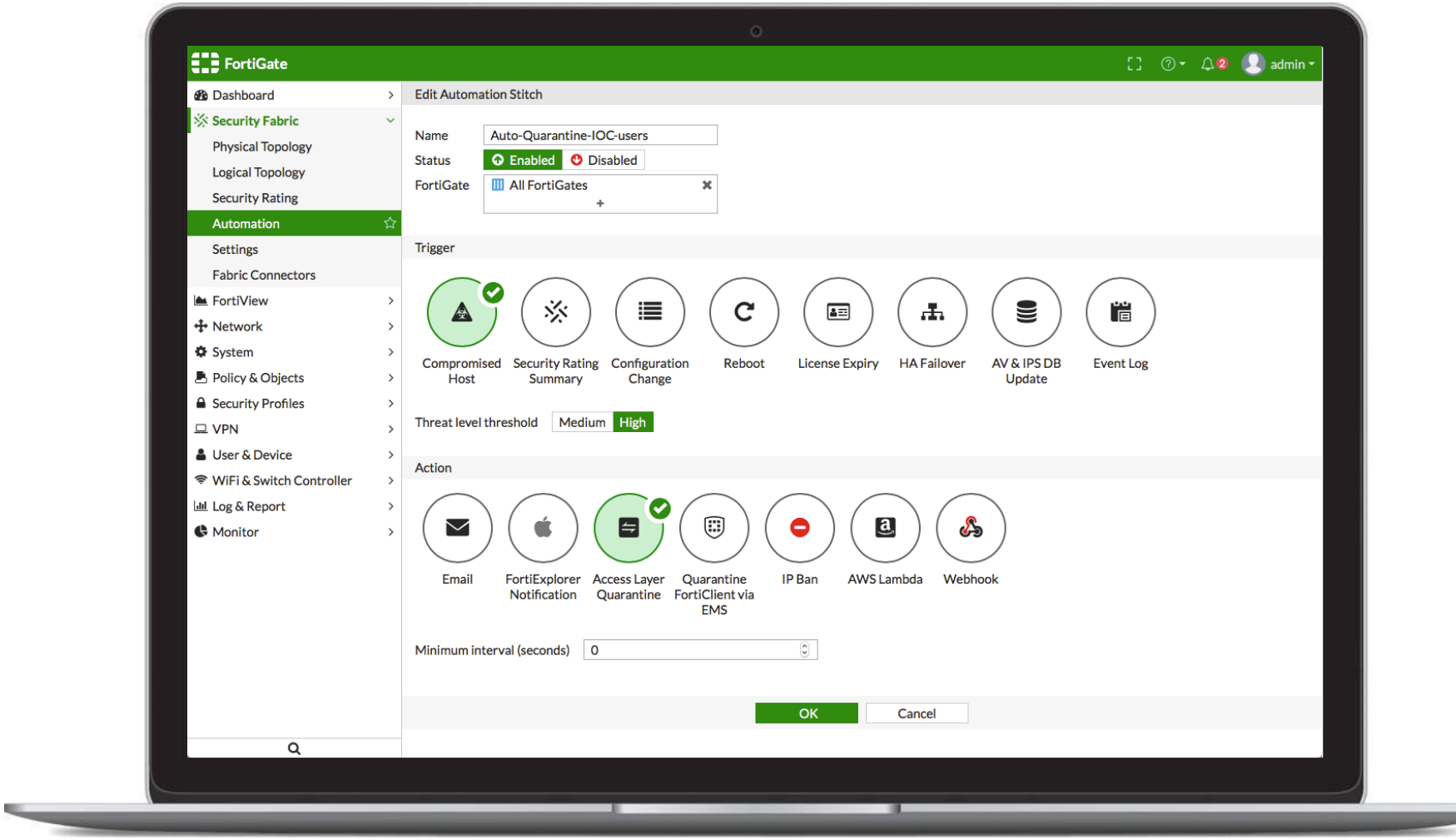


AUTOMATION

QUARANTINE

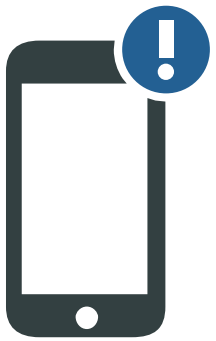


- Automatically quarantine compromised hosts via Stitch
- Option to do so using FortiClient via EMS or connection via FortiSwitch and FortiAP

