Fortinet - Vollintegrierte, leistungsstarke Sicherheit für die gesamte IT-Infrastruktur

Daniel Marquardt & Dimitri Dukarski

klopfer datennetzwerk gmbh – Fortinet Workshop – 15. Mai 2019

Agenda

1. **Ganzheitlicher Security Ansatz mit Fortinet**
   - Kurzüberblick Fortinet
   - FortiGate als Controller für Secure Access
   - FortiNAC für Netzwerke bei denen 802.1x schwierig ist
   - FortiAnalyzer zur Netzwerküberwachung
   - FortiPresence zur WLAN-Standortanalyse
2. **Professionelle WLAN-Lösung mit Fortinet-Controllern und Aps**
   - Ein Praxisbeispiel – Einsatz von Fortinet-Produkten in einer Industrieumgebung

Kurzüberblick Fortinet

Wer steht heute vor Ihnen?

Global

FOUNDED IN 2000
BY KEN XIE

HEADQUARTERED IN SUNNYVALE CALIFORNIA

100+
OFFICES ACROSS THE GLOBE

5,800+
EMPLOYEES WORLDWIDE

IN EXCESS OF
$1.2B

4.4M+

GROWTH
YOY 2018 IN BILLINGS

ISSUED
199 IN PROCESS
PATENTED

Confidential

Wer steht heute vor Ihnen?

Deutschland

PRÄSENT SEIT 2003

4 BÜROS

HEADQUARTER IN FRANKFURT

2015 ERÖFFNUNG DES SUPPORT-CENTERS

90+ MITARBEITER

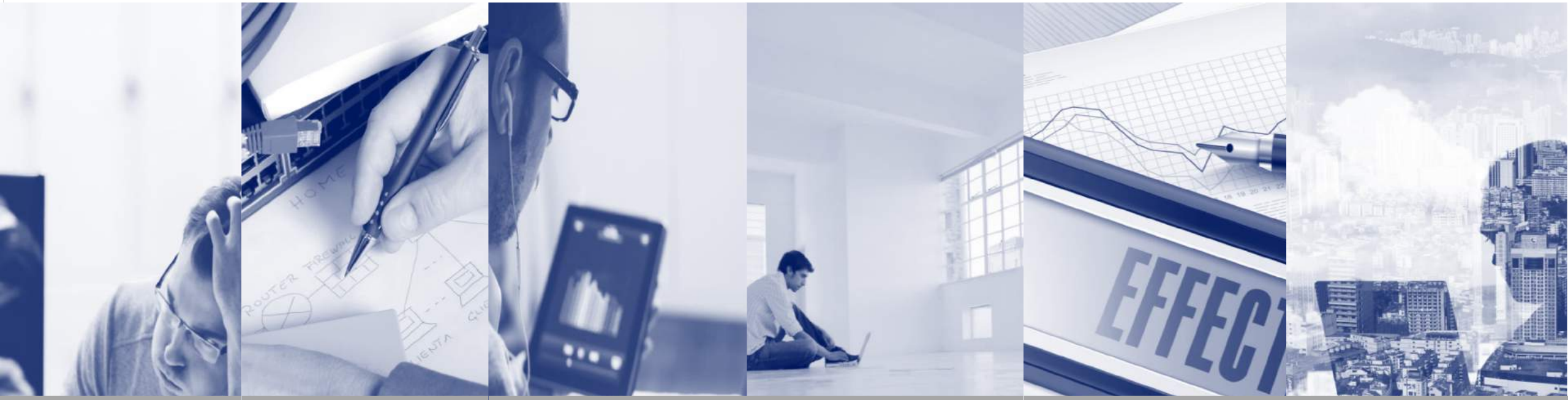
150k

UMSATZ-STEIGERUNG YOY

199 ANGEMELDET

Aktuelle Herausforderungen am Markt

Erkennen Sie sich wider?

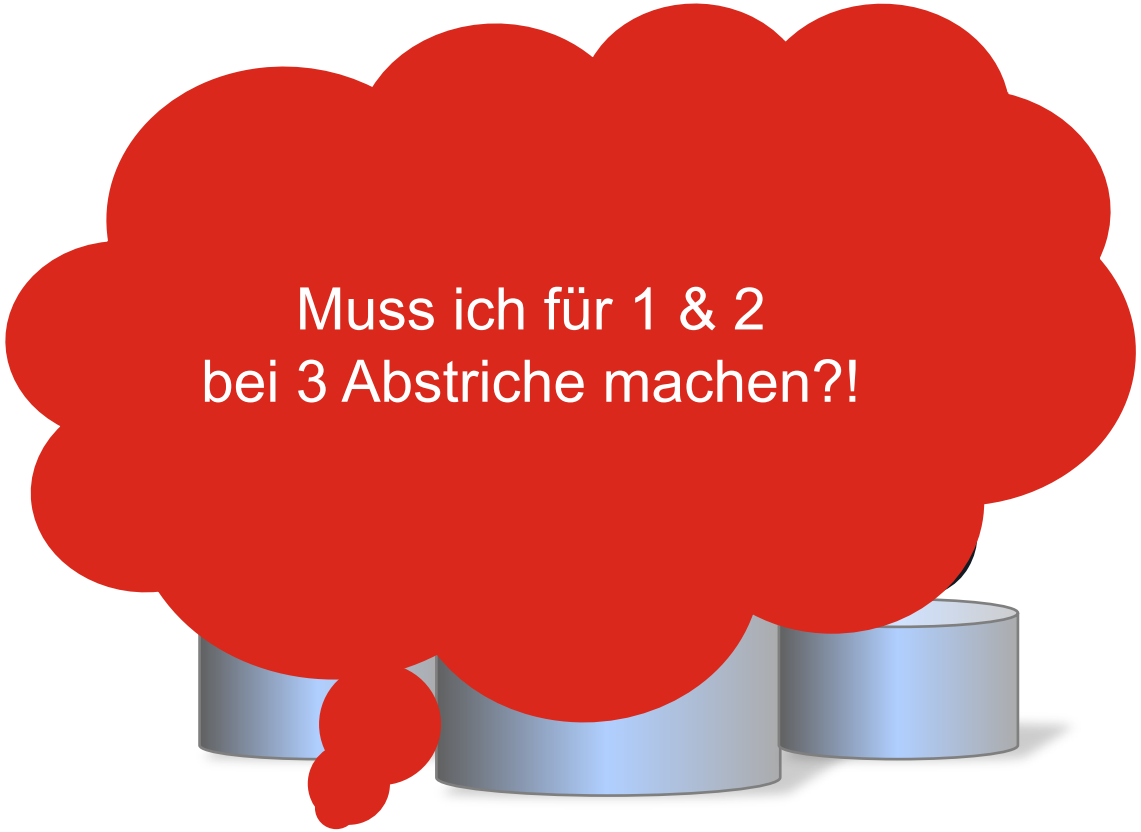


Prio Nr. 1: Wachstum	Begrenzte IT-Ressourcen	Anforderungen: Ständige System-Verfügbarkeit	Von überall und allen Geräten	Einfach, zuverlässig, kostengünstig	Sind Sie ein potentielles Ziel für Hacker?

Was sind Ihre IT-Security-Prioritäten?

Statistisch gesehen...

1. **Bedienkomfort**
2. **Kosteneffizienz**
3. **Security-Effektivität**



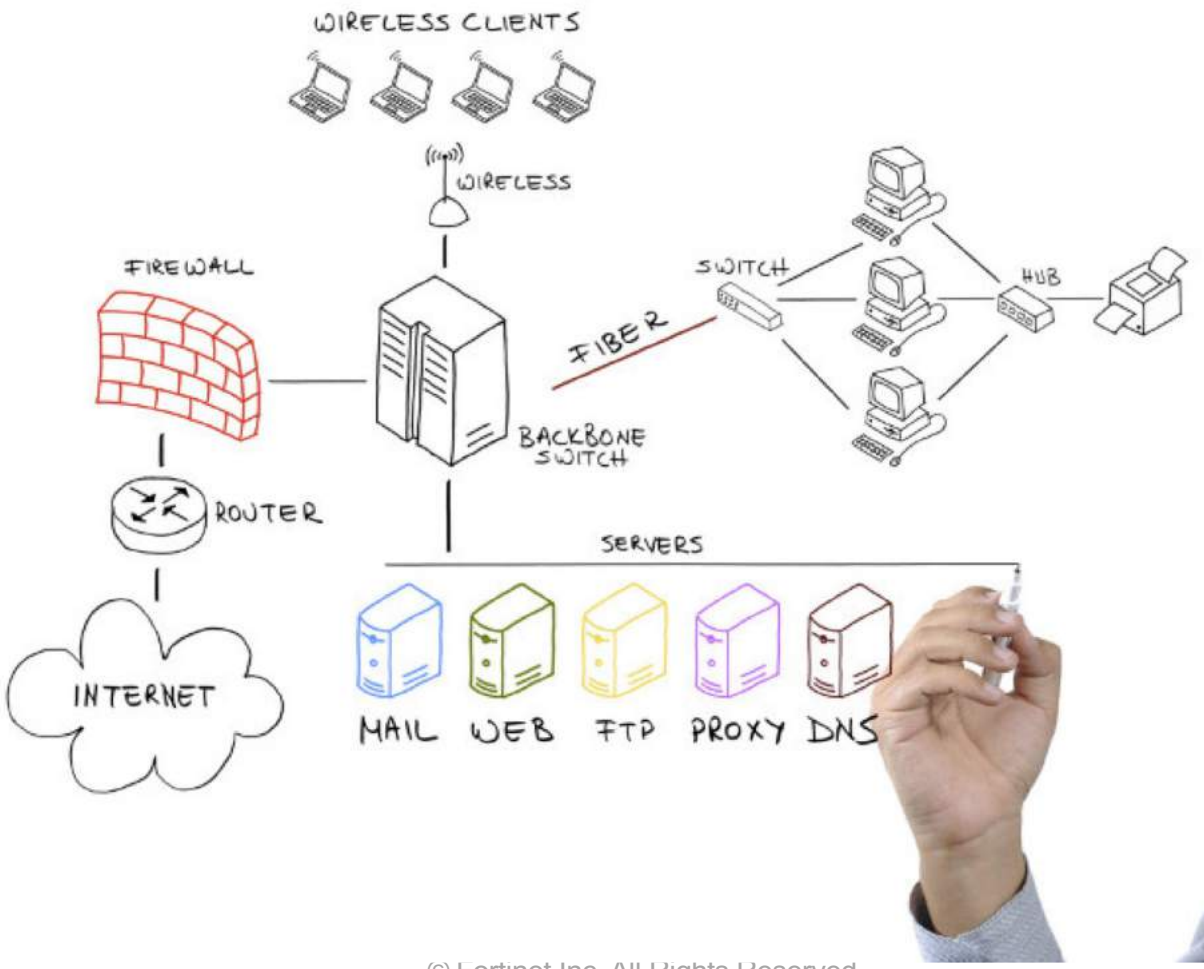
Eine Frage vor ab?

Wieviele IT-Security-Lösungen haben Sie im Einsatz?

𝍸 |||

… und wieviele verschiedene Hersteller?

𝍸

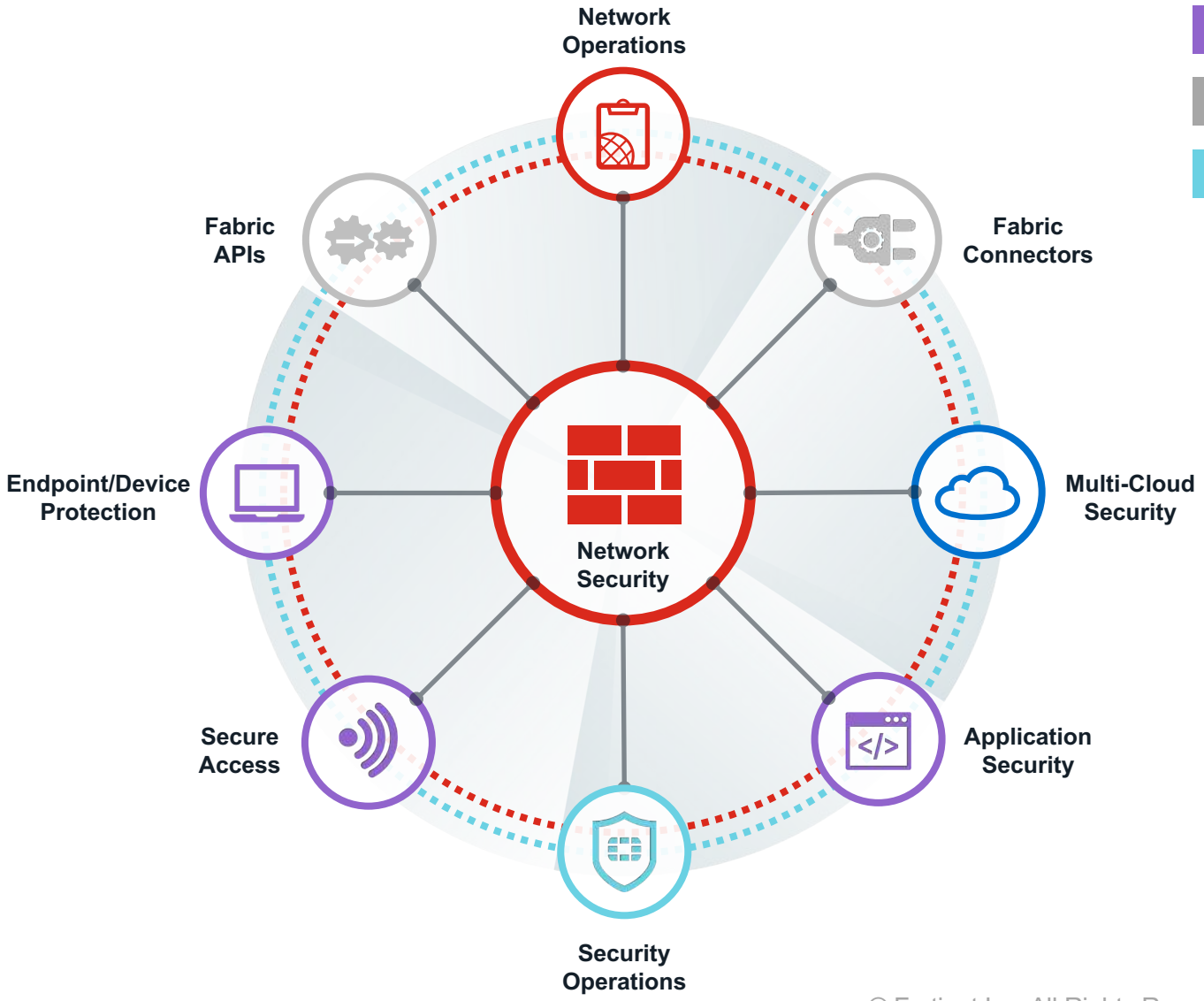


Die Fortinet Security Fabric

BREITE
Sichtbarkeit & Schutz

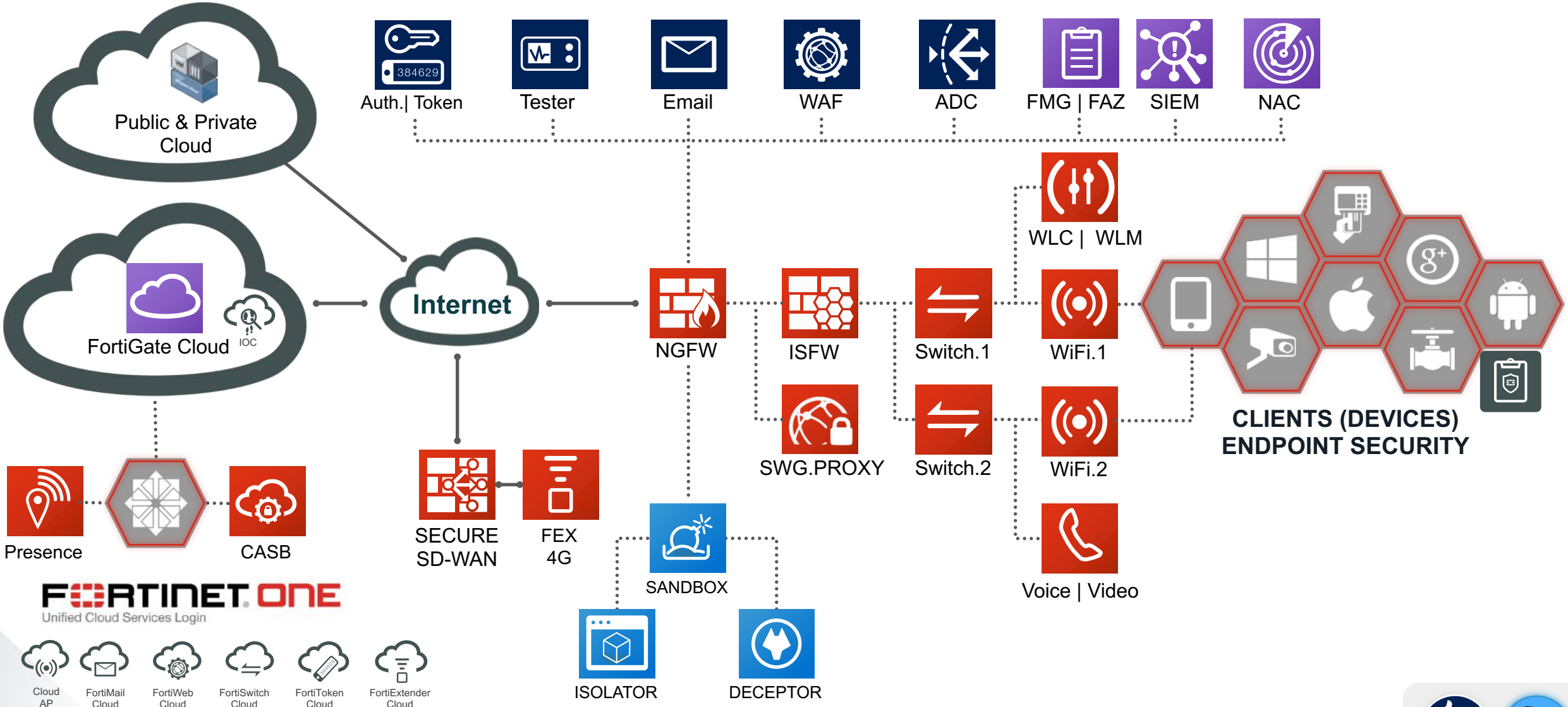
INTEGRIERTE
Erkennung fortgeschrittener Bedrohungen