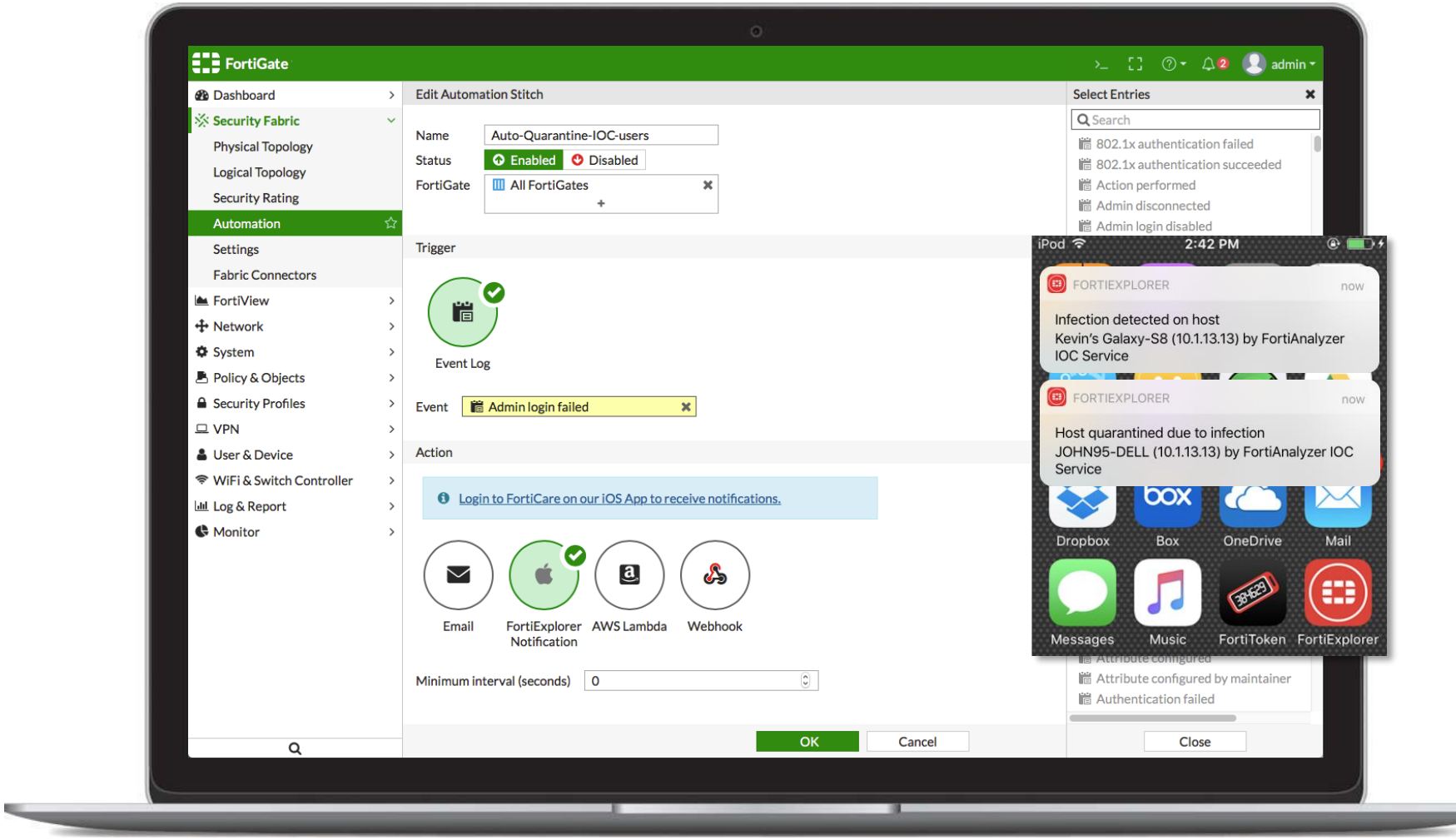


AUTOMATION

NOTIFICATIONS



- iOS Push notification via FortiExplorer



Security Rating Feature Illustrative Model

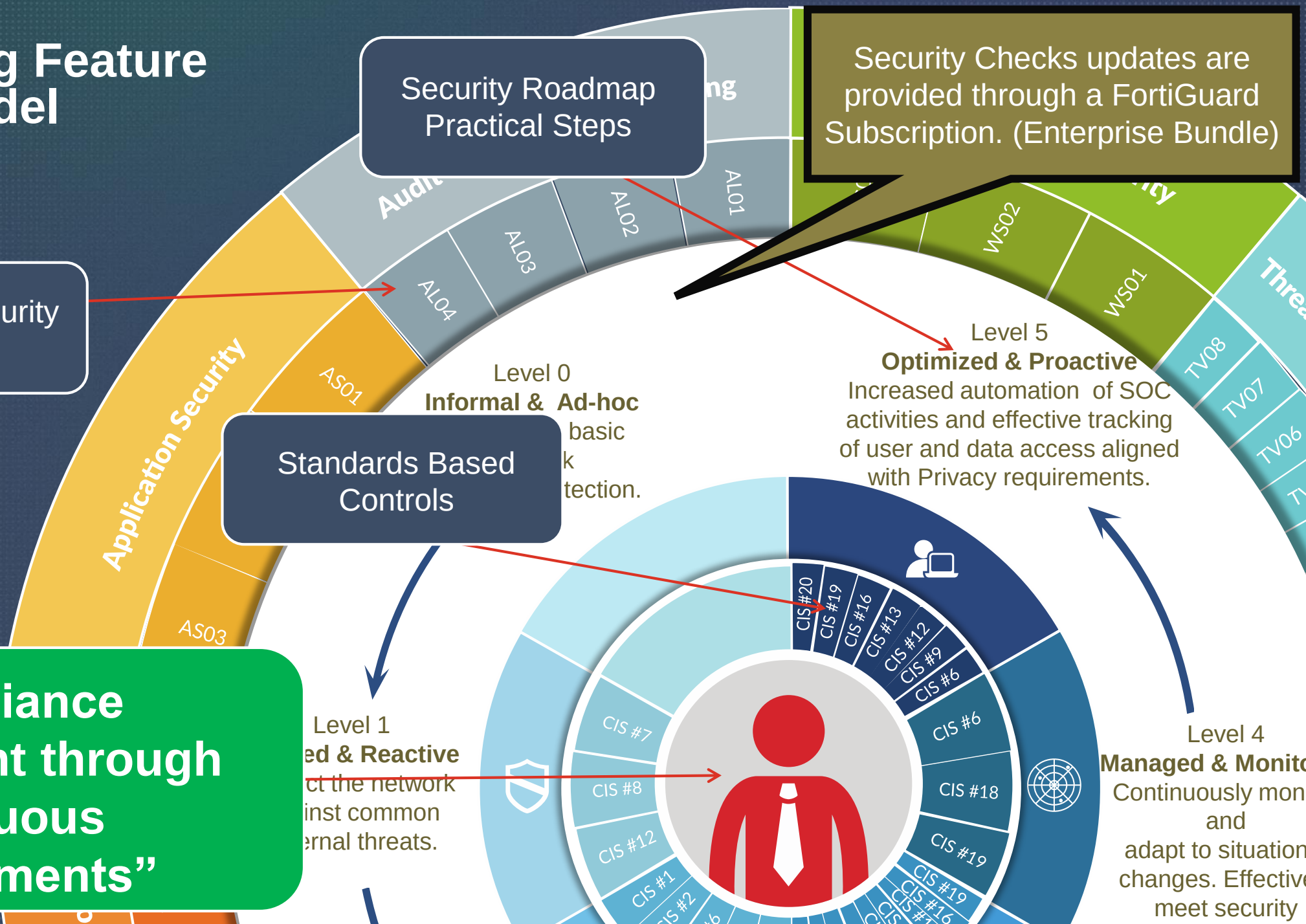
FORTINET

Technical Security Checks

Security Roadmap Practical Steps

Security Checks updates are provided through a FortiGuard Subscription. (Enterprise Bundle)

Standards Based Controls



Level 0
Informal & Ad-hoc
basic
k
tection.

Level 1
ed & Reactive
ct the network
inst common
ernal threats.

Level 5
Optimized & Proactive
Increased automation of SOC activities and effective tracking of user and data access aligned with Privacy requirements.

Level 4
Managed & Monito
Continuously mon
and
adapt to situation
changes. Effective
meet security

"Compliance management through continuous measurements"

ENTERPRISE CORE – SECURITY RATING - DETAILS

FortiGate VM64-KVM Enterprise_Core | Interim build21439 | Security Fabric Demo | admin

- Dashboard
- Security Fabric
  - Physical Topology
  - Logical Topology
  - Security Rating
  - Automation
  - Settings
  - Fabric Connectors
- FortiView
- Network
- System
- Policy & Objects
- Security Profiles
- VPN
- User & Device
- WiFi & Switch Controller
- Log & Report
- Monitor

Security Rating

1 View Results | 2 Easy Apply | All FortiGates | Failed 15 | All Results 48 | Print | Run Now | Scheduled Run

Security Rating: 95th Percentile Security Rating Score: +305

Rated Against All Regions and All Industries in SMB (1 - 256 endpoints)

Ran: 7 minute(s) and 48 second(s) ago Version: 1.00009

33 Passed 10 Medium 5 High

Show Topology

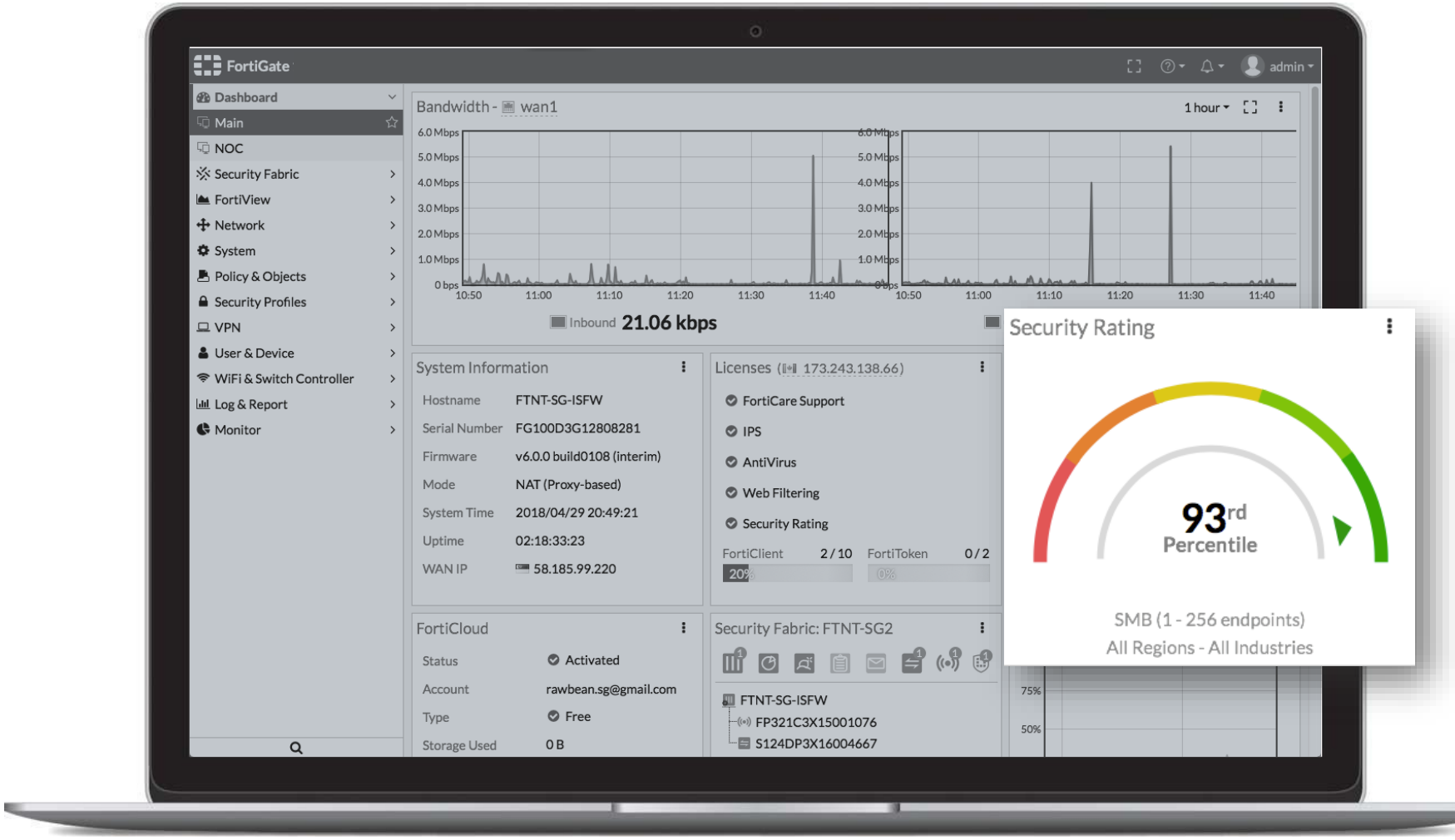
Security Control	FortiGate	Result	Recommendation
Fabric Security Hardening (SH) 4 7			
Unsecure Protocol - HTTP Interfaces should not allow HTTP administrative access. FSBP SH01.2	Enterprise_Core	-120	Disable HTTP access on the following interfaces: Internet Access (port1) DMZ Segment (port2) ISFW (port3) Management (port4) Easy Apply
Trusted Hosts For each administrator, login access should be restricted to trusted hosts. FSBP SH01.3	Enterprise_Core	-20	For each administrator, restrict login access by configuring a trusted host.
Default Port HTTPS HTTPS should not use the default port. FSBP SH01.8	Enterprise_Core	-30	Assign HTTPS a non default port.
Default Port SSH SSH should not use the default port. FSBP SH01.10	Enterprise_Core	-30	Assign SSH a non default port.
Valid HTTPS Certificate - Administrative GUI	Enterprise_Core		Configure a valid certificate. The current certificate "self-sign" does not meet the following requirements:

Easy Apply >

COMPLIANCE & SECURITY RATING

SECURITY RATING RANKING

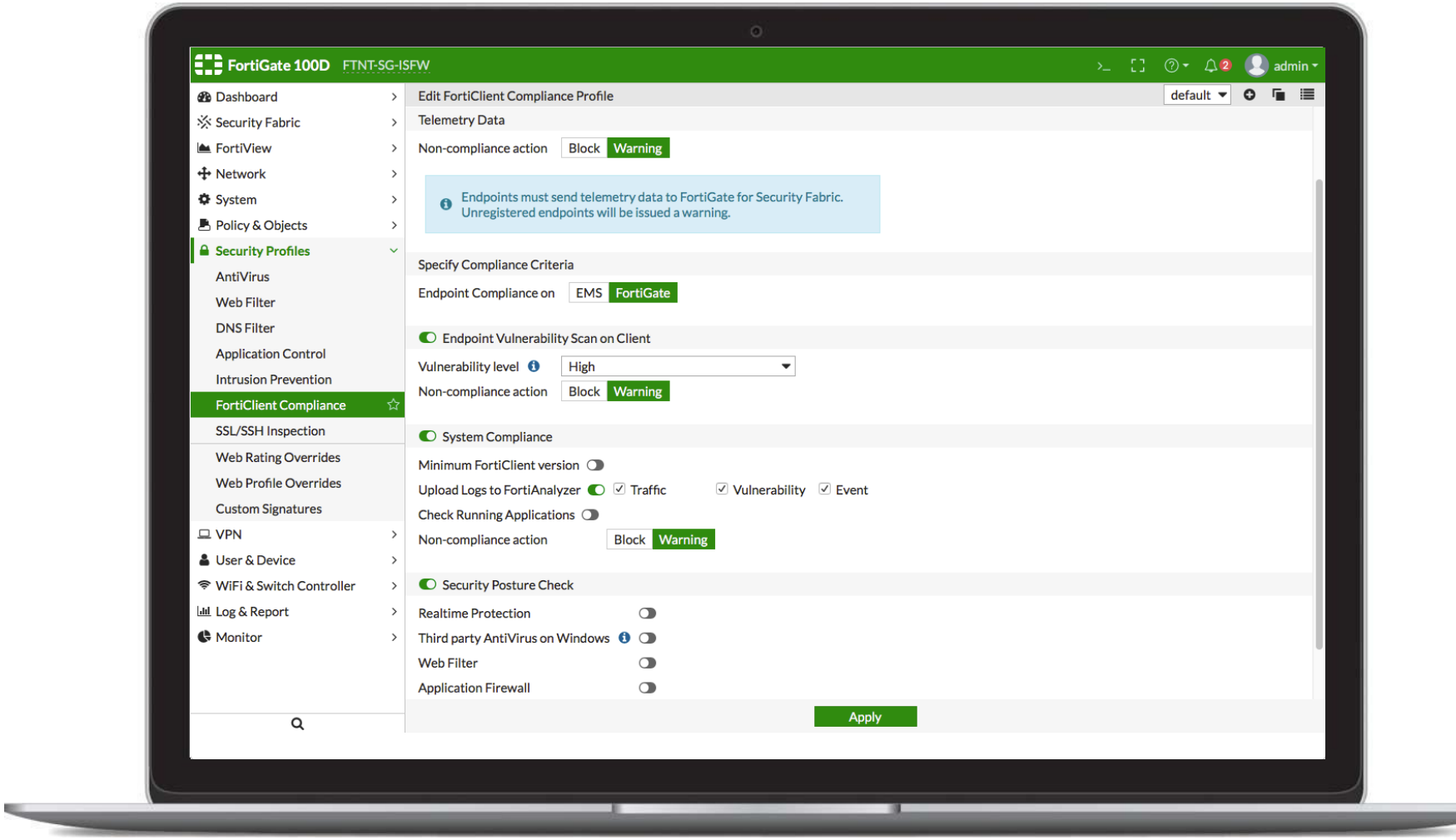
- Benchmark against peers
  - » Rank against similar organizations in term of size and industry by percentile
  - » Requires FortiGuard Security Rating subscription