AUTOMATISIERTE
Reaktionen & fortlaufende Analysen



Network Security
Multi-Cloud Security
Device, Access, and Application Security
Open Ecosystem
Security Operations

Fortinet Produktüberblick



Gartner Quadrant

Figure 1. Magic Quadrant for Unified Threat Management (SMB Multifunction Firewalls)

Source: Gartner (September 2018)

Figure 1. Magic Quadrant for Enterprise Network Firewalls

Source: Gartner (October 2018)

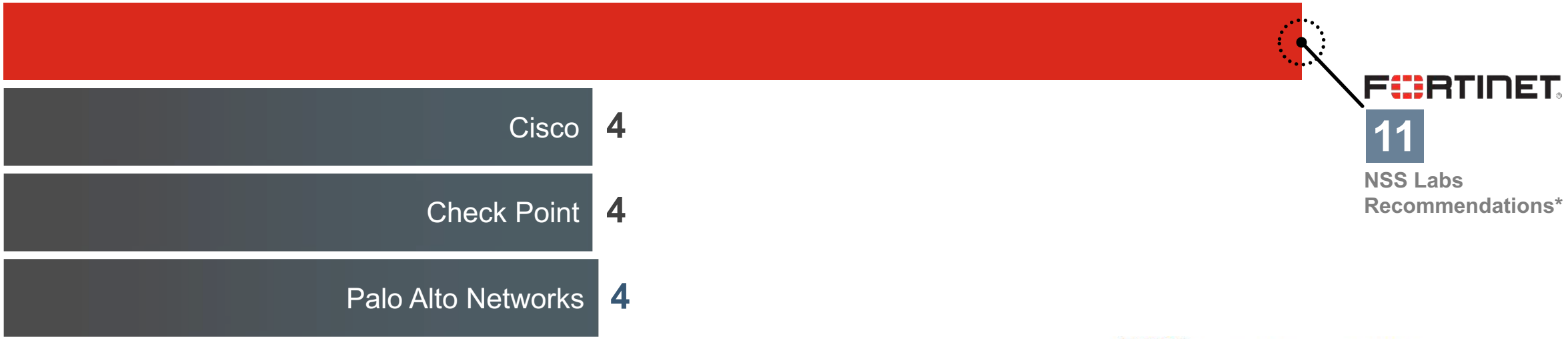
Gartner Magic Quadrant for Enterprise Network Firewalls, Adam Hills, Jeremy D'Hoinne, Rajpreet Kaur, 4 October 2018

Disclaimer: This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from Fortinet. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

FORTINET

Unequalled Third-Party Certifications

#1 Certified Security Vendor Recommended in 8 out of 8 NSS Tests



FORTINET


FORTINET

Fortinet - Vollintegrierte, leistungsstarke Sicherheit für die gesamte IT-Infrastruktur

Daniel Marquardt & Dimitri Dukarski

klopfer datennetzwerk gmbh – Fortinet Workshop – 15. Mai 2019

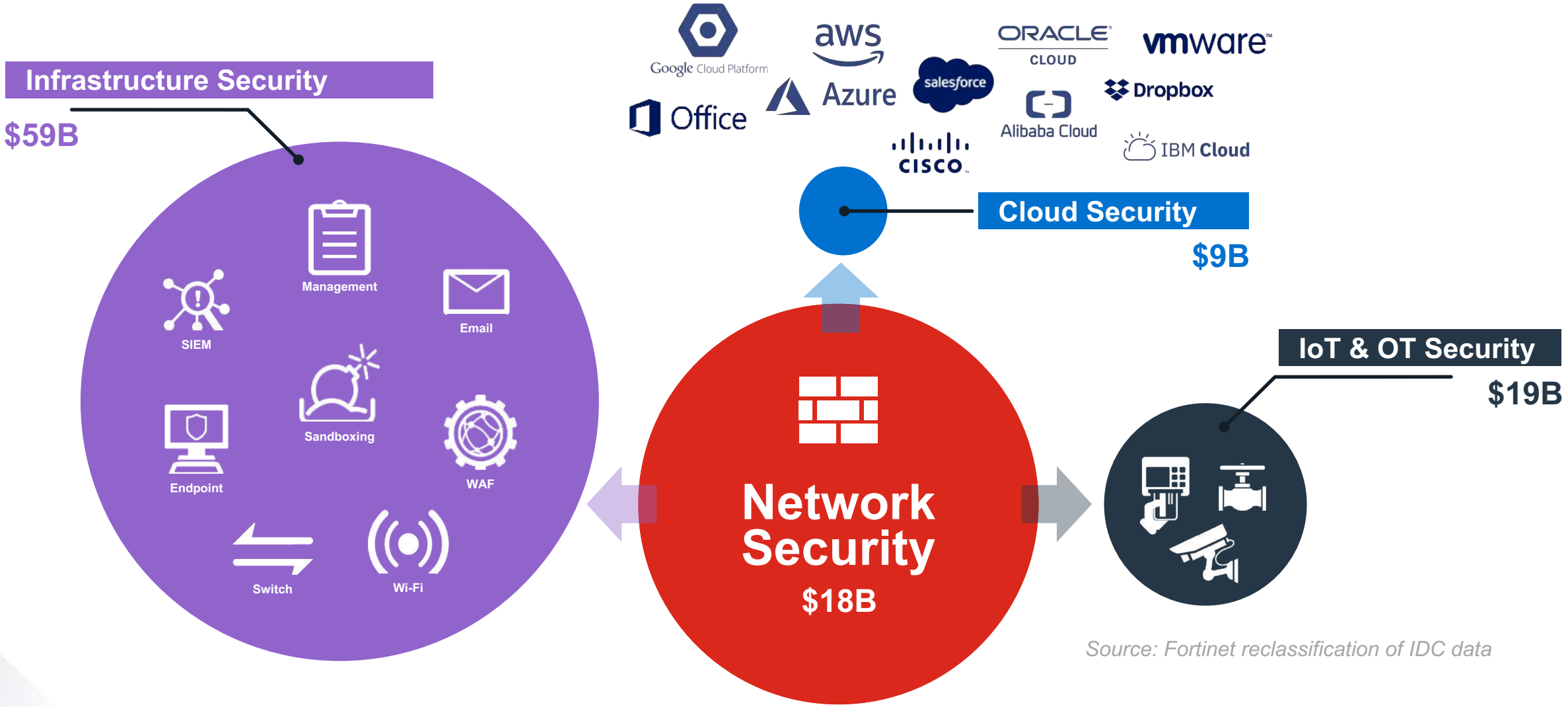
Vorstellung

Daniel Marquardt

Daniel Marquardt
Systems Engineer

E: dmarquardt@fortinet.com
M: +49 172 39 33 440
Feldbergstrasse 35 | 60323 Frankfurt | GER
Home Office Standort Dresden

Fortinet Focus on 4 Security Markets



Source: Fortinet reclassification of IDC data

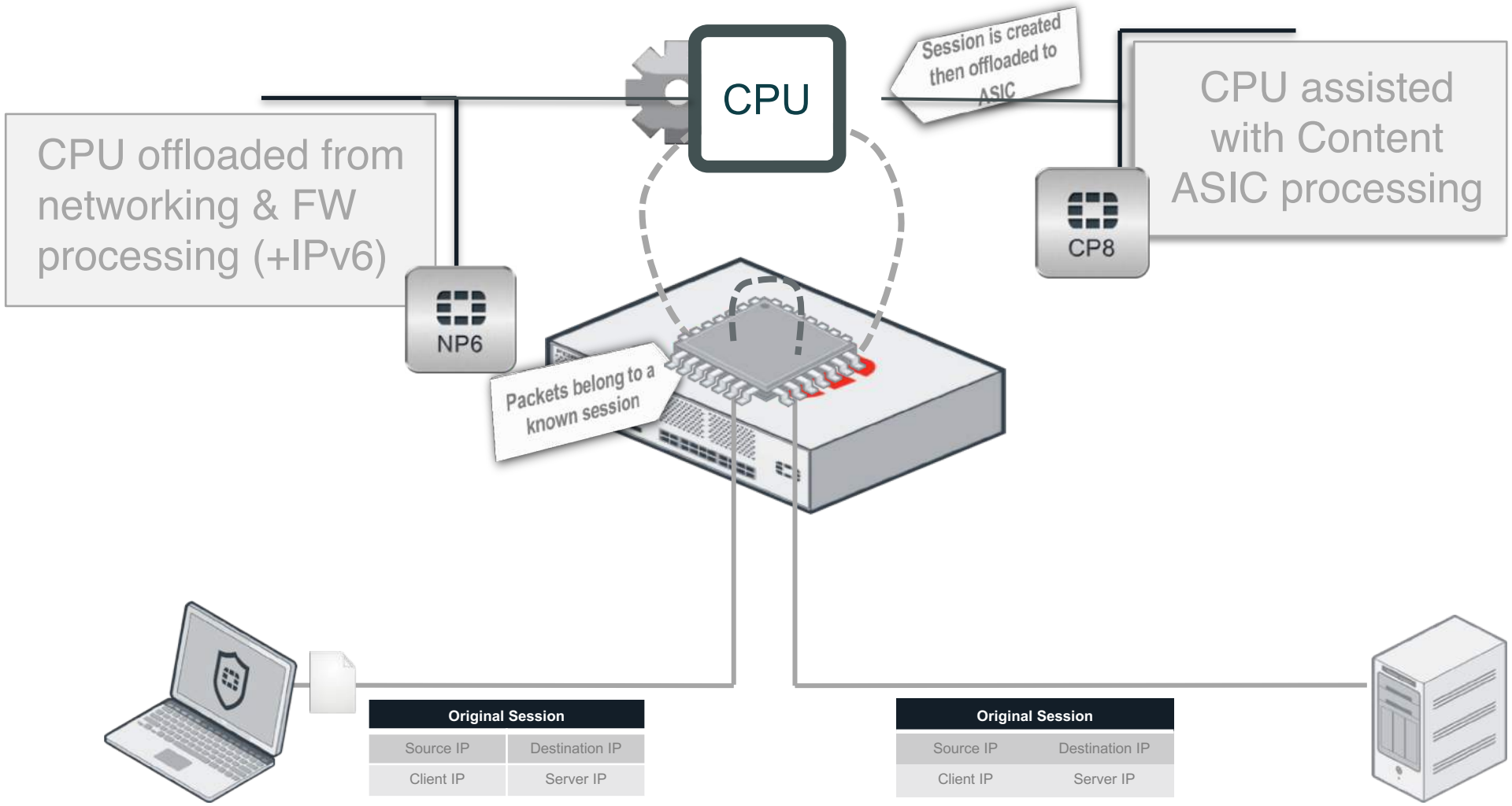
FortiGate als Controller für Secure Access

Firewall at its best

Viele Security-Lösungen sind wie dieses Sandwich….

…deshalb schauen Sie bitte genau hin!

Fortinet Performance



PLATFORM SUPPORT

PHYSICAL APPLIANCE

HARDWARE ACCELERATION

SYSTEM ON-CHIP

- For entry-level FortiGate security appliances
- Simplifies appliance design and enables breakthrough performance without compromising on security

NETWORK PROCESSOR

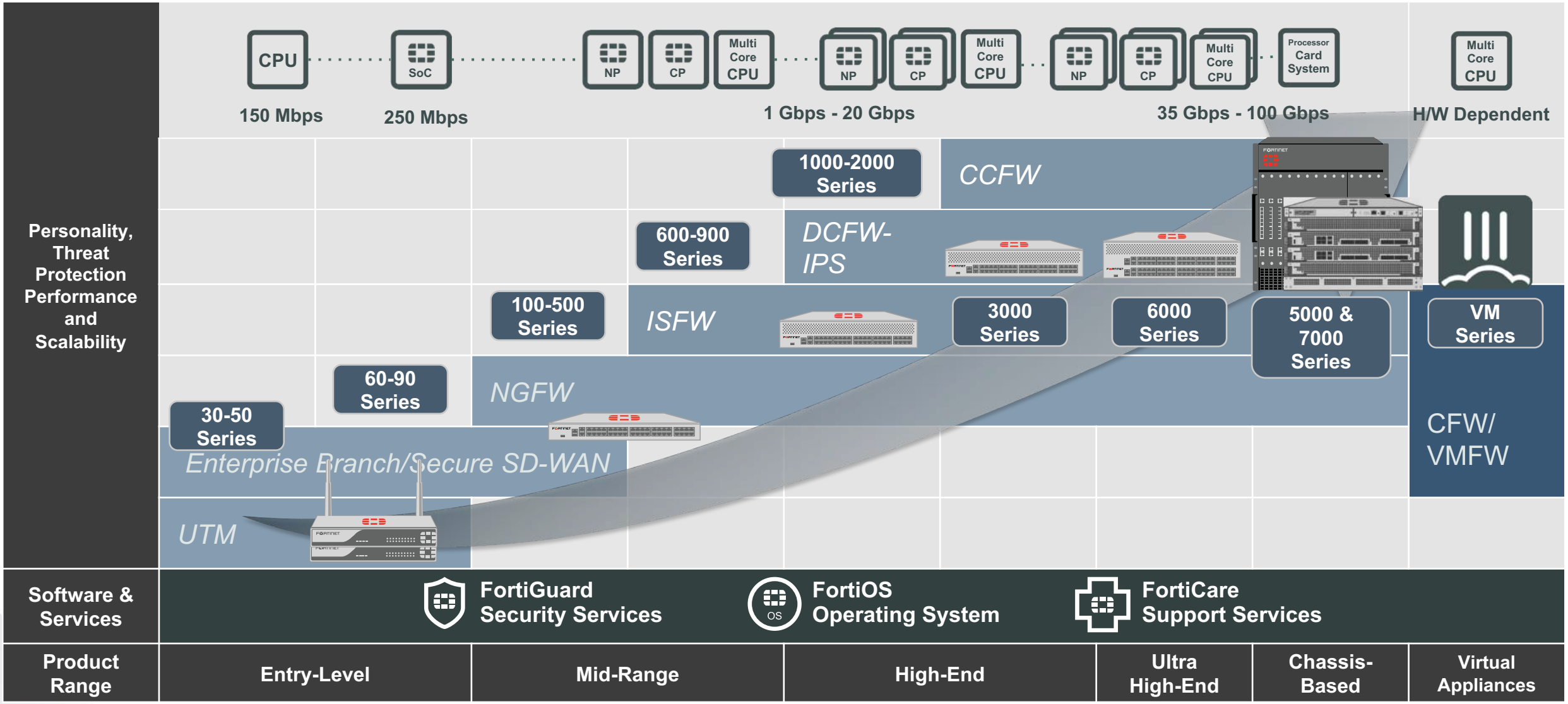
- Works in-line with FortiOS functions to deliver superior firewall performance for IPV4, IPV6, and multicast traffic with ultra-low latency

CONTENT PROCESSOR

- Works outside of the direct flow of traffic
- Provides high-speed cryptography and content inspection services such as signature matching