COMPLIANCE & SECURITY RATING

ENDPOINT COMPLIANCE

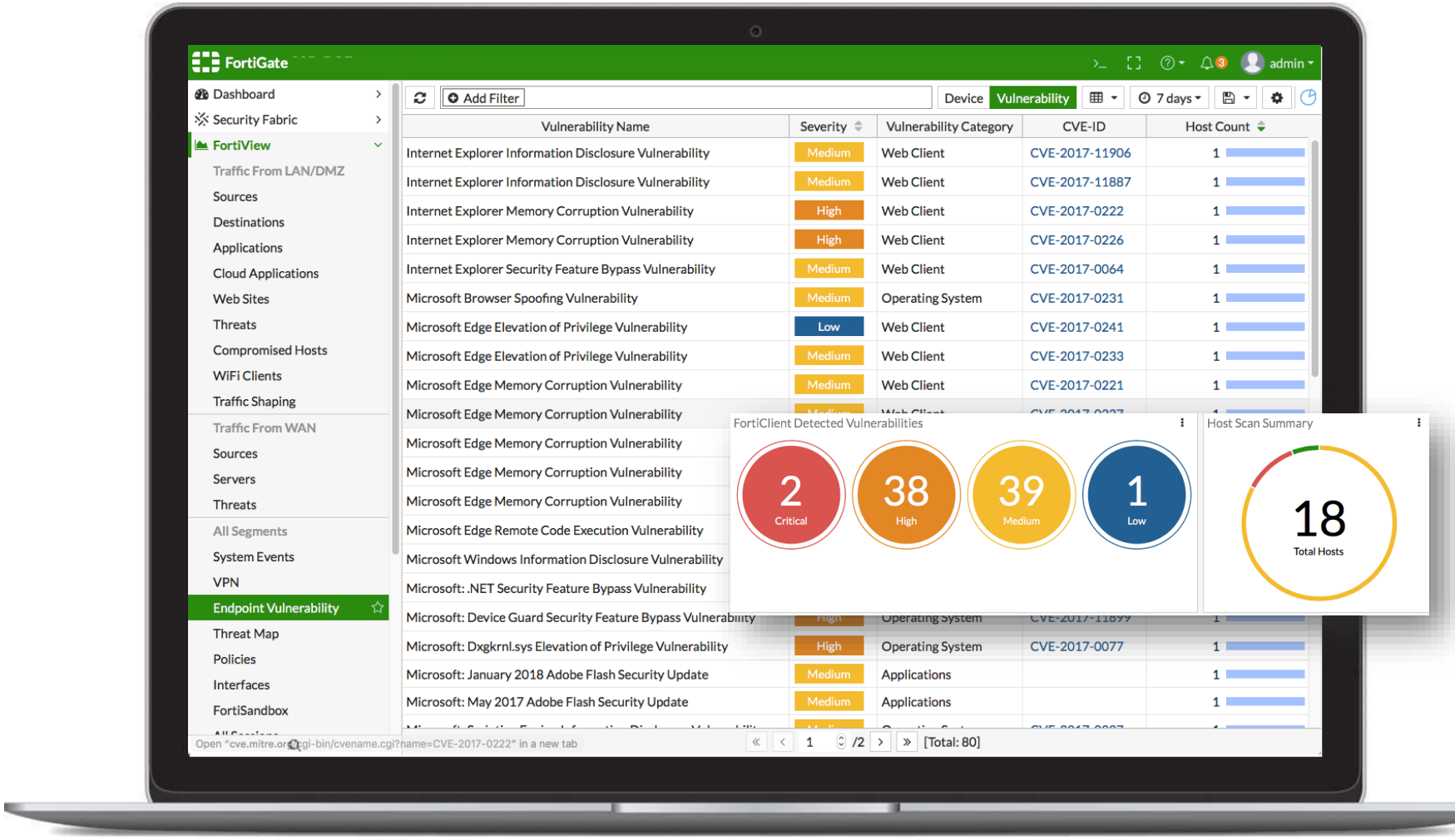
- Different profiles can be setup accordingly such as Location (Source IPs), User groups and/or Device types etc
- Compliance criteria includes Vulnerability scan status, Windows application/process presence and FortiClient configurations
- Warn or block clients if not compliant



VULNERABILITY ASSESSMENT

VISIBILITY

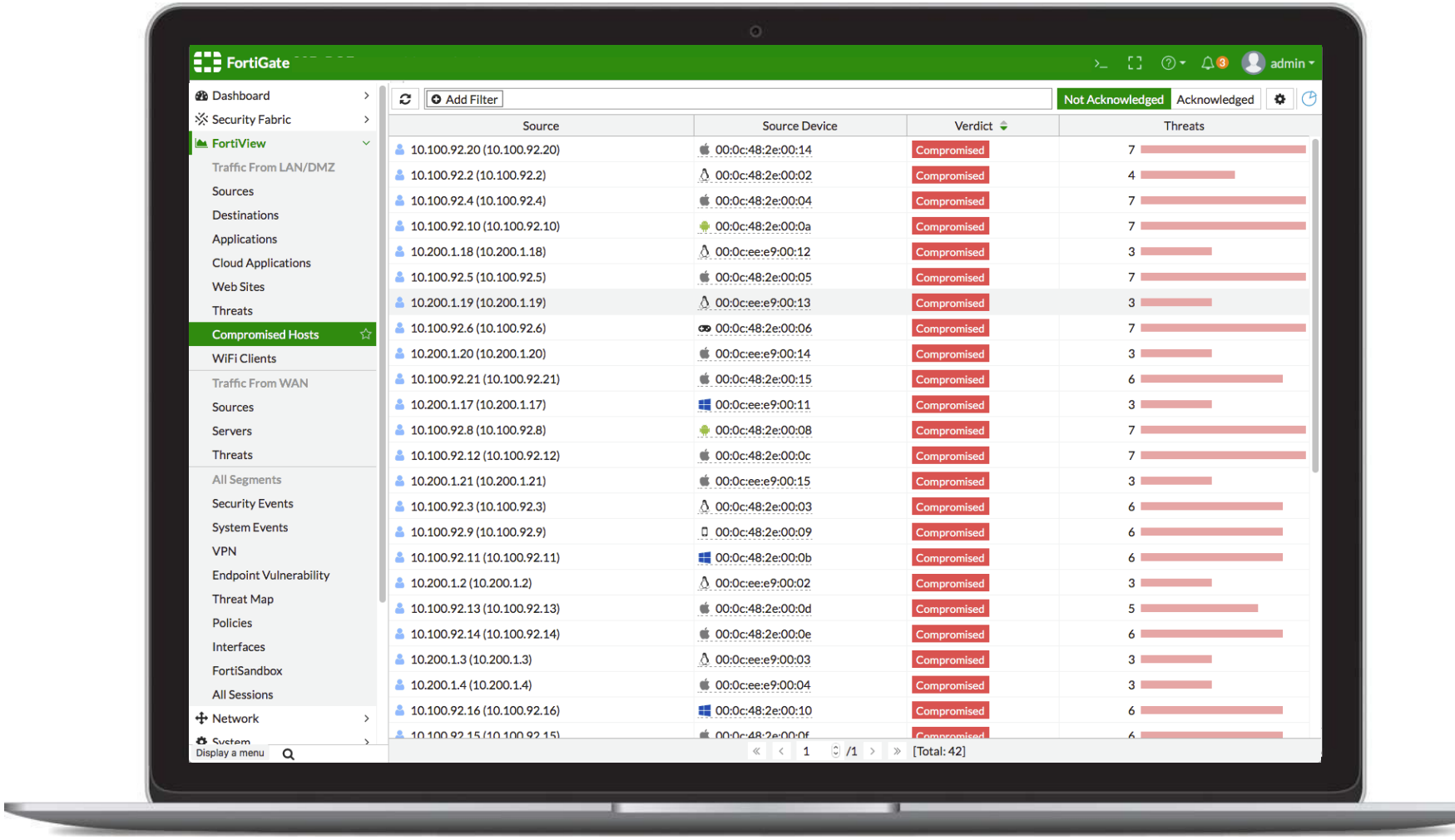
- Endpoints vulnerability assessment results are visible on FortiView and Topology maps
  - » Supports drill-in for details
- Via FortiClient telemetry with FortiGate