FORTINET

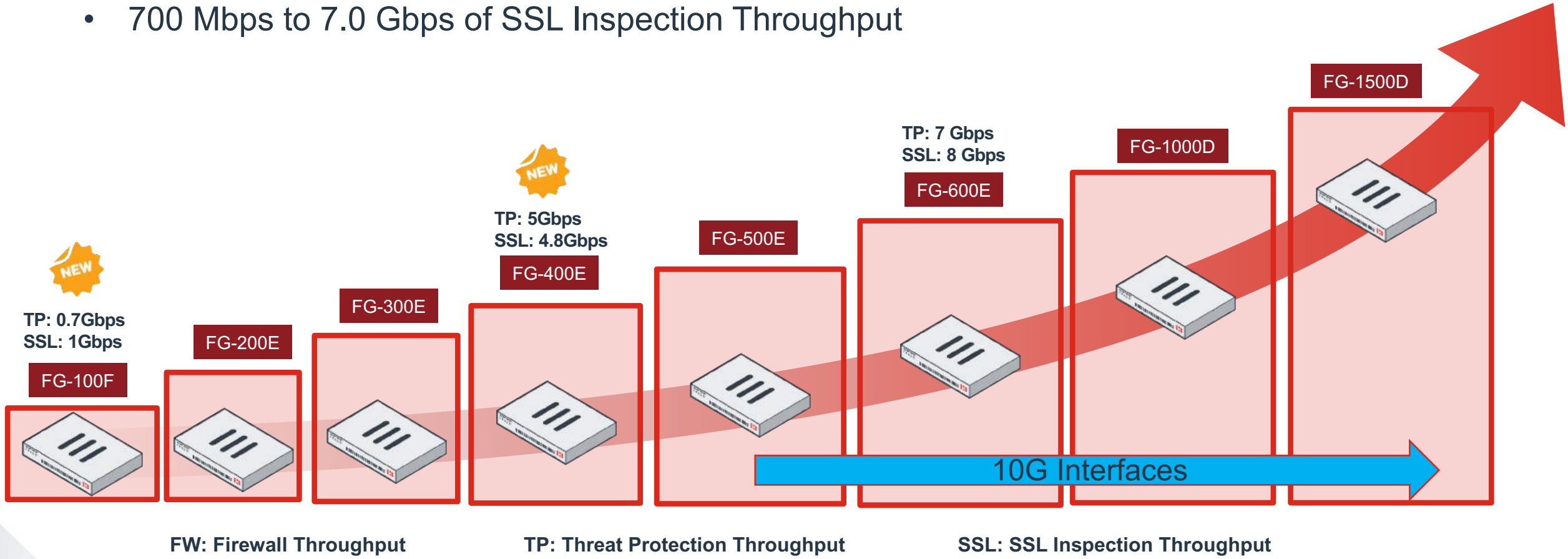
FortiGate Product Range



FortiGate – Mid-Range Enterprise Firewalls – Q2 2019

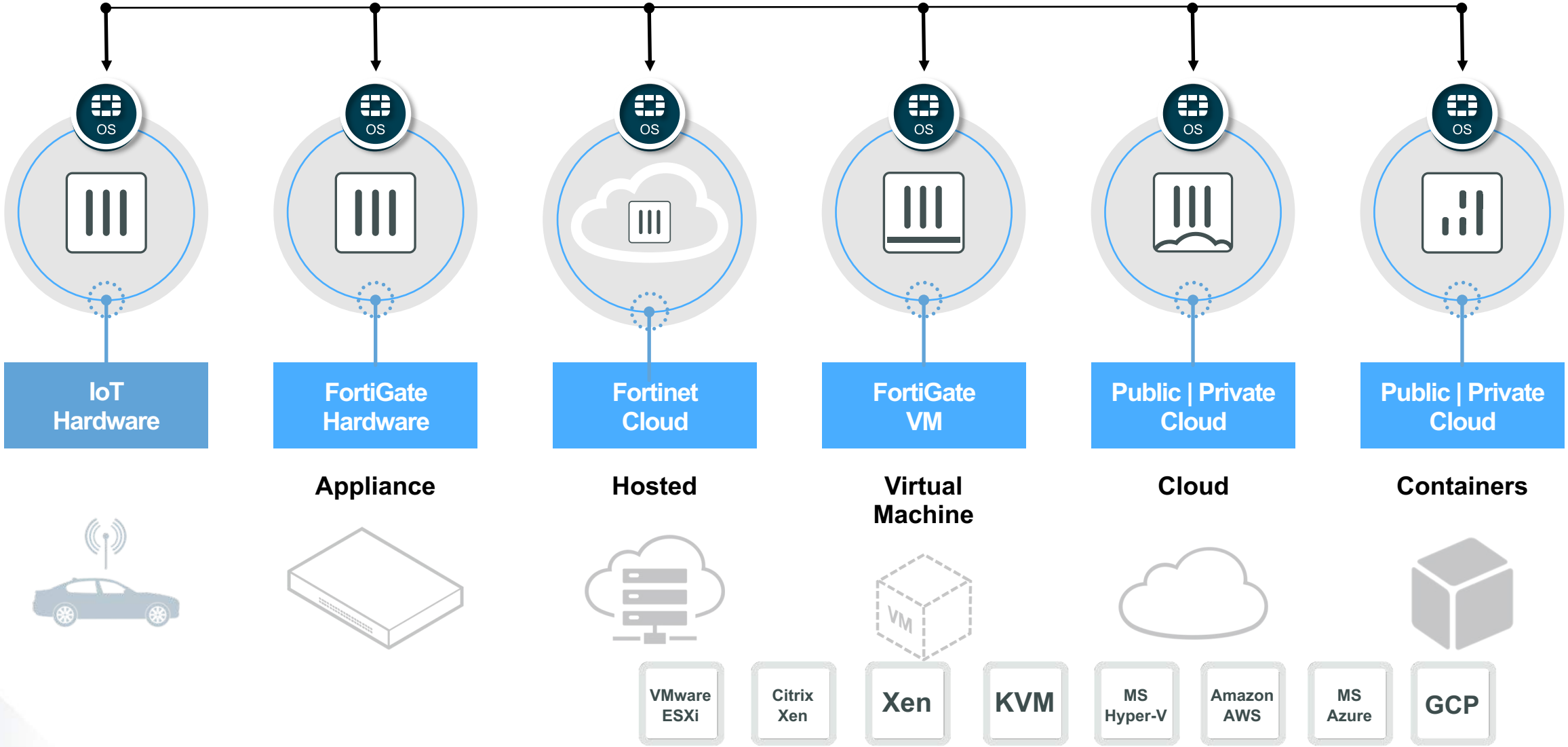
FortiGate 100 to 1500 series

- 350 Mbps to 5.0 Gbps of Threat Protection Throughput
- 700 Mbps to 7.0 Gbps of SSL Inspection Throughput



FortiOS: Adaptive Security Architecture

FortiGuard Security Updates

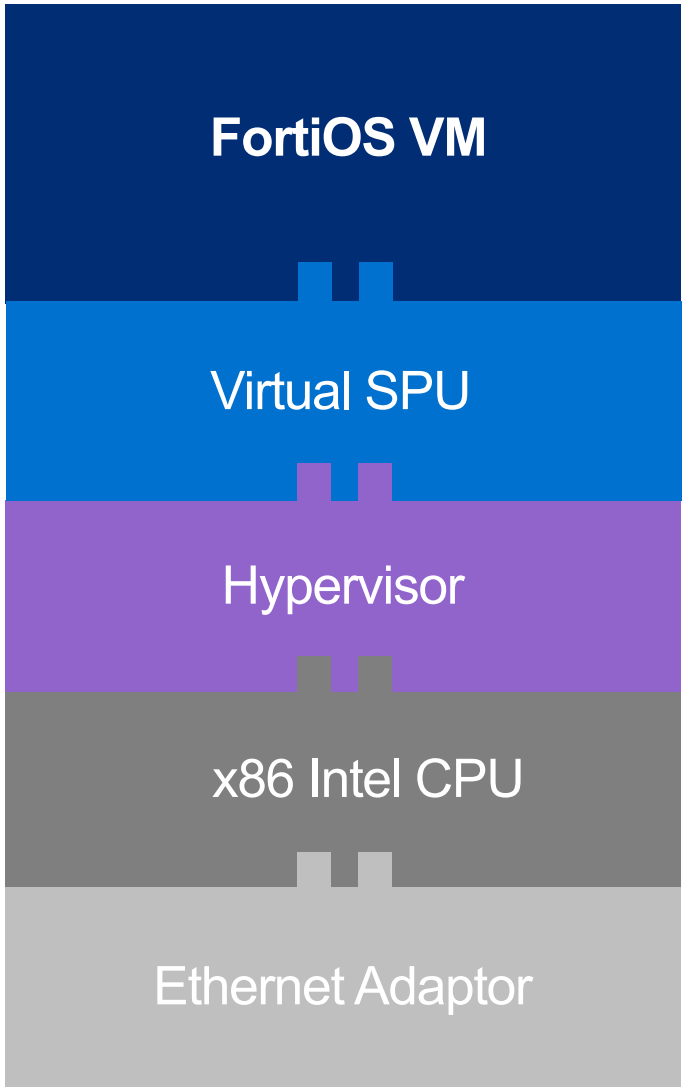


FORTINET

Virtual Hardware for a Virtual FortiGate

Optimizing Performance is a Challenge

- Virtual Appliance is Physical
- Hardware Dependencies Introduced at Every Layer
- Virtual SPU
  - Reduces FortiOS Complexity
  - Leverages Hardware Acceleration
  - Increases Performance



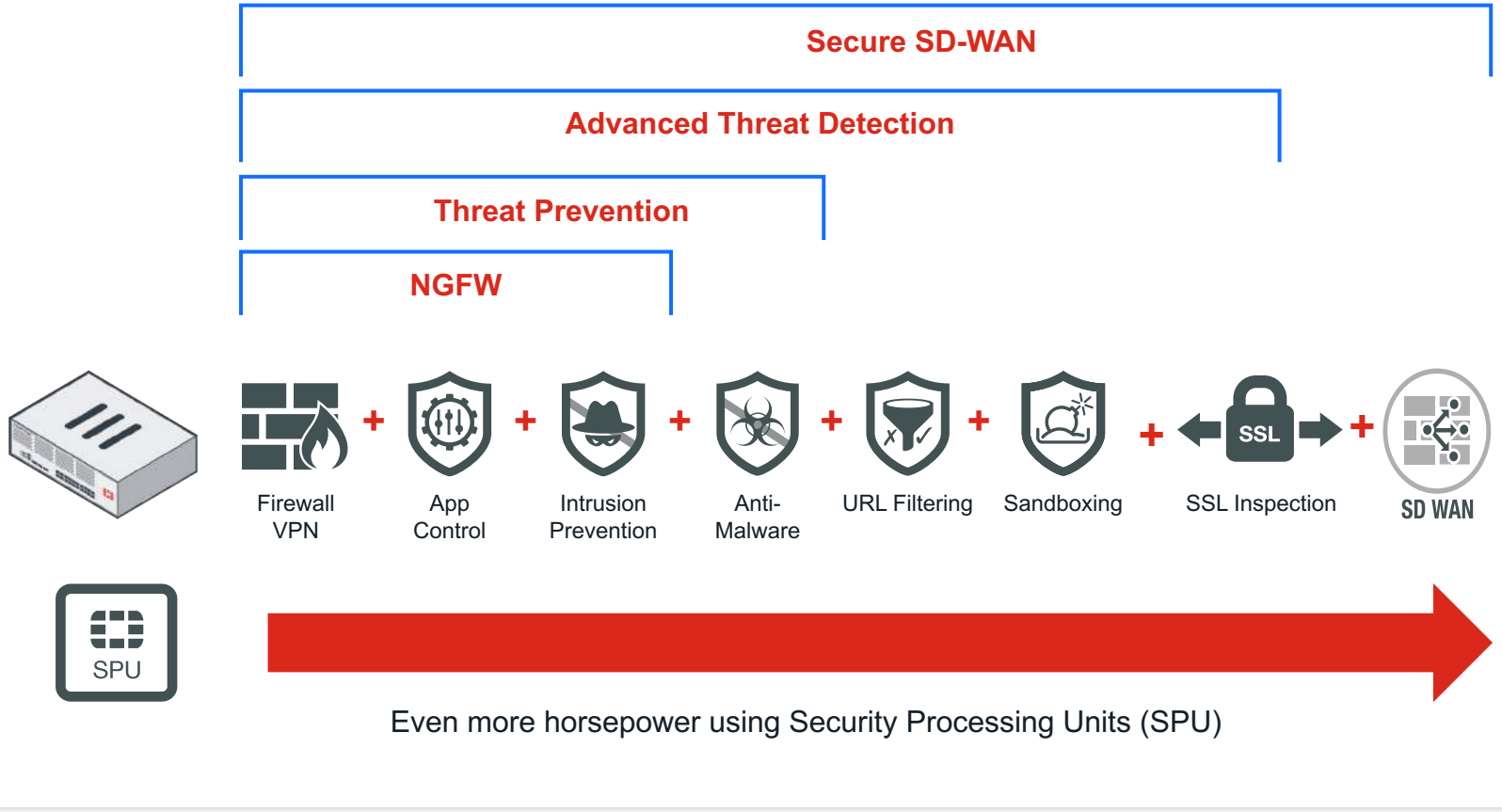
FORTINET

FortiGate – die nächste Generation der NGFW

Features

- Firewall/VPN
- Intrusion Prevention
- Web Proxy
- Antivirus
- Web-Filter
- Sandbox
- SSL Inspection

FortiGate Next Generation Firewalls



Anatomy

FortiOS 6.2

Configuration	Log & Report	Diagnostics	Monitoring	**Operation**	Systems Integration	Central Mgmt. and Provisioning	Cloud & SDN Integration
					Visibility	Automation	
Policy Objects	Device Identification	SSL inspection	Actions	**Policy and Control**	AAA	Compliance & Security Rating	
Anti-Malware	IPS & DoS	Application Control	Web Filtering	**Security**	Advanced Threat Protection (ATP)	Vulnerability Assessment	IOC Detection
Firewall	VPN	DLP	Email Filtering				
SD WAN	Explicit Proxy	IPv6	High Availability	**Networking**	Wireless Controller	Switch Controller	WAN Interface Manager
Routing/NAT	L2/Switching	Offline Inspection	Essential Network Services				
Physical Appliance (+SPU)	Virtual System	Hypervisor	Cloud	**Platform Support**	**Security Fabric**		

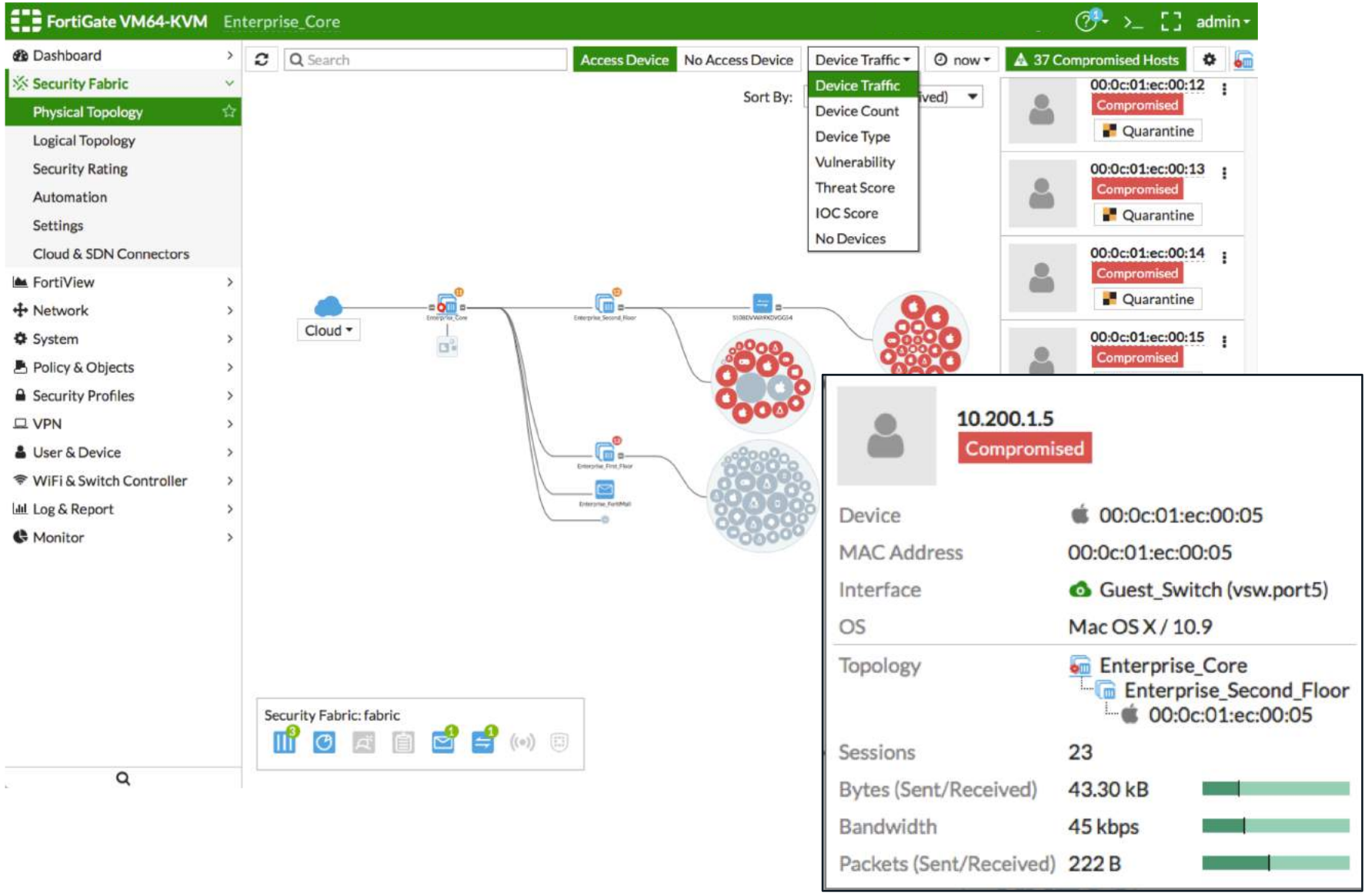
FORTINET

SECURITY FABRIC | OPERATION

VISIBILITY

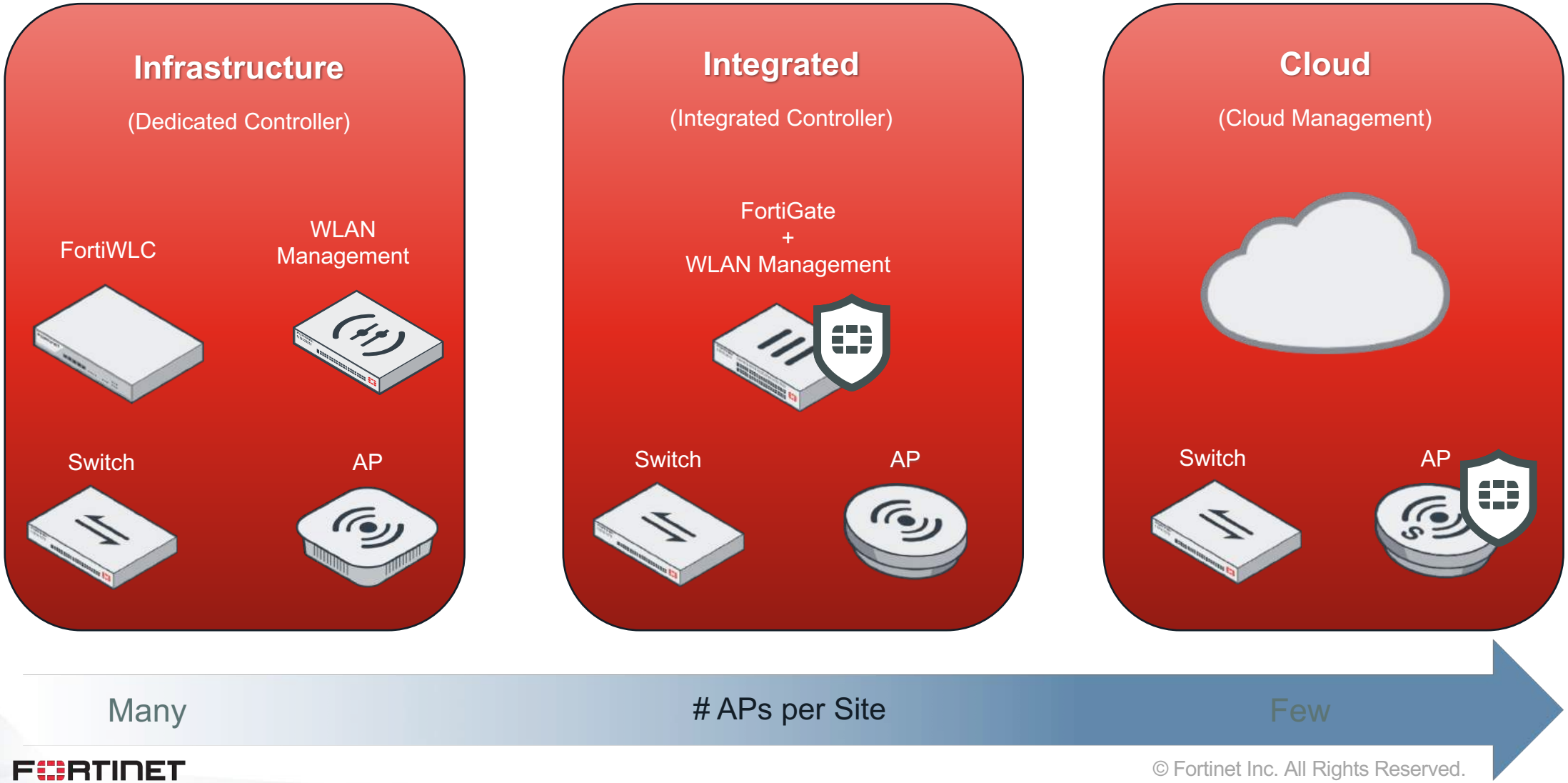
TOPOLOGY MAPS

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



Wireless...

Secure Access Architecture



FortiGate is a Wireless Controller

- **Every** FortiGate has a built-in wireless controller
- Models with integrated wireless and PoE available

30E
2/2 AP´s

60E-WiFi
5/10 AP´s

94D-POE
16/32 AP´s

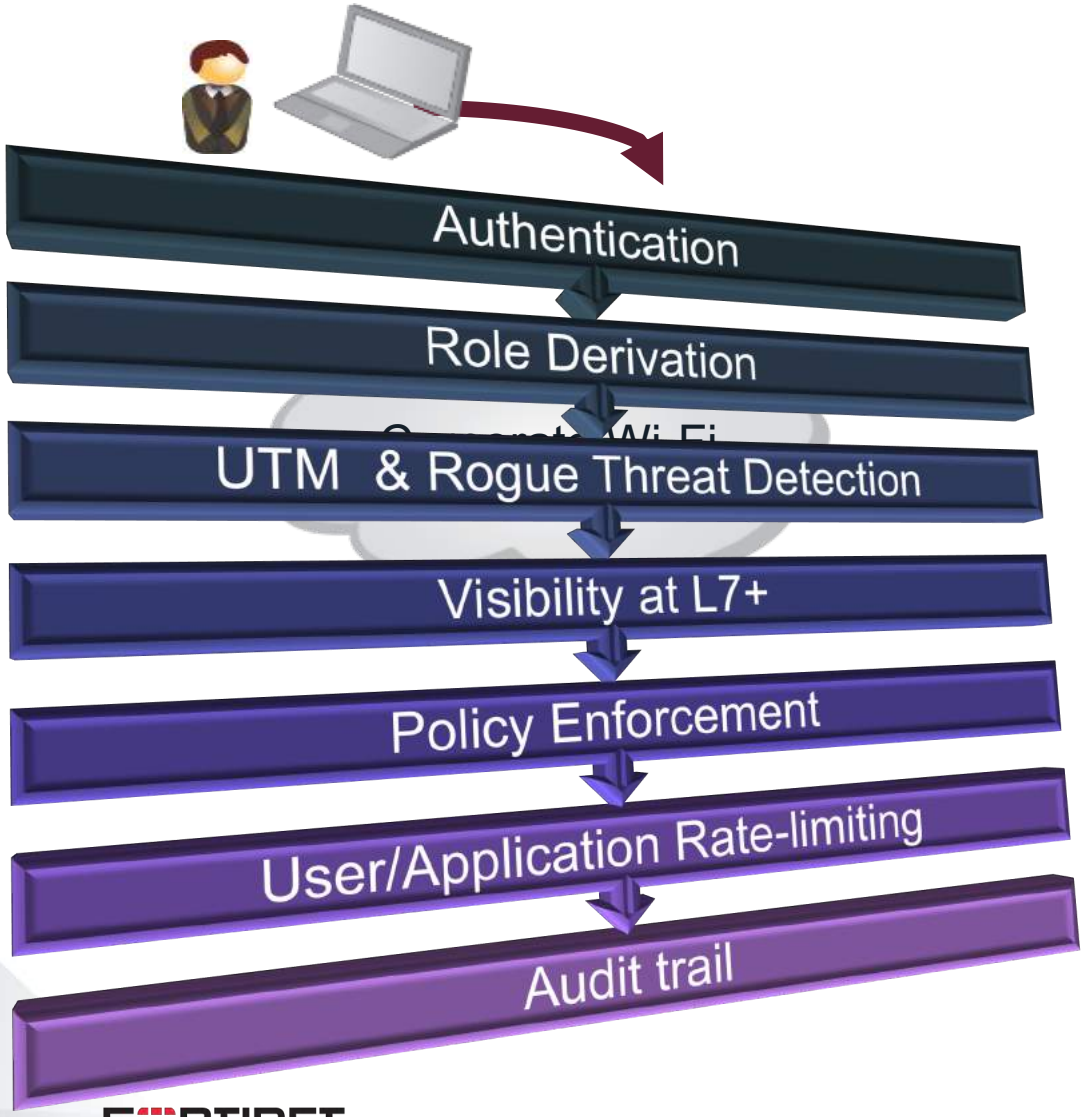
600E
512/1024 AP´s

1500D +
1024/4096 AP´s

FORTINET

SECURITY FABRIC | NETWORKING

WIRELESS CONTROLLER



SECURE ACCESS APPROACH

1. Captive Portal, 802.1x—Radius /shared key
2. Assign users and devices to their role
3. Examine wireless traffic to remove threats
4. Identify applications and destinations
5. Apply policy to users and applications
6. Ensures Business traffic has priority
7. Reports on policy violations, application usage, destinations and PCI DSS

FORTINET

WIRELESS CONTROLLER

USER ACCESS

MAC Address Filtering

- Using a filter list to either permit or exclude a list of clients identified by their MAC addresses
- List may be local or via RADIUS server

Captive Portal

- Web browsing intercept user login

WPA Personal (PSK)

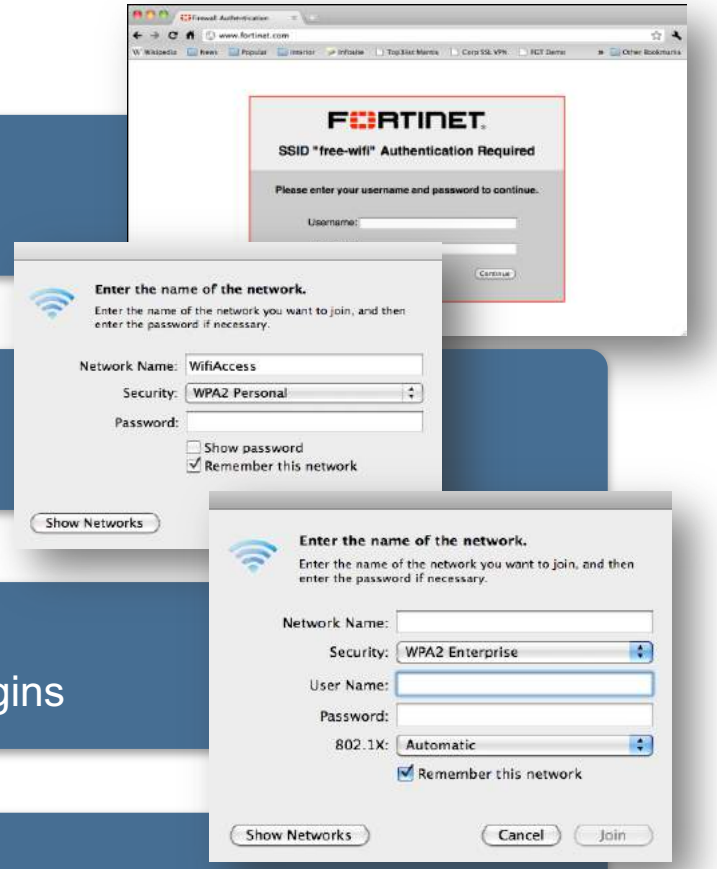
- Wireless access using pre-shared keys

WPA-Enterprise (802.1x)

- More secure access with individual user logins

OSEN

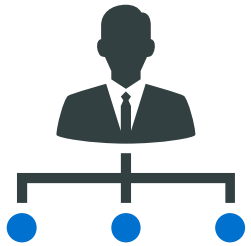
- Access option for Hotspot 2.0



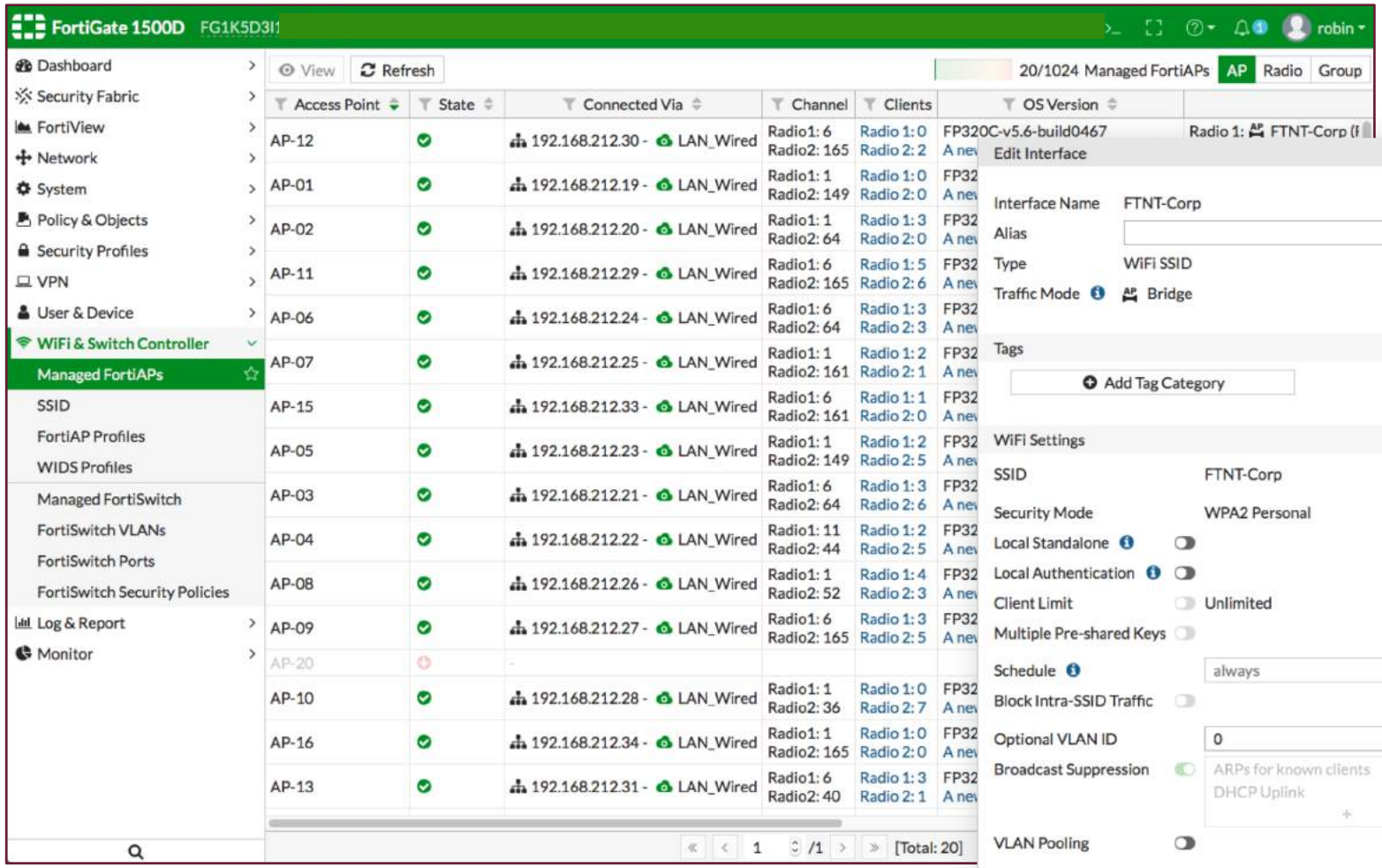
SECURITY FABRIC | NETWORKING

WIRELESS CONTROLLER

AP MANAGEMENT



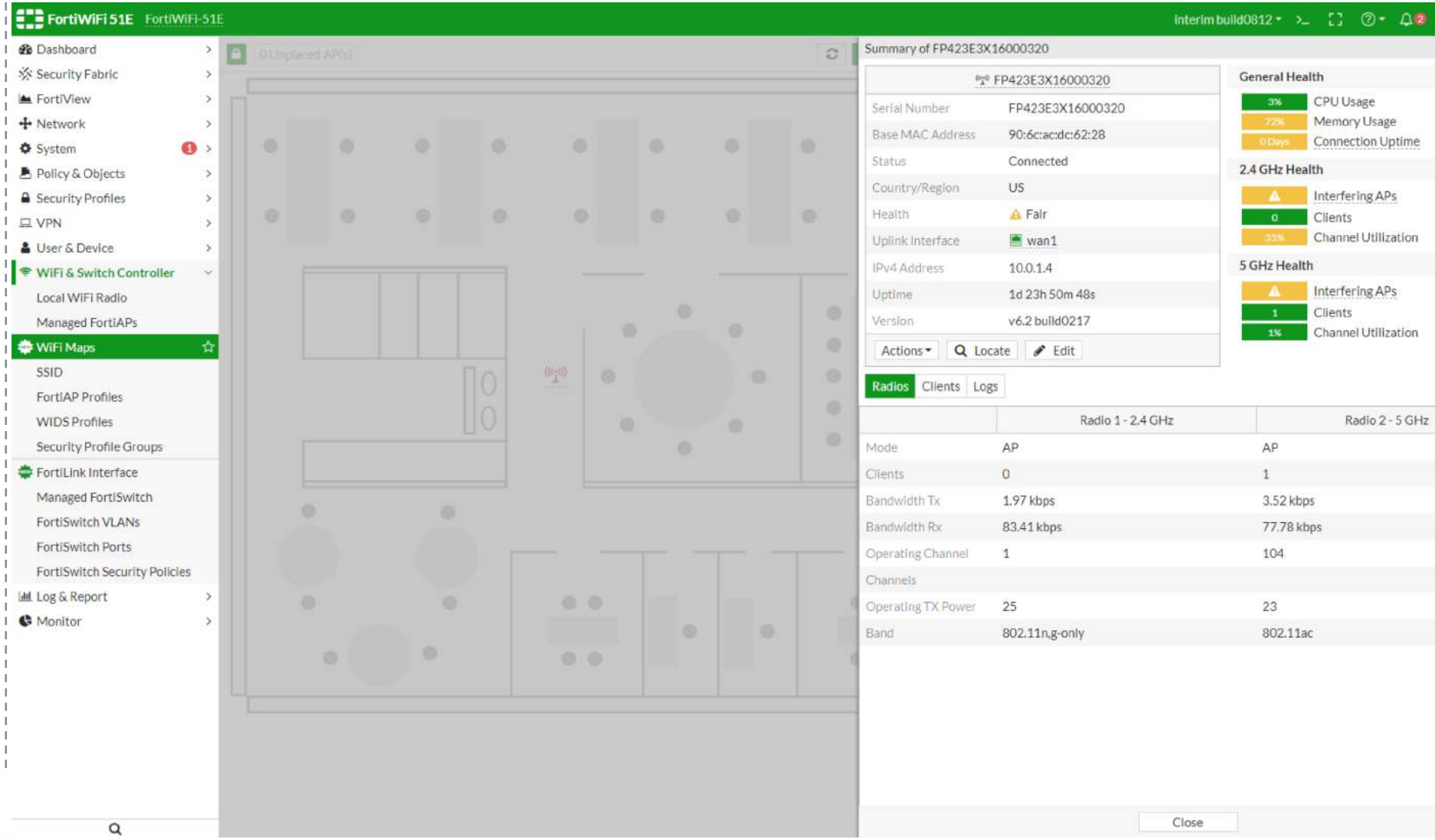
- Discover and (pre)authorize APs easily
- Batch configurations and upgrades on multiple APs through GUI
- Setup firewall policies with optional UTM profiles applied to SSIDs (wireless networks)



Wireless Management Extension

WIFI LOCATION MAP

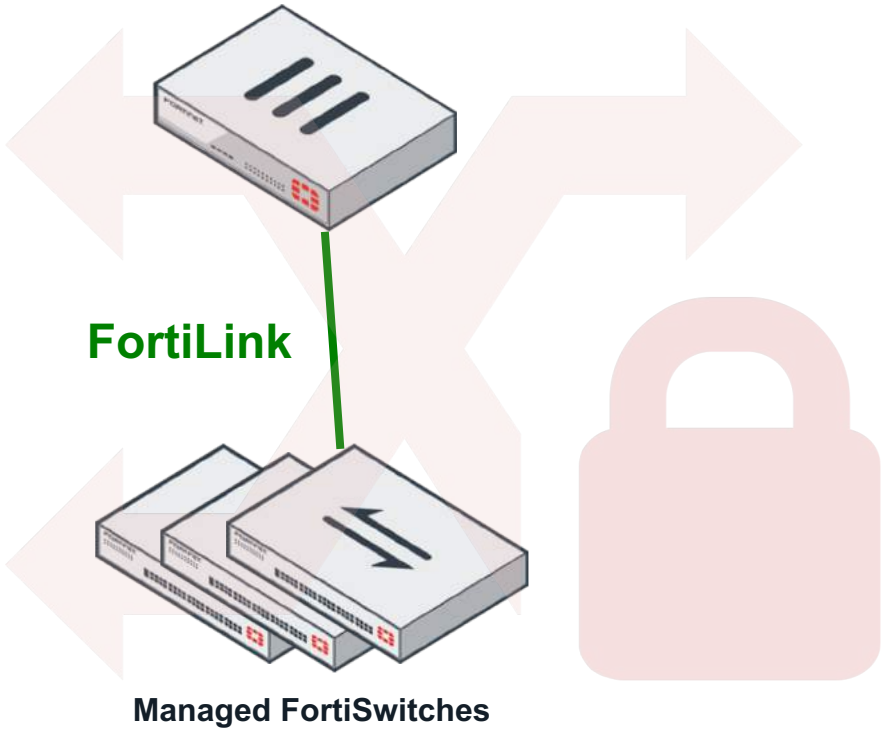
- New “WiFi Regions” GUI panel
- Allows admin to upload floor plans and place managed APs.
- Display statistics for each AP, including Client Count, Channel, Op TX power and Channel Utilization
- Mouse-over for AP details