IOC DETECTION

VISIBILITY

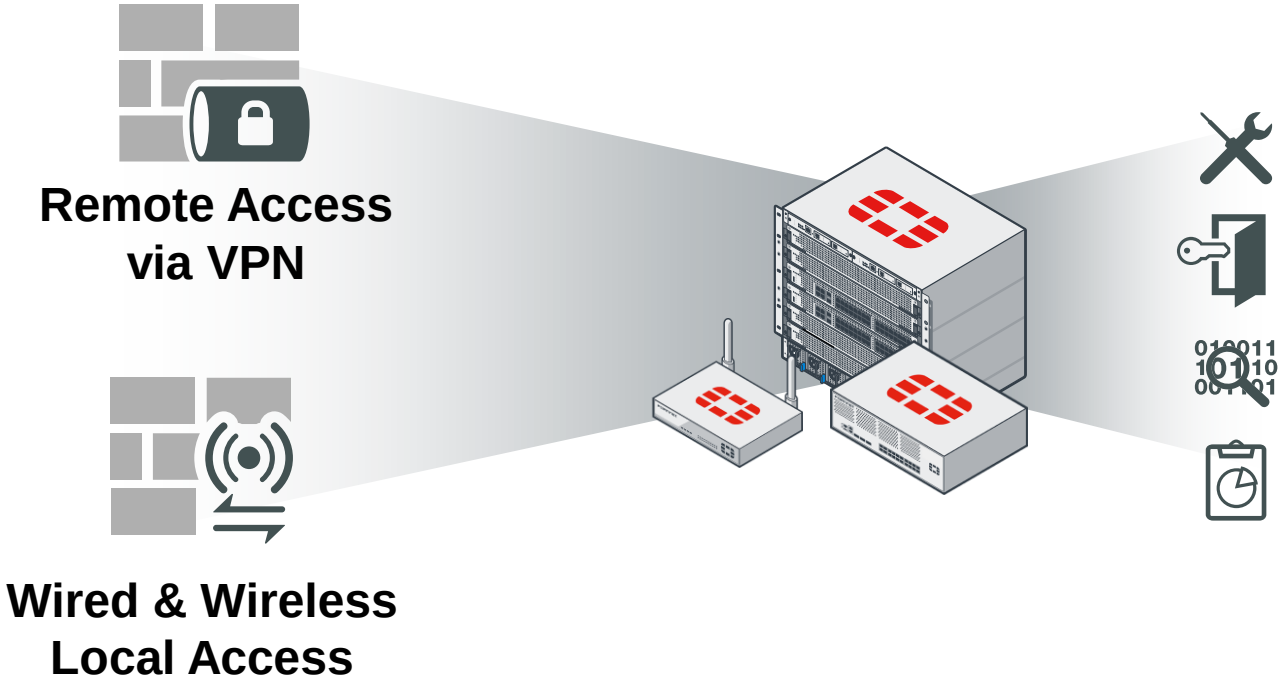
- Compromised terminals as determined by FortiAnalyzer IOC detection are visible on FortiView and Topology maps
  - » Supports drill-in for details
  - » Actionable



SECURITY FABRIC: NETWORKING

Wireless Controller | Switch Controller | WAN Interface Manager

UNIFIED SECURE ACCESS



Shared Services

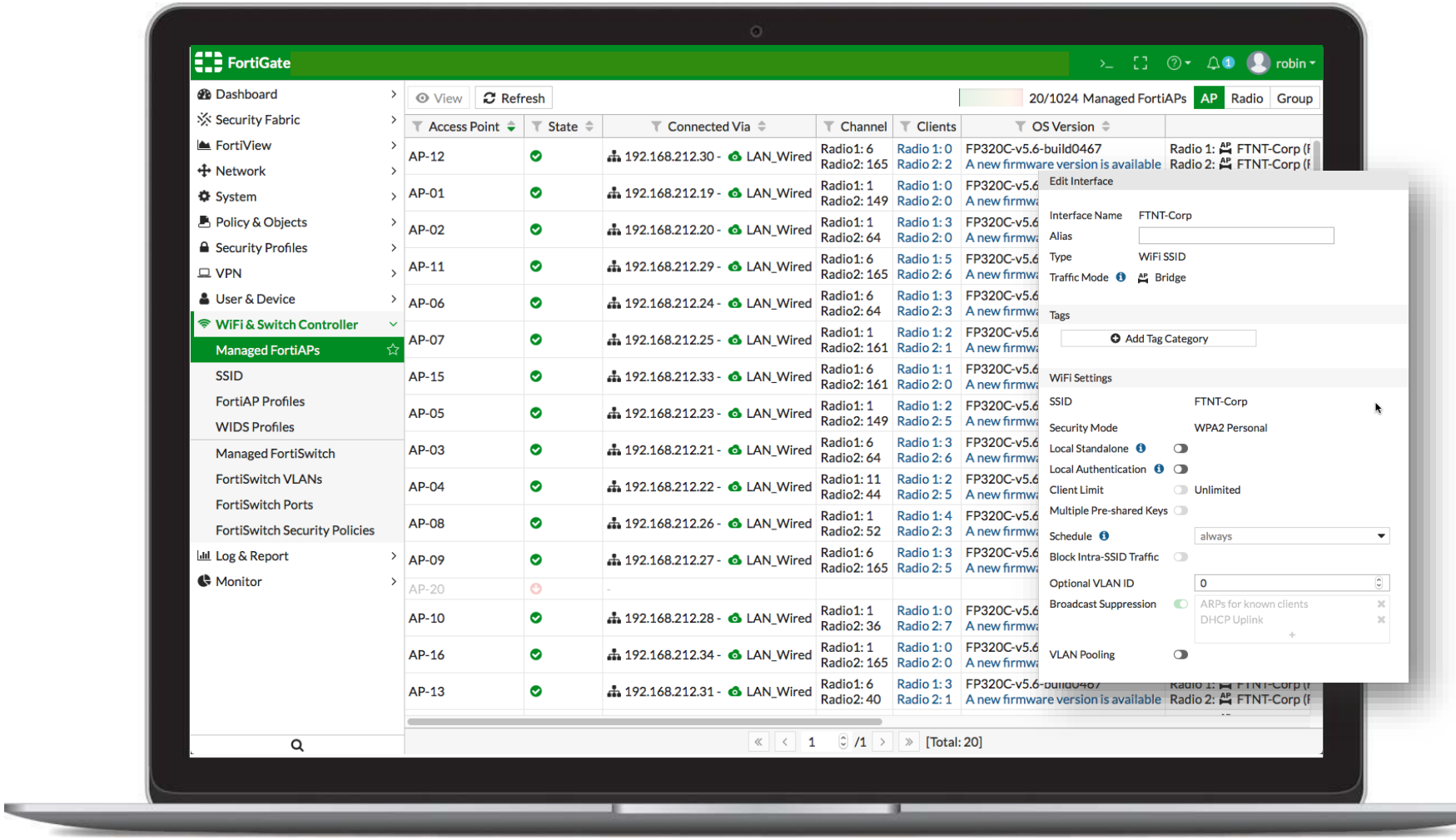
- Configuration
- User/Device Identification and Control
- Content Inspection and Protection
- Visibility
- Logs & Reports

Integrated Connectivity Management with Security

WIRELESS CONTROLLER

AP MANAGEMENT

- Discover and (pre)authorize APs easily
- Batch configurations and upgrades on multiple APs through GUI
- Setup firewall policies with optional UTM profiles applied to SSIDs (wireless networks)



WIRELESS CONTROLLER

DYNAMIC USER VLAN ASSIGNMENT

- A VLAN pool can assign a specific VLAN based on the AP's FortiAP Group, usually for network configuration reasons, or
- assign one of several available VLANs for network load balancing purposes (tunnel mode SSIDs only)

CLIENT LIMIT

- Setting to limit the number of clients permitted to connect simultaneously
- Prevent congestion so to ensure reasonable user experience