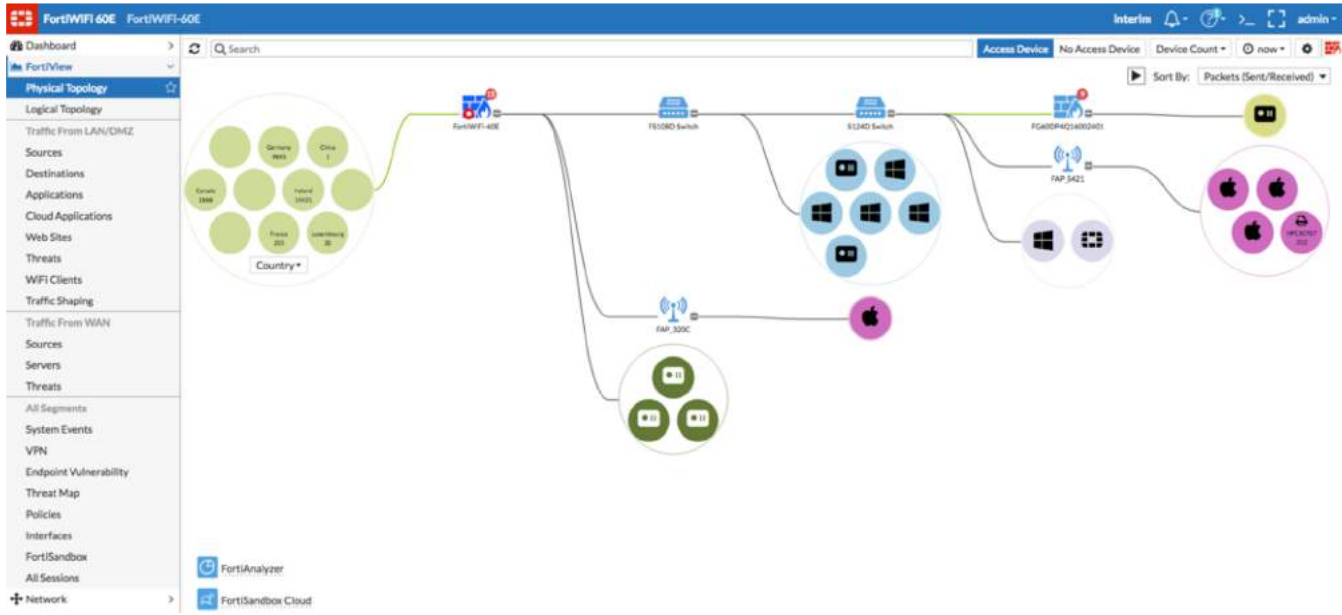


... und Wired

FortiSwitch and FortiLink

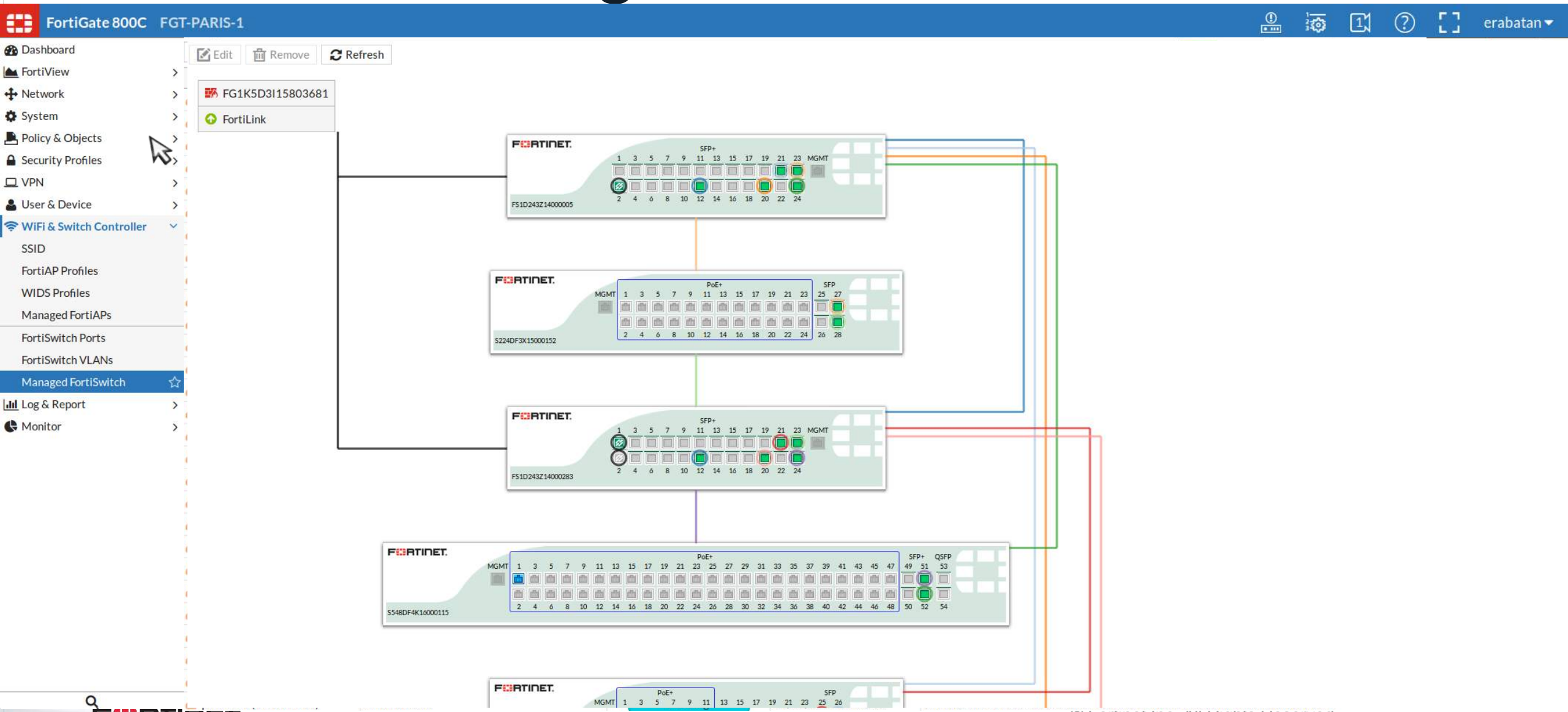
FortiSwitch becomes a logical extension of the FortiGate when connected via FortiLink





- **Easy to Deploy and Manage through Fortigate interface.**
- **Device detection and port visibility.**
- **Stacking up to 256 switches per FortiGate.**

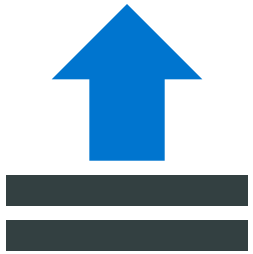
Central monitoring of the Fabric



SECURITY FABRIC | NETWORKING

SWITCH CONTROLLER

FORTILINK STACKING

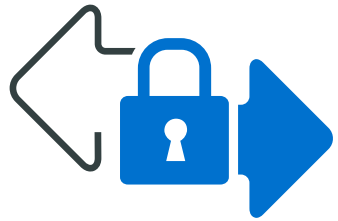


- Manage multiple switches from single (or A-P HA) FortiGate
- Connect from 1 to 256 switches in a single stack, depending on FortiGate models
- Switches form ISL (inter-swtch links) automatically
- Supports various topologies, including MCLAC 2 tier switching and daisy-chain

ENTERPRISE-CLASS SWITCHING

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

ACCESS CONTROL



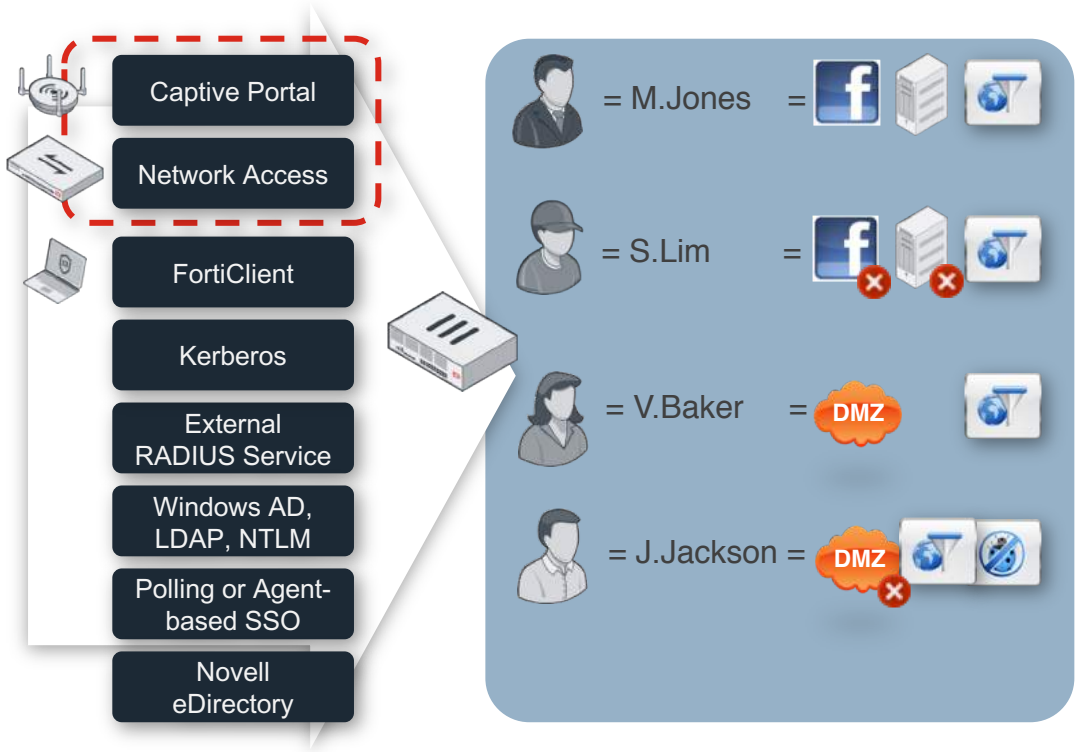
- Support port-based and MAC-based 802.1x
- MAC authentication bypass and Open-Auth. mode

FORTINET

AAA

USER IDENTITY ACQUISITION

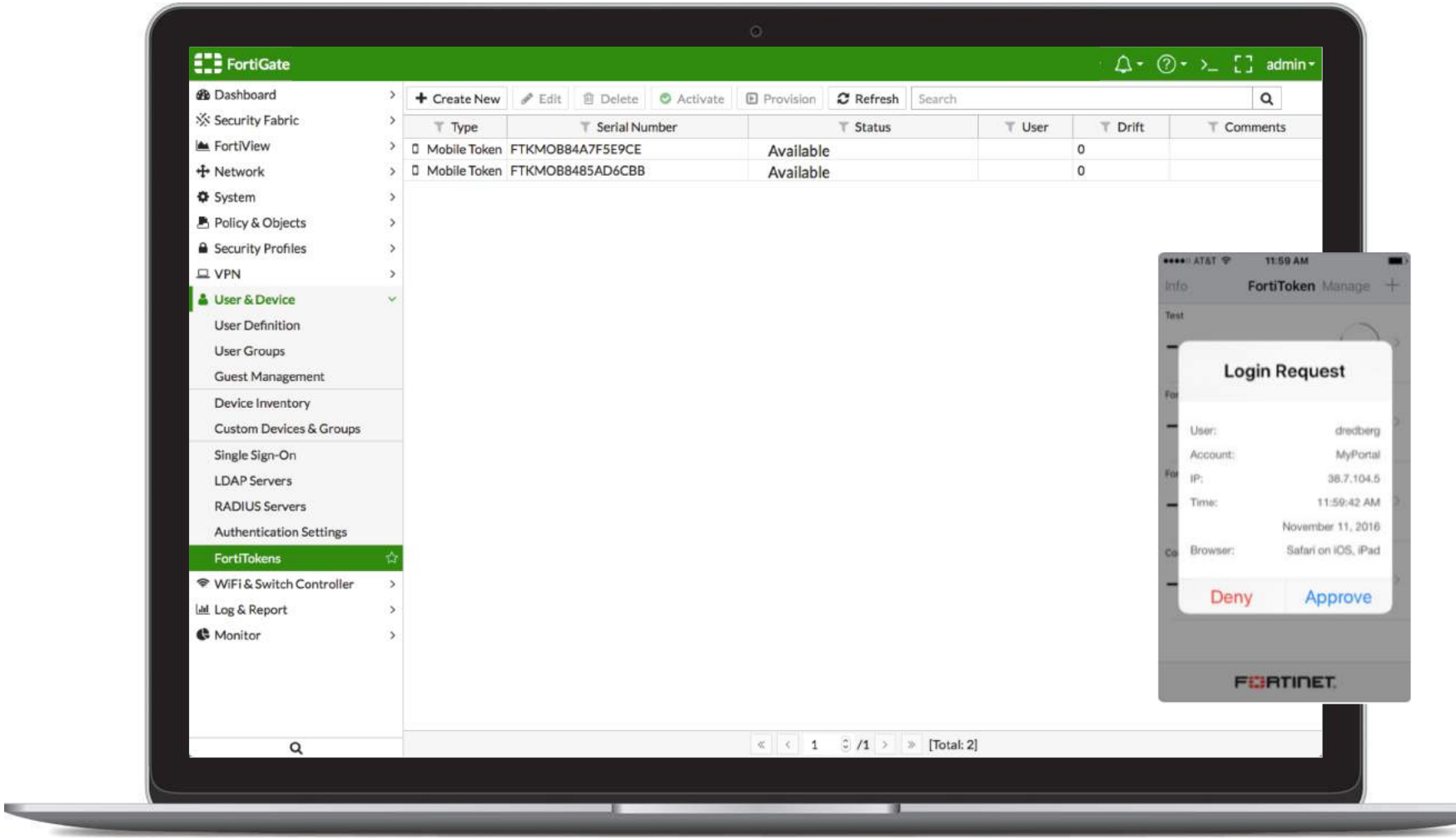
- Using both active and passive acquisition methods
- Reuse user login info for user Identity based policies



AAA

INTEGRATED TOKEN SERVER

- Provision and manage both physical and mobile FortiTokens
- Admin-Access, User-Authentication, VPN etc.
- for central management use FortiAuthenticator



New Cloud Service from Identity and Access Management

FortiToken Cloud

Identity and Access Management

Two-Factor that's Easy to Manage and Easy to Use

Everything needed for two-factor in a FortiGate environment

Key Features include:

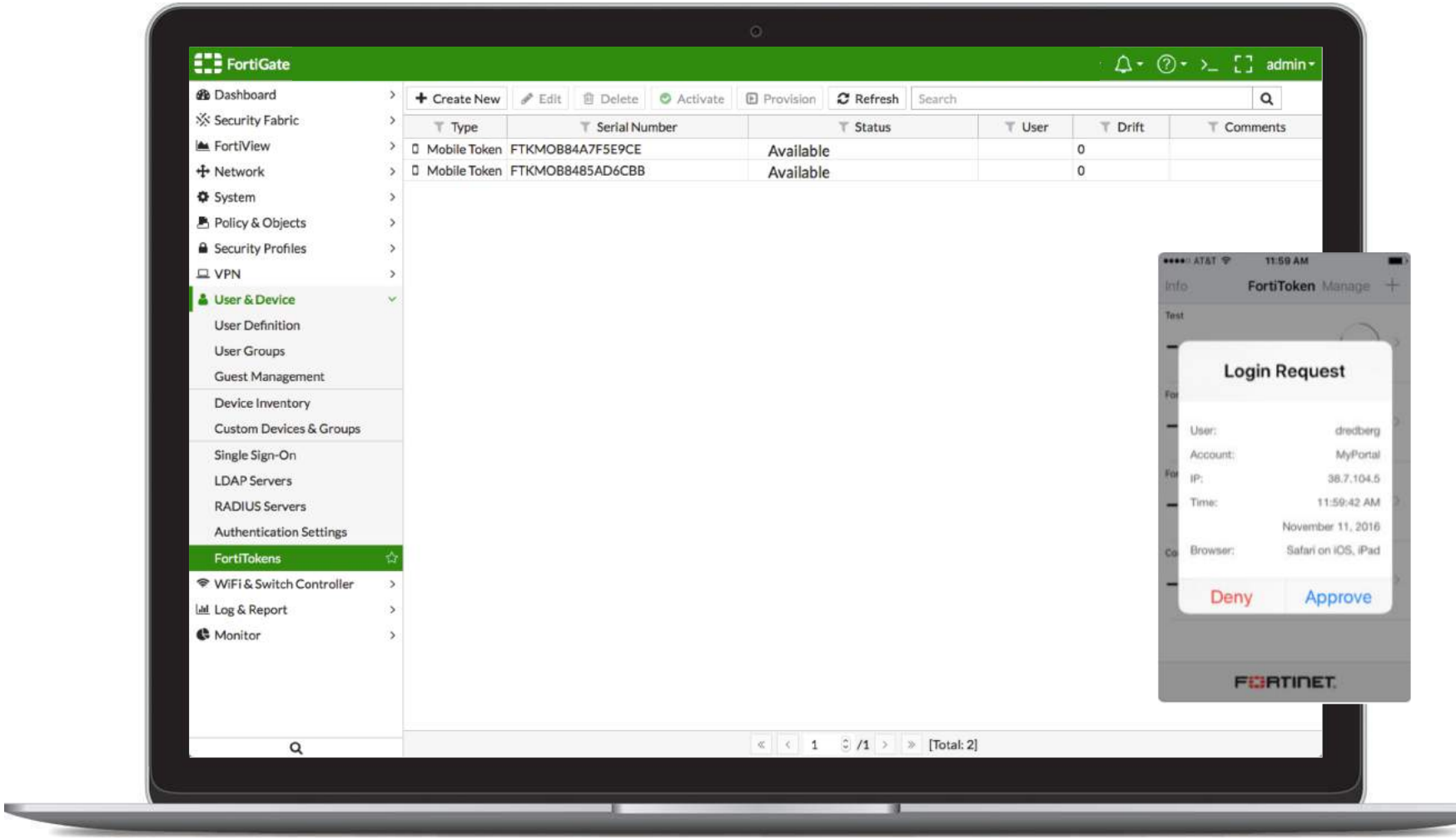
- Manage two-factor deployments from provisioning to revocation
- Includes Tokens through FortiToken Mobile app - simplifies user input to "click to accept"
- No additional onsite hardware, software, or ACL changes
- Easy expand and grow as needed.
- Access from anywhere there is an internet connection

FORTINET

AAA

INTEGRATED TOKEN SERVER

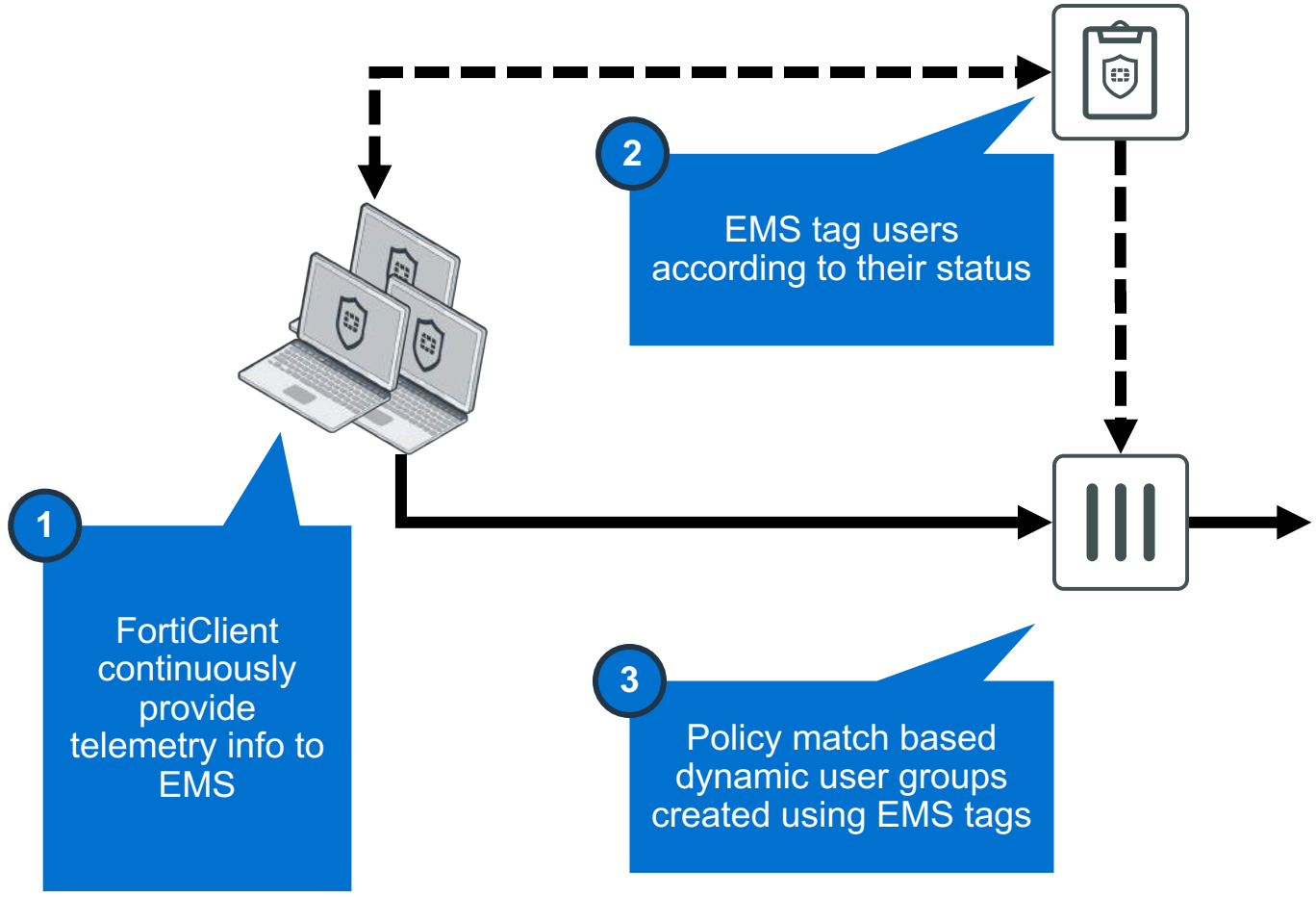
- Provision and manage both physical and mobile FortiTokens
- Admin-Access, User-Authentication, VPN etc.
- for central management use FortiAuthenticator



Endpoint Compliance with Dynamic User Objects

Requires EMS active in Security Fabric

- Functionality replaces previous endpoint compliance profiles
- Requires EMS in the Fabric to tag clients accordingly and pass information to FGT in real time. (similar to FSSO concept)
- **Compliance** is part of the Policy by using Fabric Connector features (6.2)



FortiNAC

für Netzwerke bei denen 802.1x schwierig ist

Introducing FortiNAC

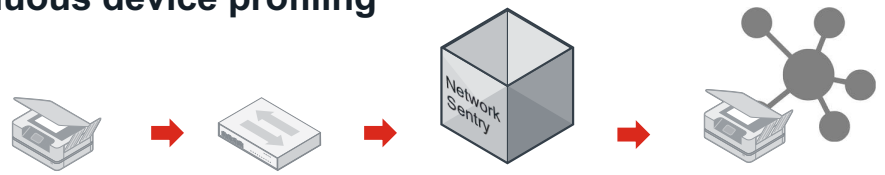
Appliance

Virtual Machine

Provides Visibility of Users and End points for Enterprise Networks and Automates Threat Response

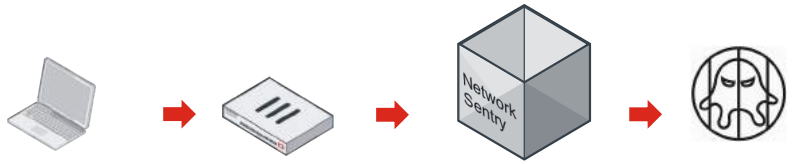
- Device identification and profiling
- Simplified guest access with self-registration
- Continuous risk assessment
- Micro-segmentation of endpoints
- Automated response to identified risks
- Orchestration of 3rd party devices

Continuous device profiling



1. Printer connected to network
2. MAC notification trap triggers FortiNAC
3. FortiNAC Profiles device as printer
4. FortiNAC Informs Fabric to allow Printer-type access to network

Containment of lateral threats at Edge



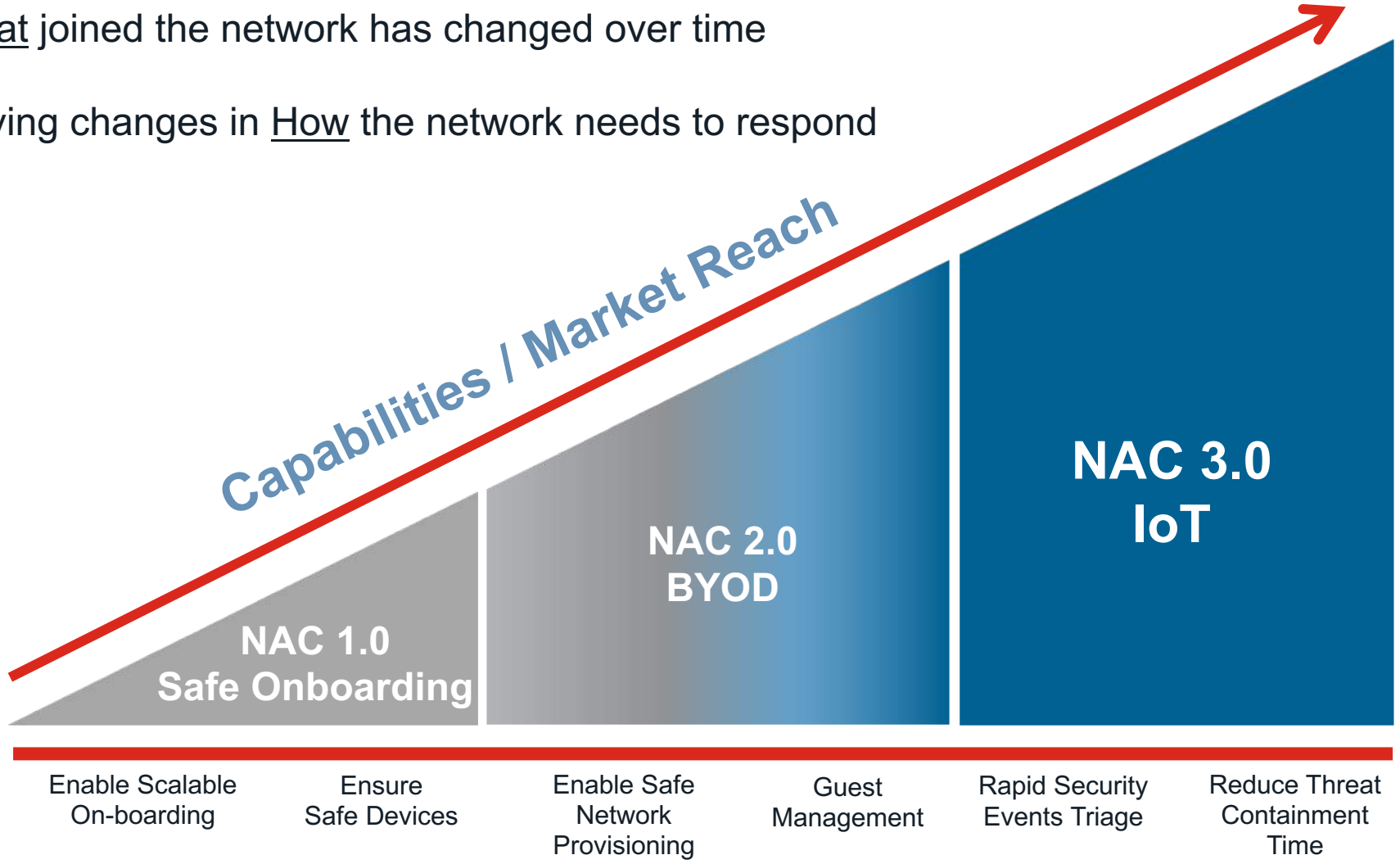
1. User brings infected laptop to work
2. FGT sends event to FortiNAC
3. FortiNAC quarantines the laptop at access layer
4. Virus contained at switch node

FORTINET

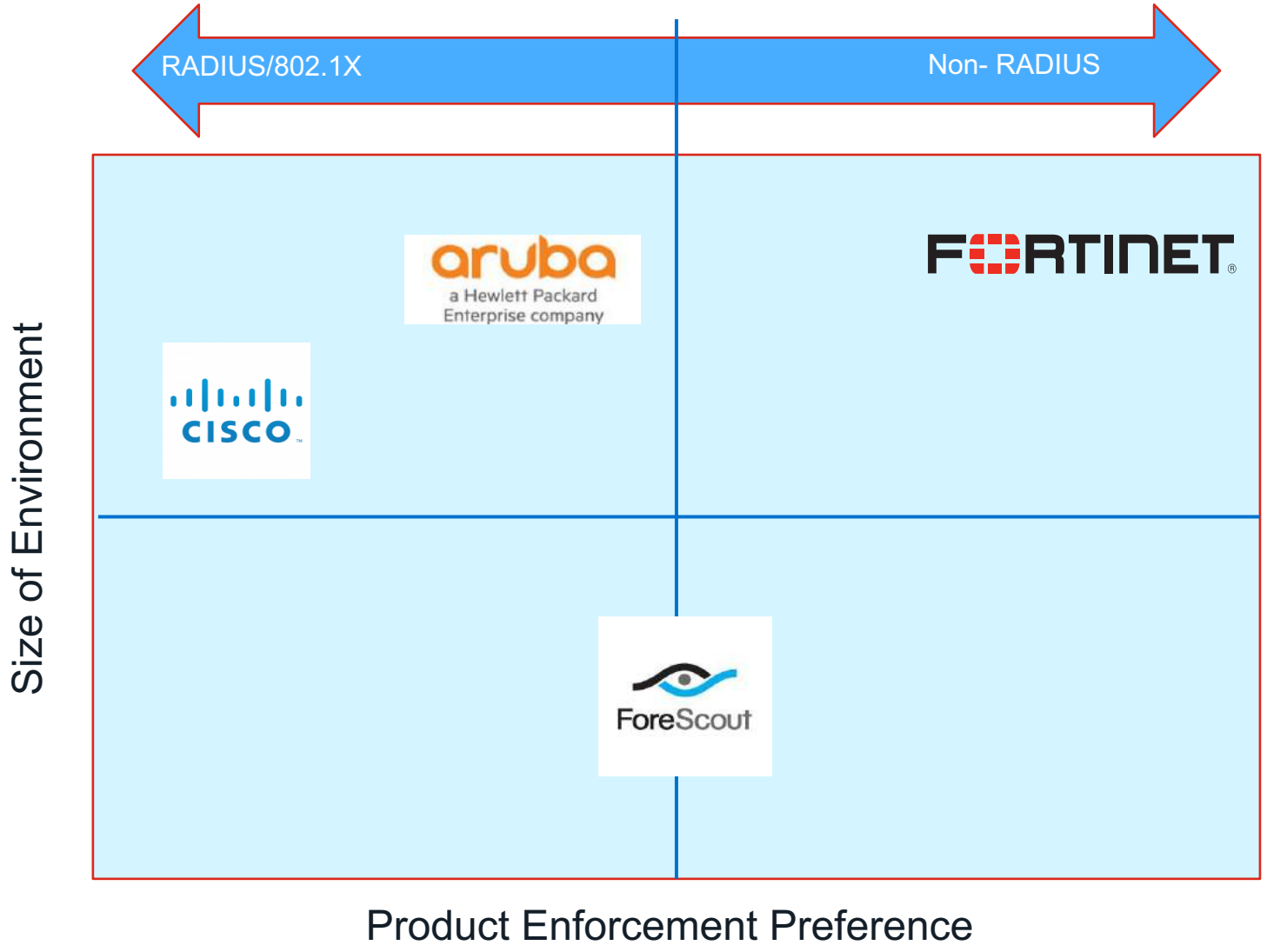
The Evolution of Network Access Security

What joined the network has changed over time

Driving changes in How the network needs to respond

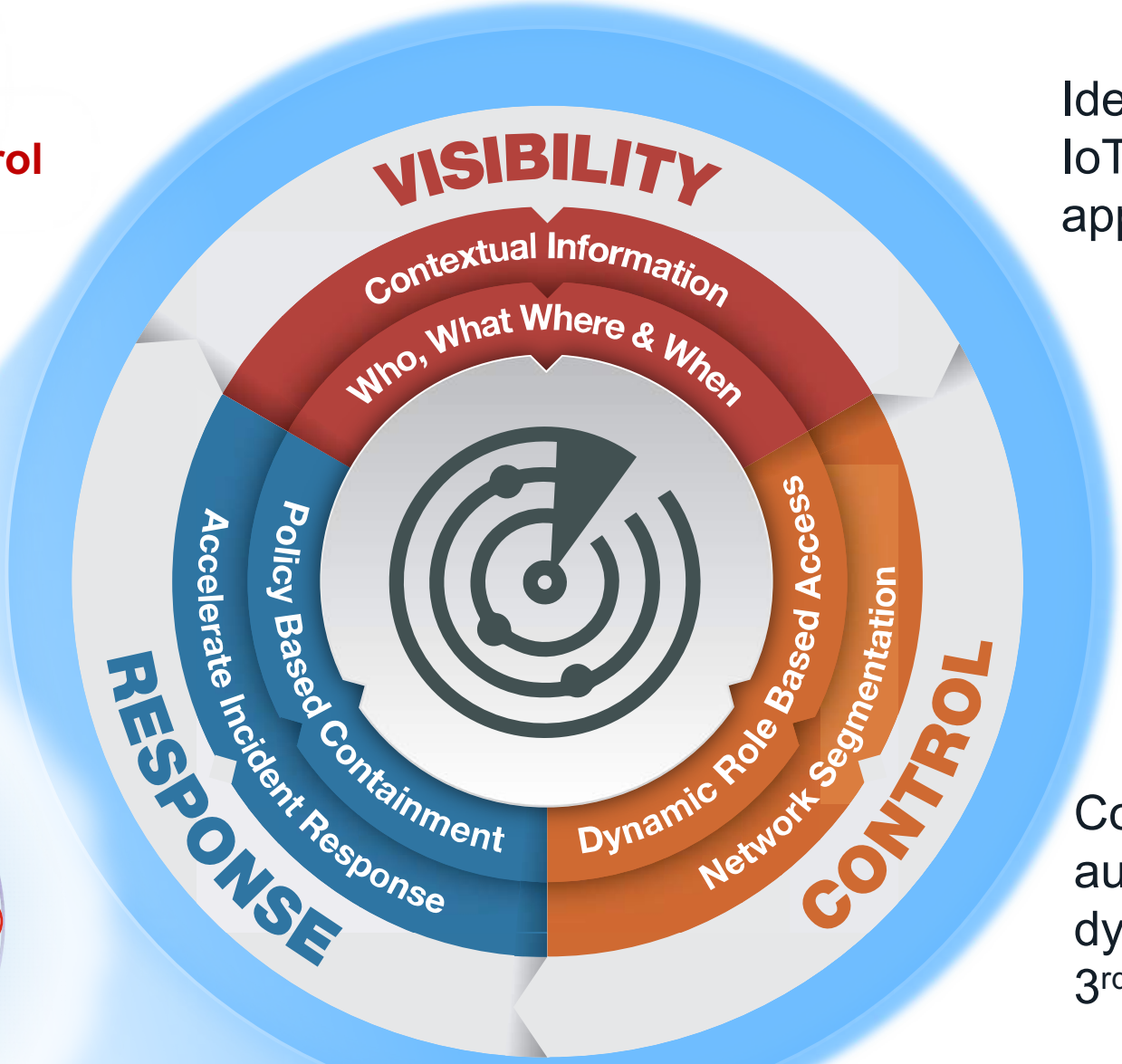


Competitive



FortiNAC

Network Access Control



Identify and profile all endpoints, IoT devices, users, & applications

Segmentation based on endpoint characteristics and behavior

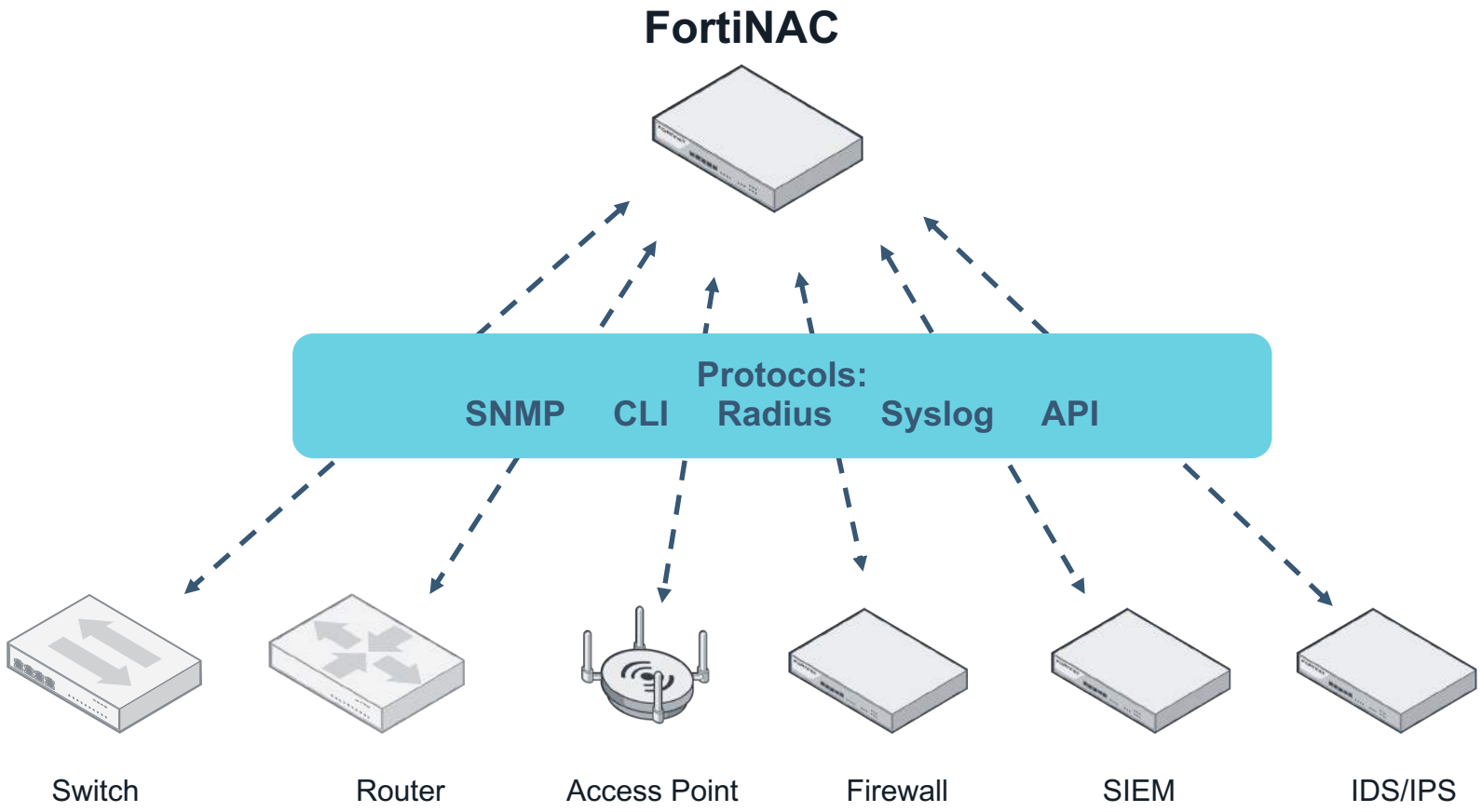
Continuous risk assessment and automated responses for dynamic network control across 3rd party devices