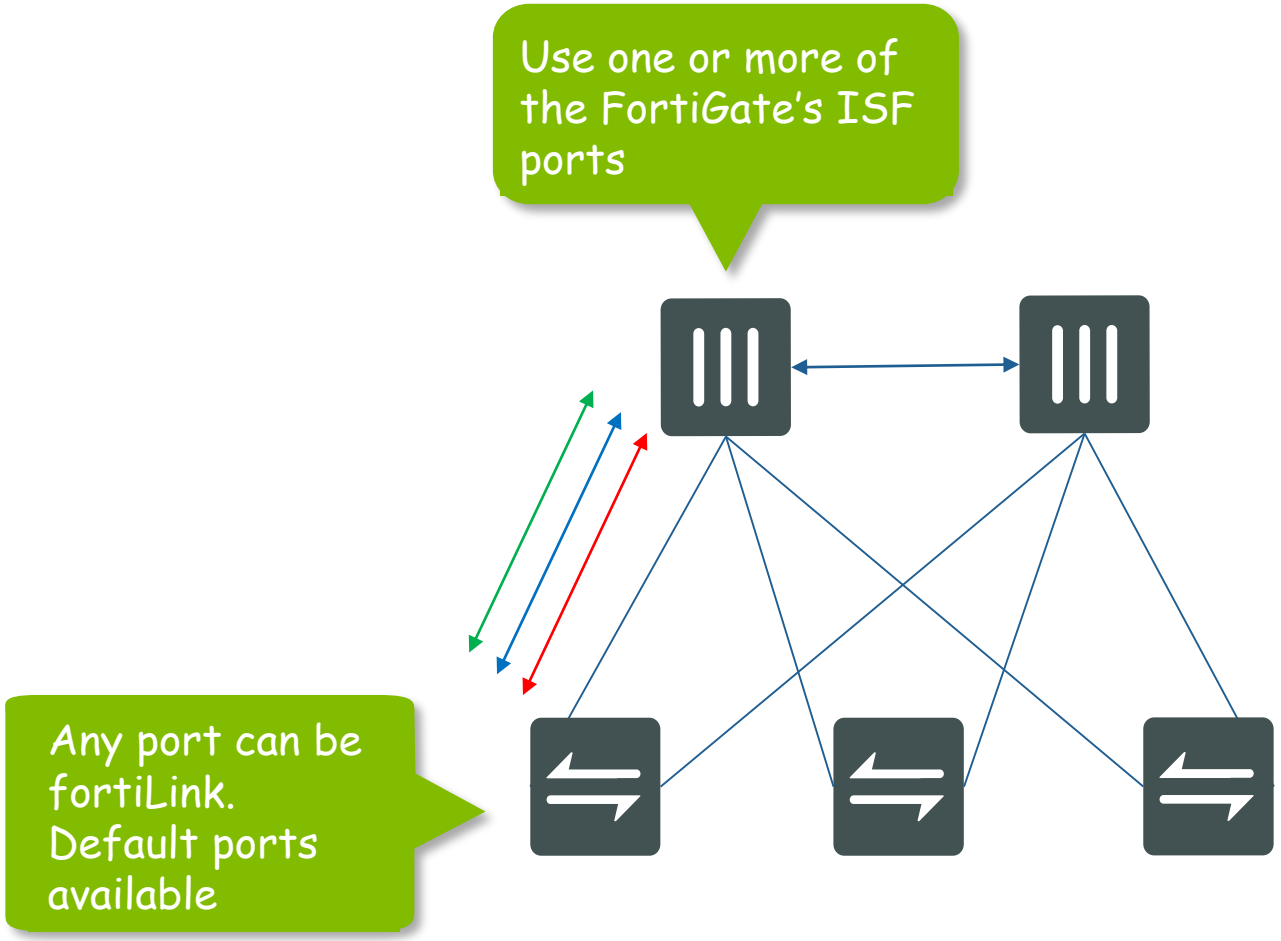
BROADCAST SUPPRESSION

- Some broadcast packets are unnecessary yet consuming valuable air time
- Admin can configure type of broadcast traffic to be suppressed,

SWITCH CONTROLLER

FORTILINK

- Management Only Protocol
- FortiLink overhead is <1%.
- Data does not use CAPWAP, can be accelerated by SPU

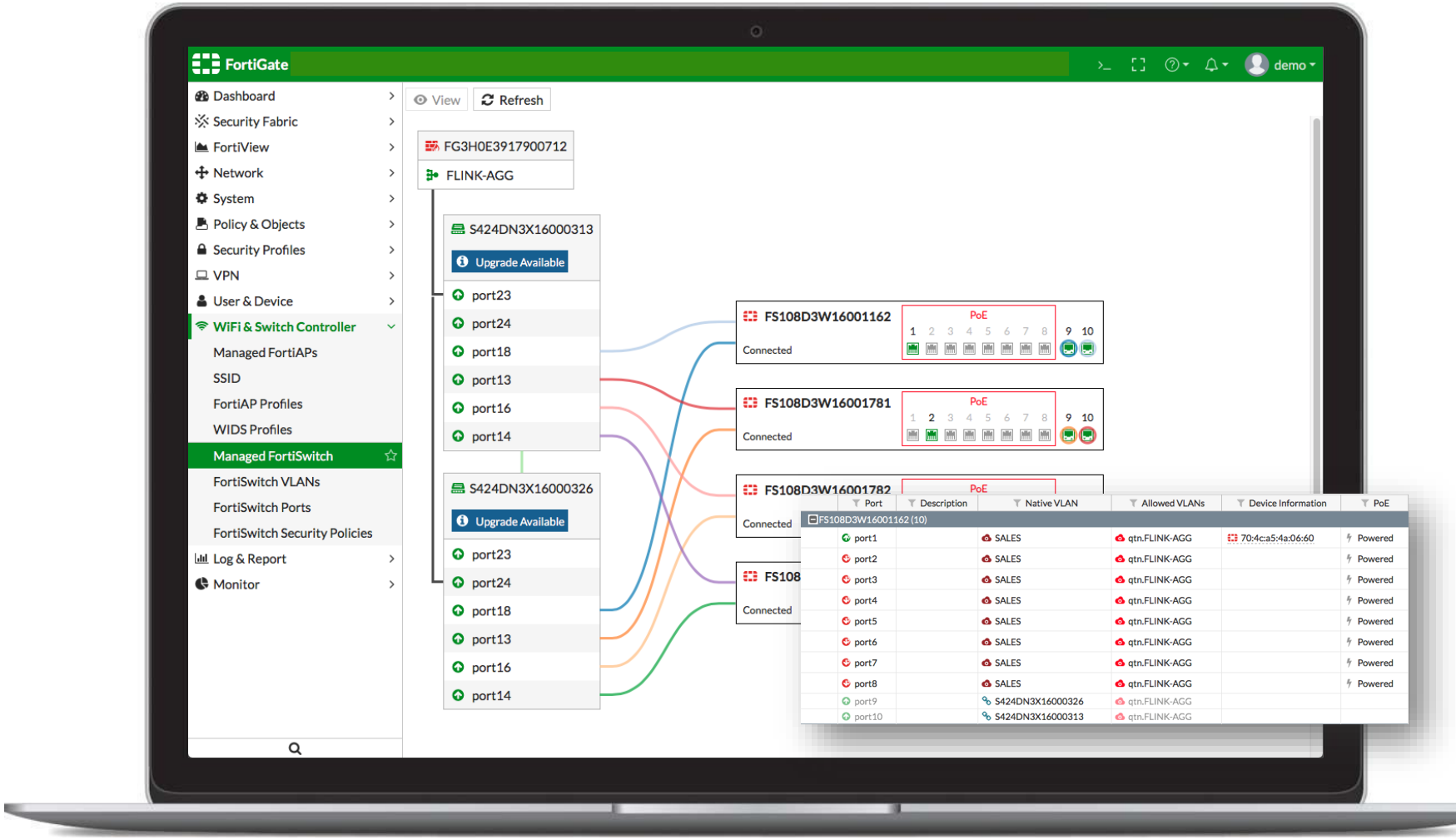


--- FortiLink heartbeat
--- CAPWAP command packets
--- 802.1Q user data

SWITCH CONTROLLER

INTEGRATED SWITCH MANAGEMENT

- Easily connects switches to FortiGate via FortiLink
- Setup stacks, configure and upgrade switches firmware with FortiOS
- Port level visibility – what is connected, plus contextual info on topology map and Device Inventory



SWITCH CONTROLLER

FORTILINK STACKING

- Manage multiple switches from single (or A-P HA) FortiGate
- Connect from 1 to 256 switches in a single stack, depending on FortiGate models
- Switches form ISL (inter-swtch links) automatically
- Supports various topologies, including MCLAC 2 tier switching and daisy-chain