WATCHING EVERY NODE ON THE NETWORK

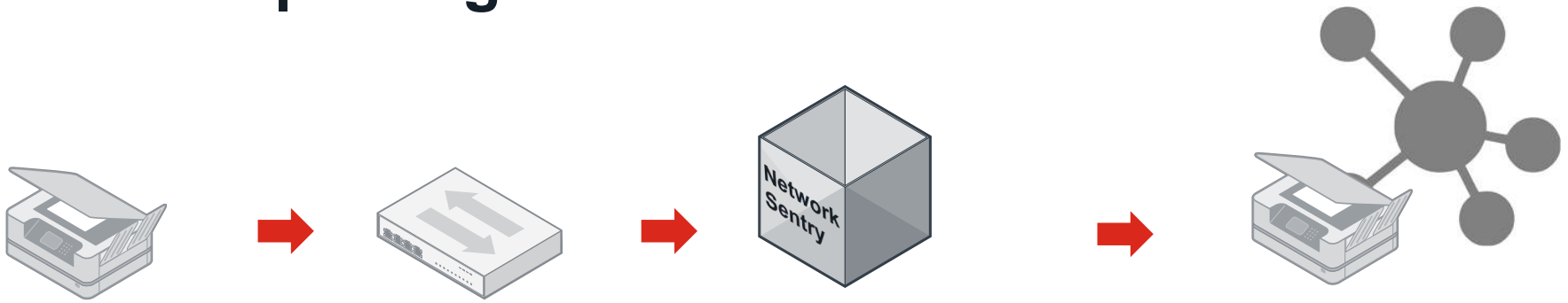
FORTINET

Visibility: Agentless Data Collection

Information Gathered from Multiple Sources

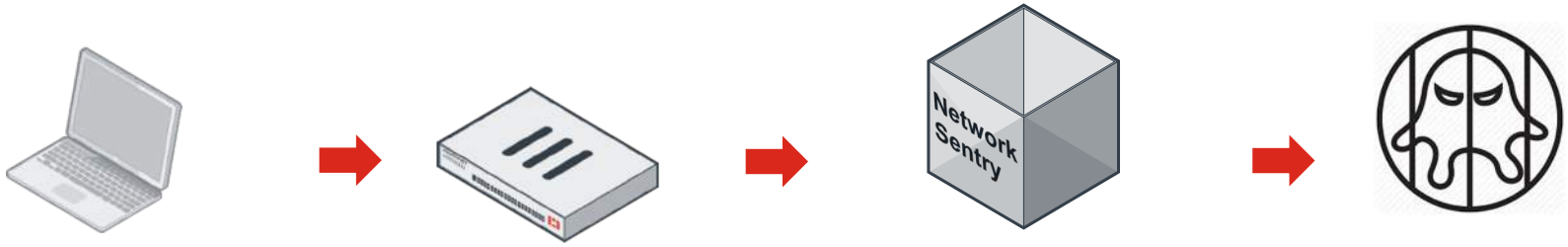


Continuous device profiling



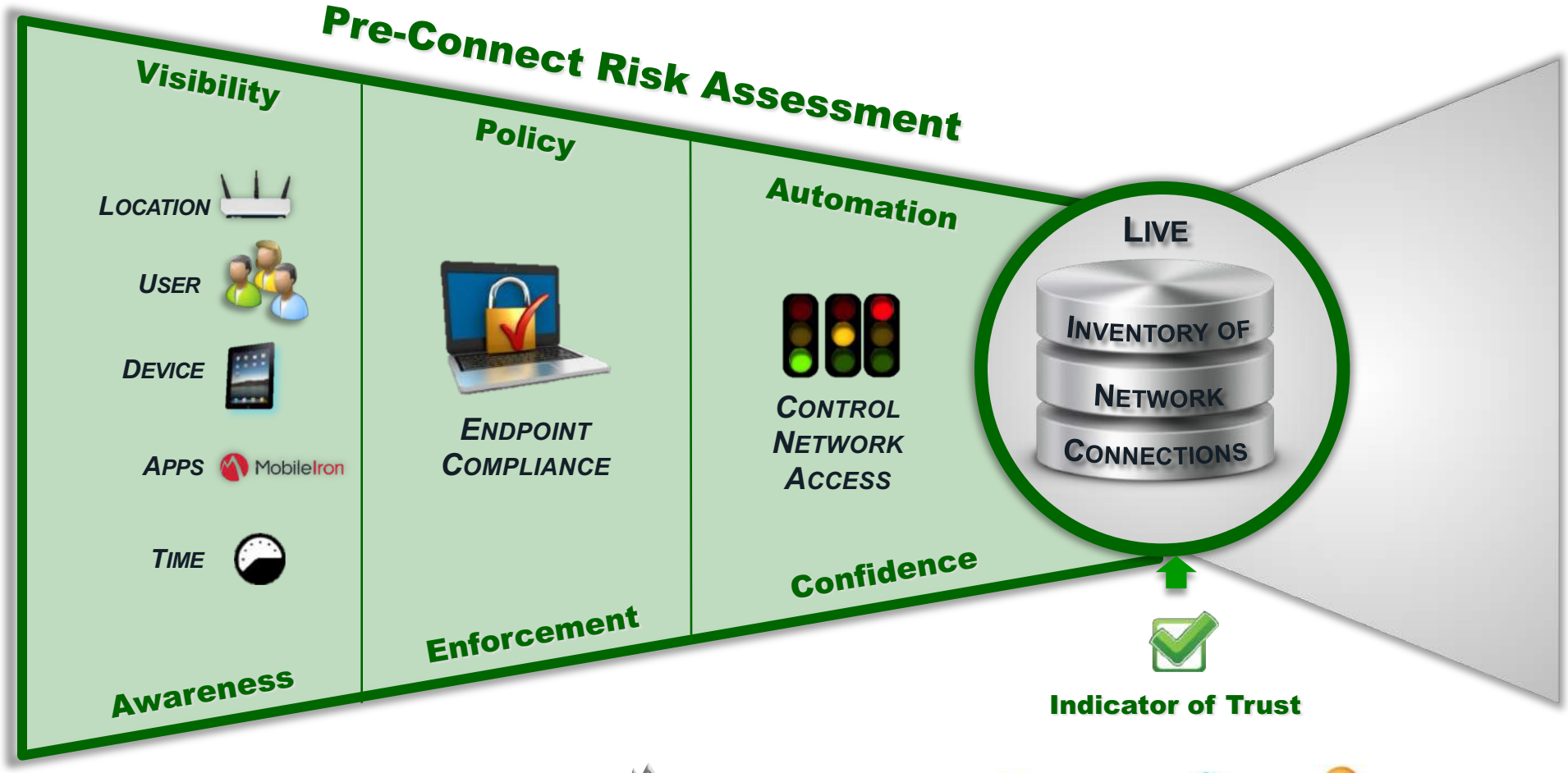
1. Printer connected to network
2. MAC notification trap triggers Network Sentry
3. Network Sentry Profiles device as printer
4. Network Sentry Informs Fabric to allow Printer-type access to network

Containment of lateral threats at Edge



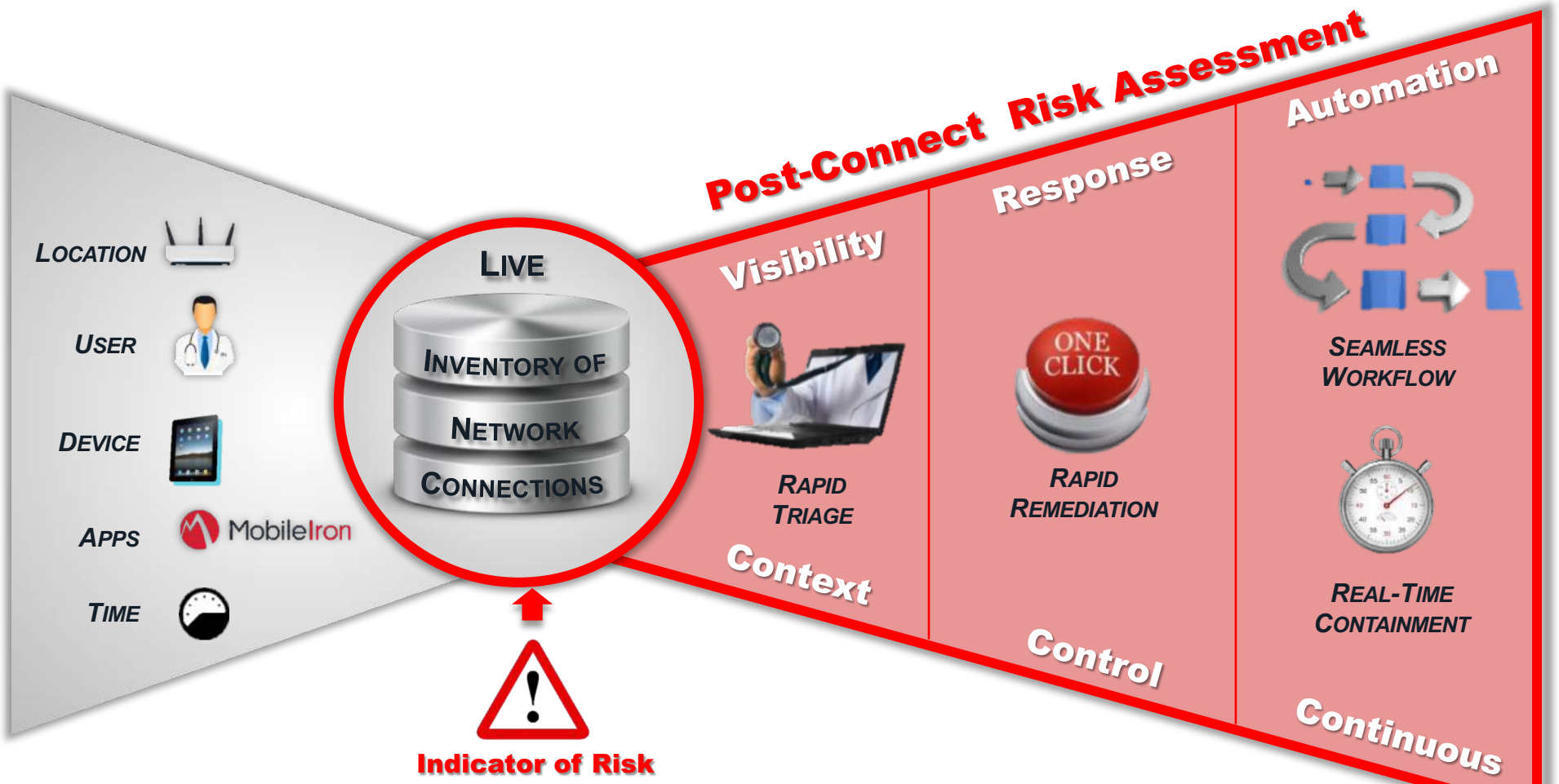
1. User brings infected laptop to work
2. FGT sends event to Network Sentry
3. Network Sentry quarantines the laptop at access layer
4. Virus contained at switch node

FortiNAC Visibility and Dynamic Network Access



FORTINET

FortiNAC Automated Threat Mitigation



FORTINET RSA FireEye splunk> 1Labs

Check Point SOURCEfire McAfee Symantec ArcSight LogRhythm

FORTINET

Elements of Network Access Control Solution

Appliances

- 3 Control & Application Appliances
- 2 Control Appliances
- 2 Application Appliances
- Manager (concurrent license coordination)

Virtual Machines (most popular)

- Control / Application VM
- Manager VM (concurrent license coordination)
- Analytics via FortiAnalyzer

Protection License Levels

1. Basic
   - Detection
2. Plus
   - Detection & Control
3. Pro
   - Detection, Control, & Response

FortiAnalyzer

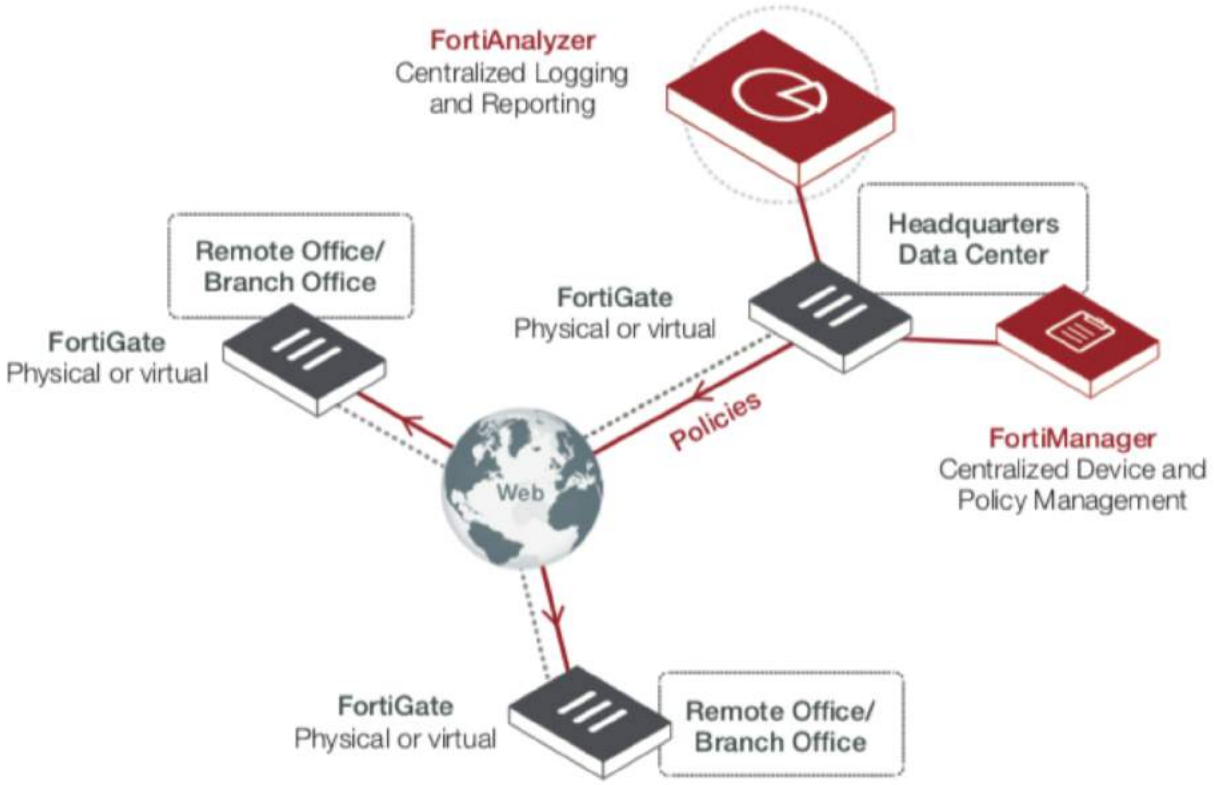
Wissen was im Netzwerk passiert

Introducing FortiAnalyzer

Appliance | Virtual Machine | Hosted | Cloud

Logging, reporting and analysis from multiple Fortinet devices

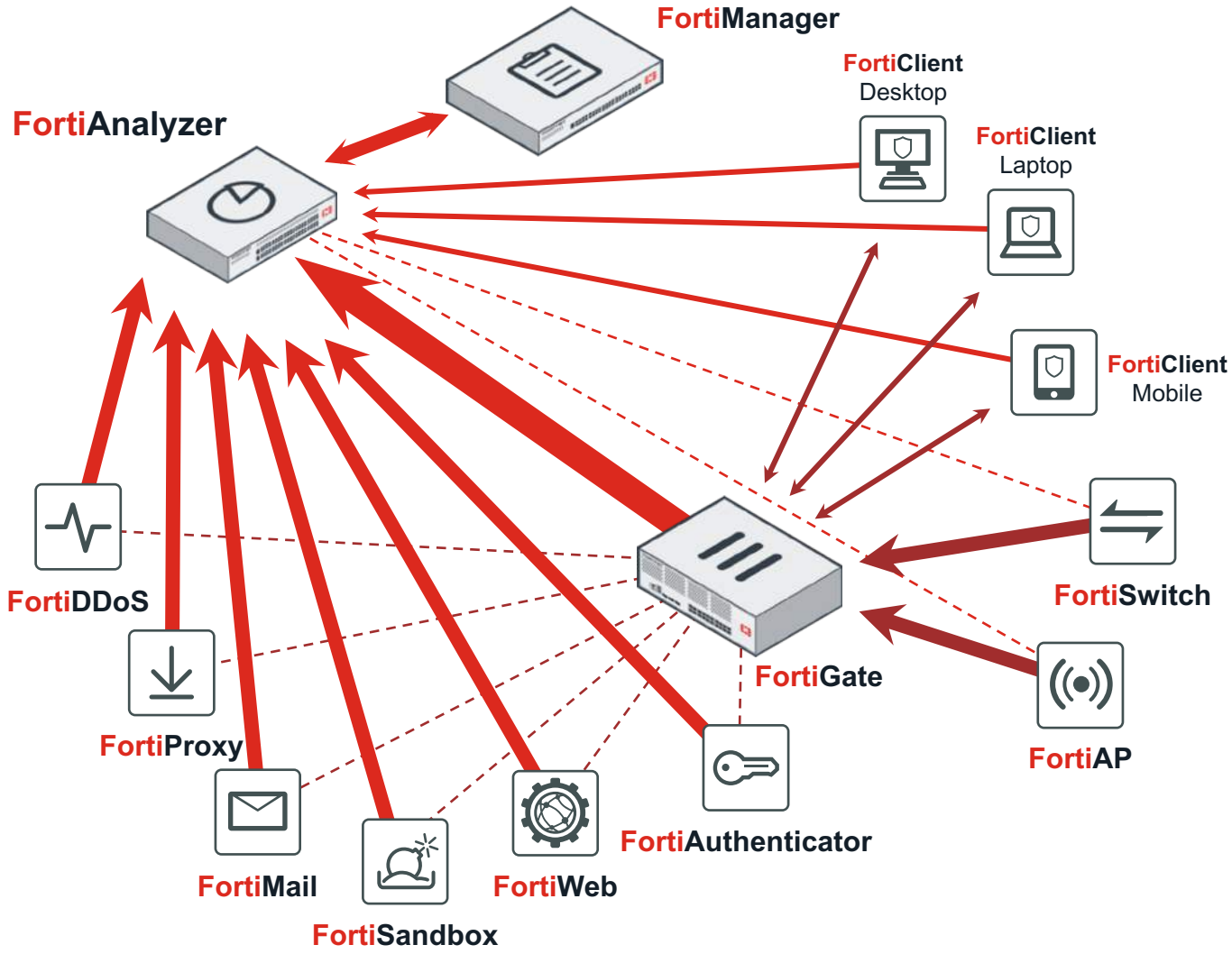
- Centralized Search and Reports
- Real-time and Historical Views into Network Activity
- Scans security logs using FortiGuard IOC Intelligence for APT detection
- Light-weight Event Management
- Seamless Integration with the Fortinet Security Fabric