ENTERPRISE-CLASS SWITCHING

- Configure various switching setup and port settings from FortiGate GUI console, including STP, link aggregation and storm control

ACCESS CONTROL

- Support port-based and MAC-based 802.1x
- MAC authentication bypass and Open-Auth. mode

SECURITY FABRIC: CONNECTORS

SDN | CLOUD | IAAS | AUTOMATION | THREAT FEEDS | SSO

TYPES OF PARTNER INTEGRATIONS

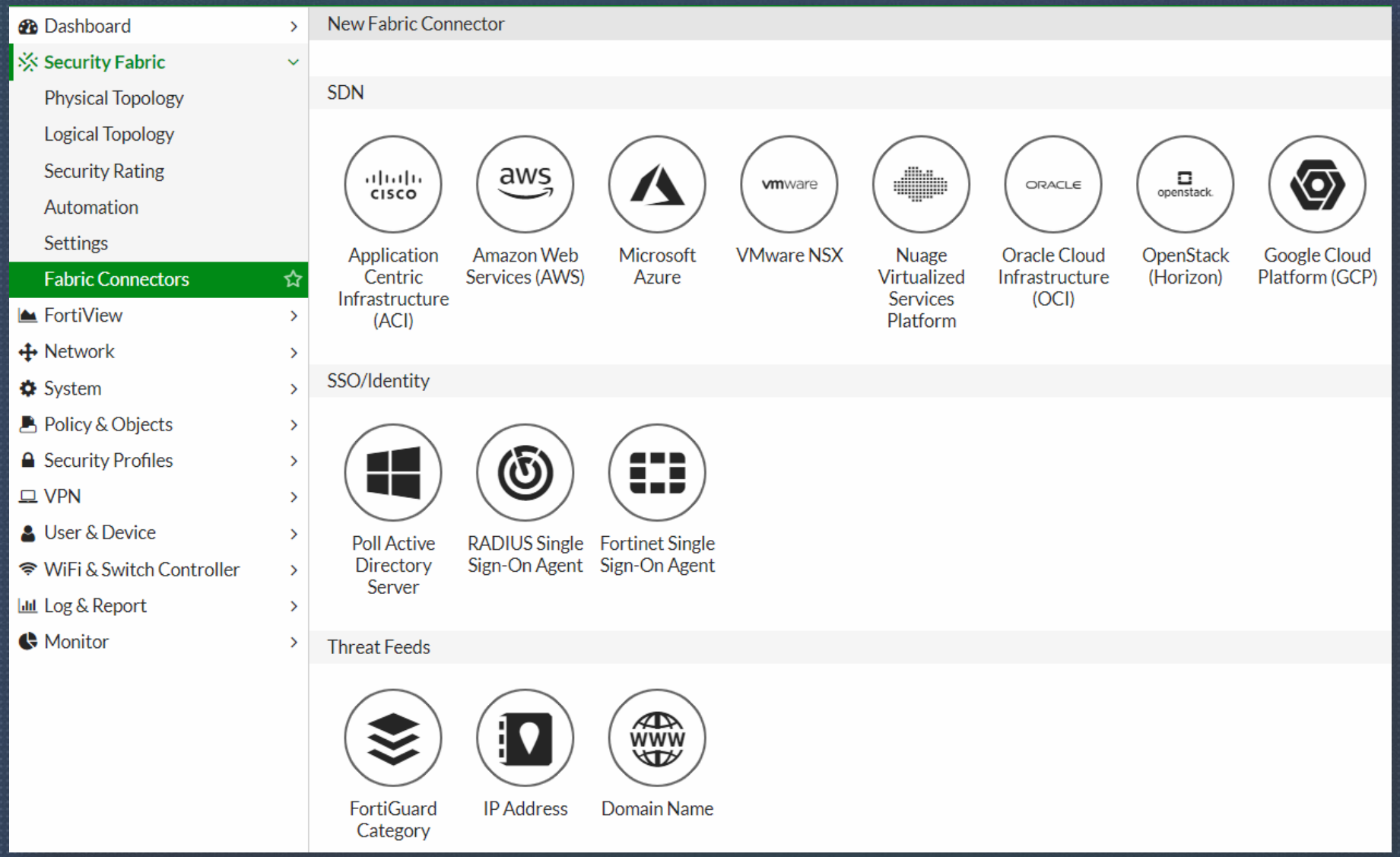
Fabric-Ready

- Partner developed solutions to integrate with FTNT products
- Based on existing APIs and/or standard protocols(RADIUS, SYSLOG, SSH, etc)
- (usually) no specific code development from FTNT side
- FTNT tests solution to assure it works as expected

Fabric Connectors

- Fortinet develops specific code in our products
- Explicitly referenced in our GUI/CLI
- Mainly based on APIs
- Feature development made by FTNT
- Validation might require testing with the partner

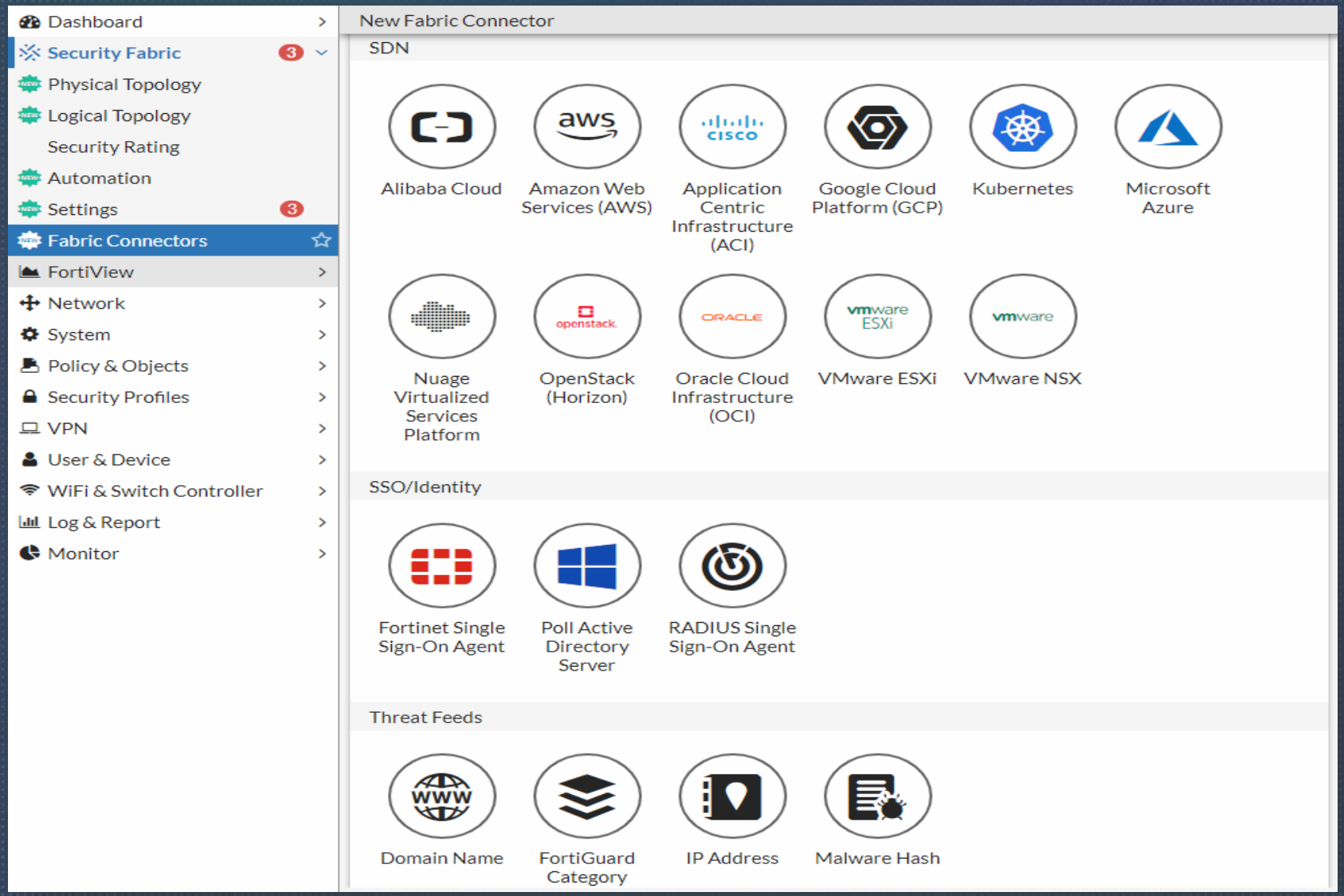
FOS 6.0.3 FABRIC CONNECTORS



FORTINET

FOS 6.2B.3 FABRIC CONNECTORS

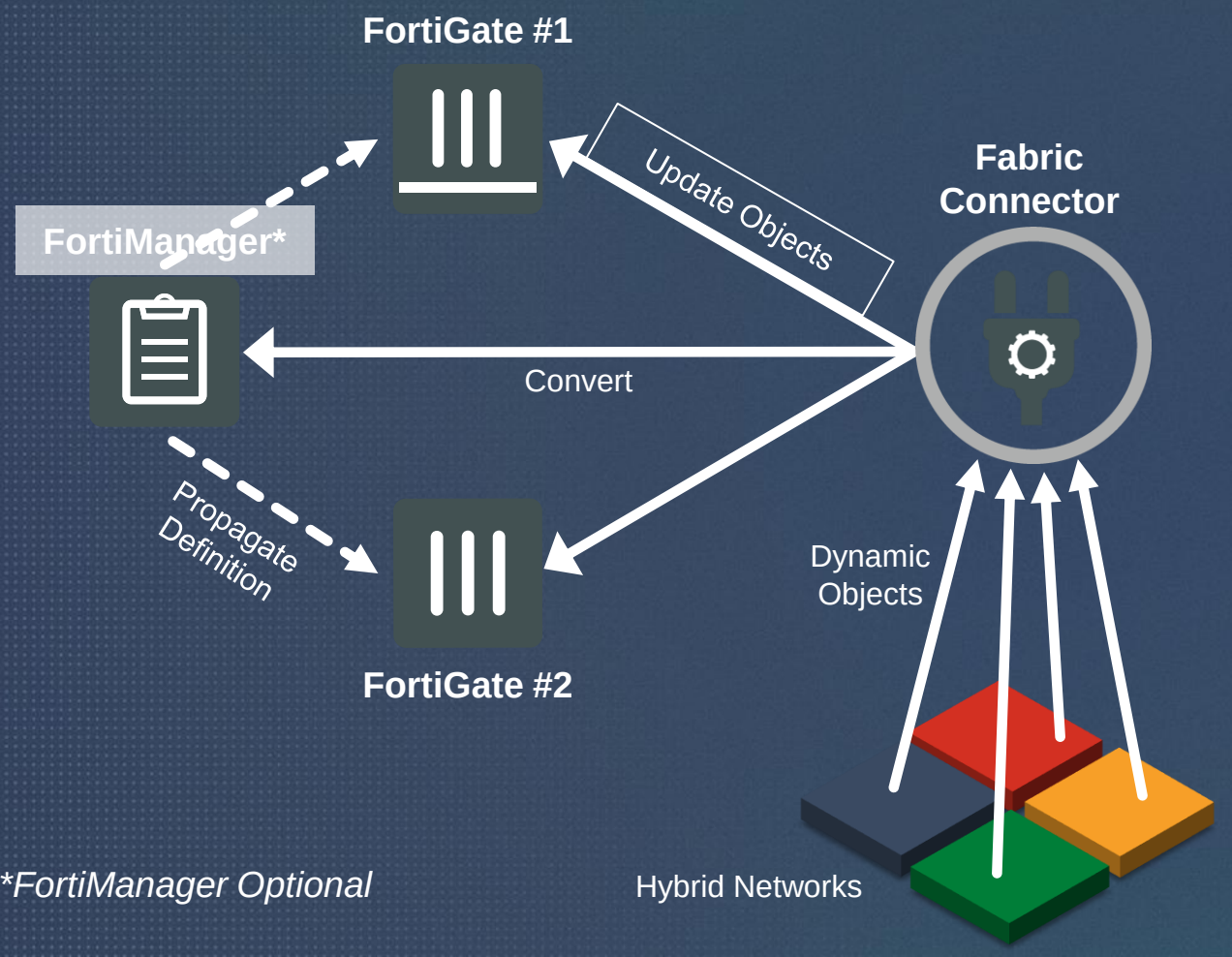
roadmap



FORTINET

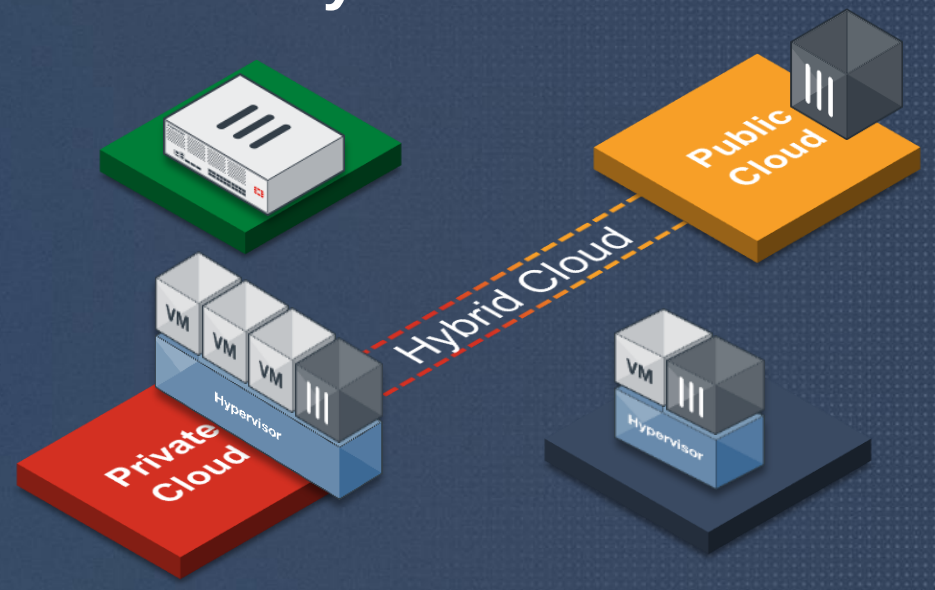
FABRIC CONNECTOR IN ACTION | AUTOMATIC SYNCHRONIZATION

No manual updates necessary



**FortiManager Optional*

Hybrid Cloud



FORTINET

FORTINET FABRIC-READY TECHNOLOGY ALLIANCE PARTNERSHIPS

FORTINET Fabric-Ready

SDN/NFV & VIRTUALIZATION

ADVA Optical Networking, BROCADE, cisco, CLOUDIFY, intel, NEC, nuagenetworks, silver peak, UBiqube, vmware

CLOUD

aws, Microsoft Azure, IBM Security, Google Cloud Platform, ORACLE, vmware, HPE Helion, ribbon communications, VERISIGN

ENDPOINT

Attivo NETWORKS, CARBON BLACK ARM YOUR ENDPOINTS, McAfee Together is power., Pulse Secure, SentinelOne, Symantec, ziften

MANAGEMENT

algosec, ARISTA, BACKBOX, CSPi, cyber OBSERVER, cyglass, FIREMON, HUGHES An EchoStar Company, IBM Security, MICRO FOCUS, Phantom, Qualys, servicenow, WhiteHat SECURITY, rubrik, tufin, FORTINET

IDENTITY MGMT.

Centrify, CYBERARK

IoT & OT

ForeScout, NOZOMI NETWORKS, CLAROTY Clarity for OT Networks

SIEM

IBM Security, MICRO FOCUS

FORTINET®