FORTINET

FortiAnalyzer Security Fabric Integration

- **FortiGate**
  - Primary source of data for FortiAnalyzer
  - FortiAnalyzer receives full logs on security alerts, traffic and status
  - FortiGate collects and writes data from other Security Fabric elements into its own logs
- **FortiSwitch, FortiAP**
  - FortiAnalyzer receives alerts, traffic and status as it is passed and written to FortiGate logs
- **FortiClient**
  - FortiAnalyzer receives alerts and status from each Client individually
- **FortiMail, FortiSandbox, FortiWeb, FortiAuthenticator, FortiDDoS**
  - FortiAnalyzer receives security alerts and status directly from these Security Fabric components
- **FortiManager**
  - FortiAnalyzer can be managed by FortiManager and embed its interface and data directly inside the FortiManager interface



FortiAnalyzer Product Line

Hardware Appliances

- 7 models
- Store from 200 GB of logs per day to 8.3 TB of logs per day
- 12 TB storage up to 240 TB storage

Virtual Appliances

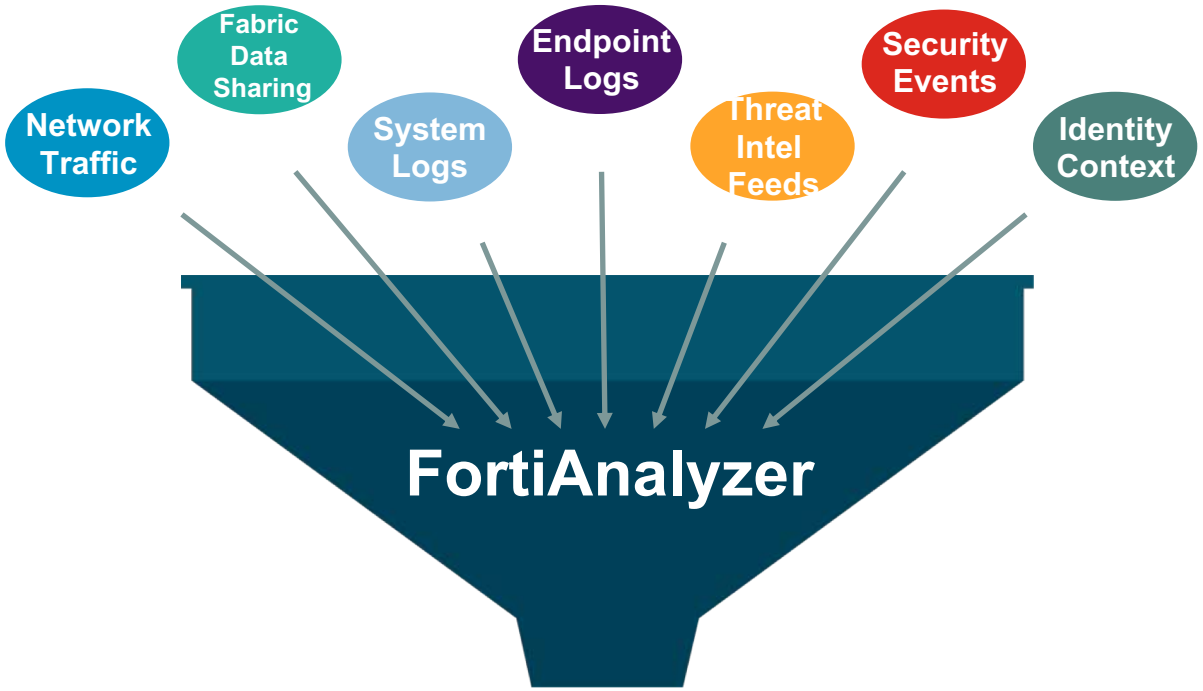
- 3 VM models
- Licensing by GB logs per day and total TB overall storage
- Perpetual licensing

SECURED BY FORTIGUARD®

Indicator of Compromise Subscription

- Scans web logs, identifying likely compromised hosts
- Presents prioritized list of compromised hosts
- Retroactively scans 7 days of logs each time to find previously infected hosts too

FortiAnalyzer provides powerful integrated network visibility to rapidly pinpoint problems

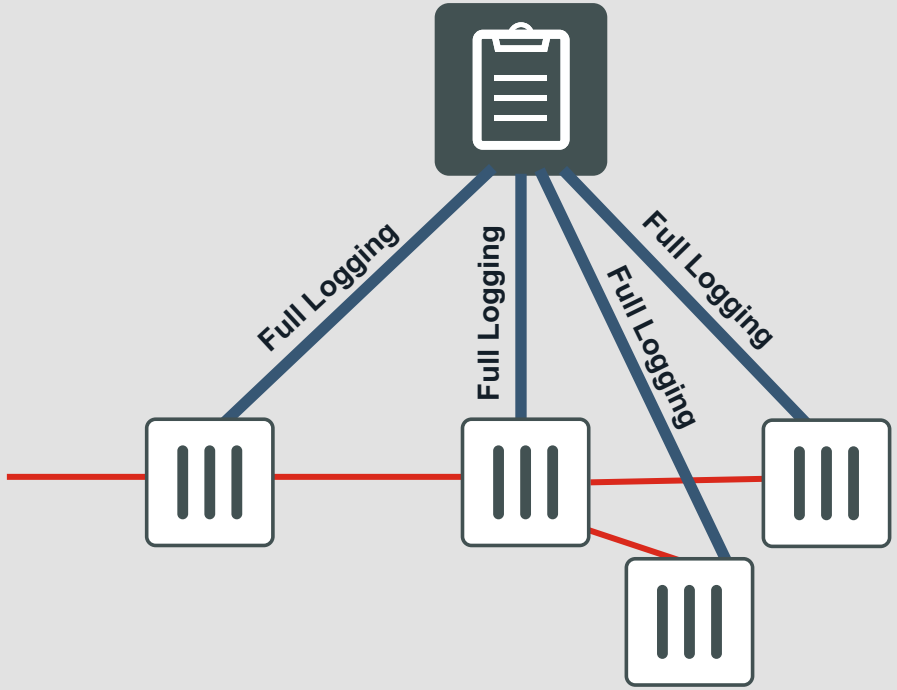


- Analytics with FortiView, Reports and Alerts
- Allows IT administrators to quickly identify and respond to network security threats across the network
- Available in Appliance, Virtual Machine and Cloud format
- FortiAnalyzer offers complete and deep visibility, situation awareness, real-time threat intelligence and actionable analytics for Fortinet's Security Fabric

FORTINET

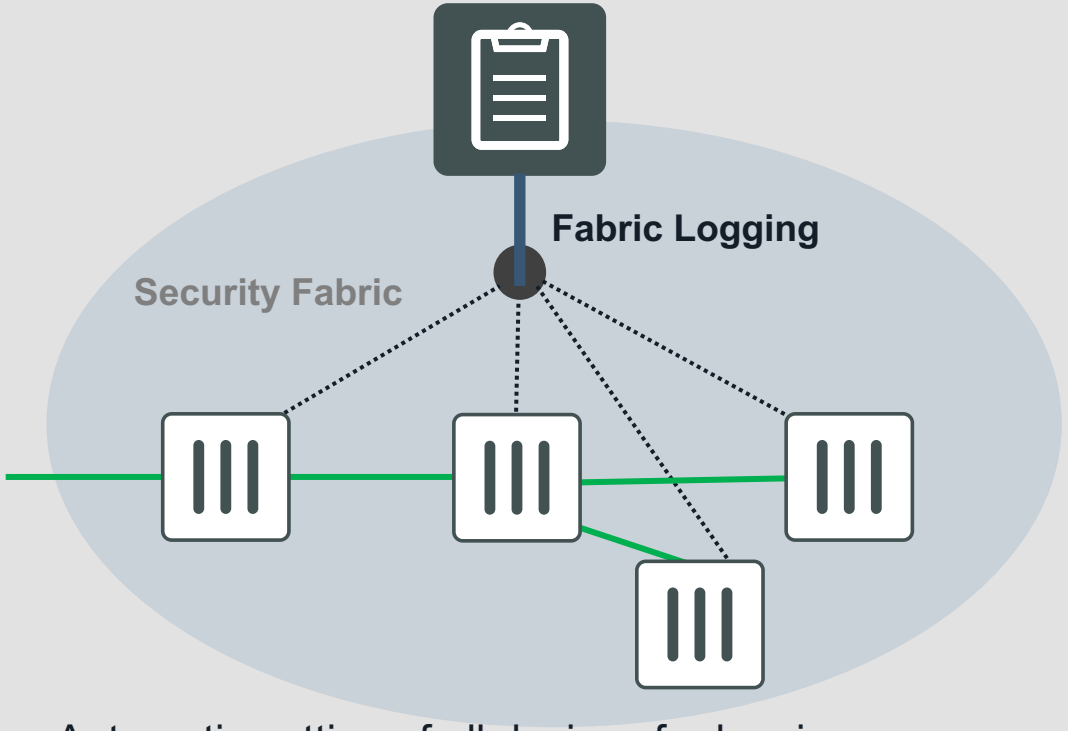
Coordinated Logging Provides Deep Visibility and Better Performance

Uncoordinated



- Manual setting for each device for logging
- Each device sends full logging to FortiAnalyzer

Coordinated



- Automatic setting of all devices for logging
- Topology aware – log only what's needed

Security Fabric – Topology Aware

Fabric Logging

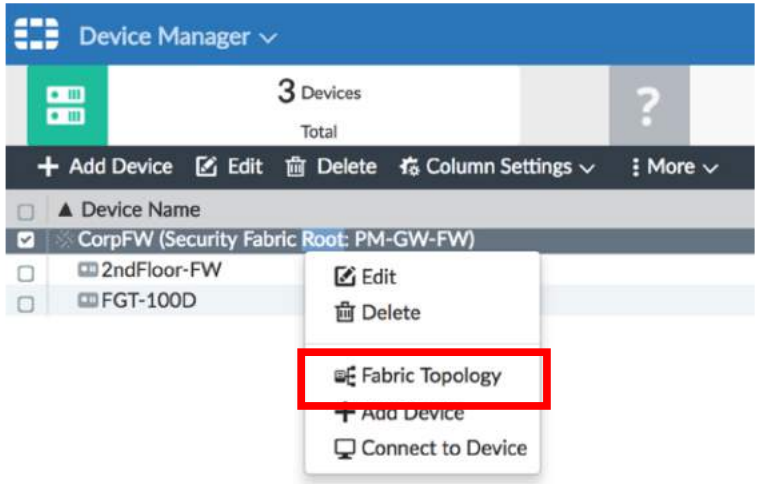
- Logs of a SF cluster stored together
- Fabric data exchange

Topology Learning

- Sync'd from root to FAZ
- Dedicated FGT ⇔ FAZ connection
- Logging & Device topology

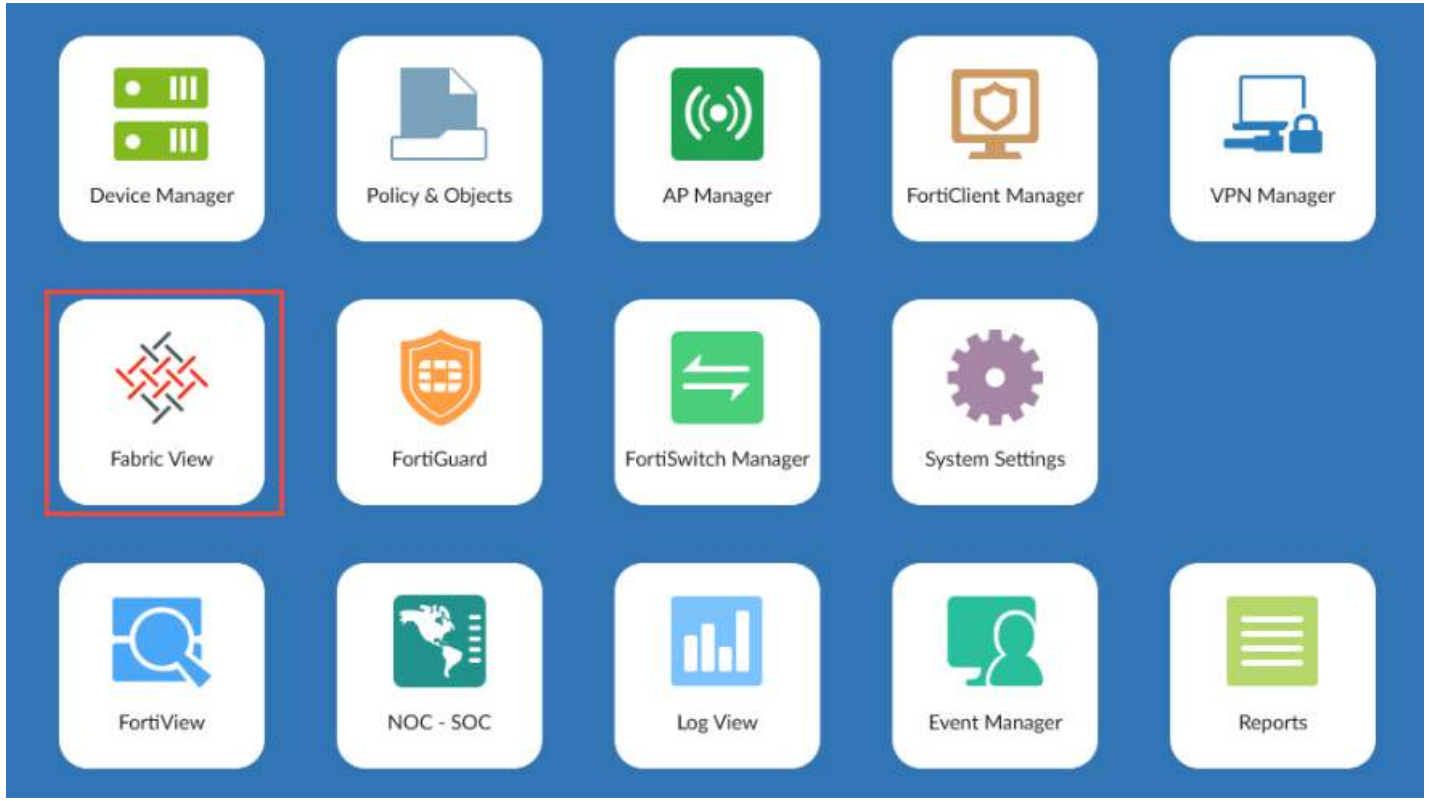
Collector/Analyzer

- Topology info sync'd

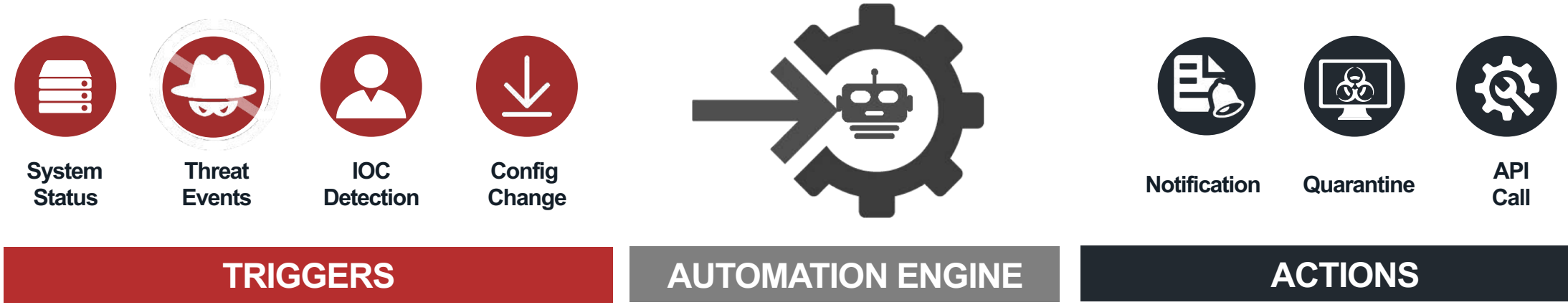


Fabric View

- Fabric View
  - Enables you to view Security Fabric ratings
  - Can view ratings for multiple Security Fabric groups
  - Security Ratings are part of the Risk Scoring and Assessment capability we will talk about shortly



Automation Ready: Automated Response



- Automated work flows (called stitches) use if/ then statements to cause FortiOS to automatically respond to an event in a pre-programmed way. Because this workflow is part of the security fabric you can set up if/then statements for any device in the Security Fabric.

FortiPresence

Tool für die WLAN Standortanalyse

LOCATION ANALYTICS

PRESENCE ANALYTICS

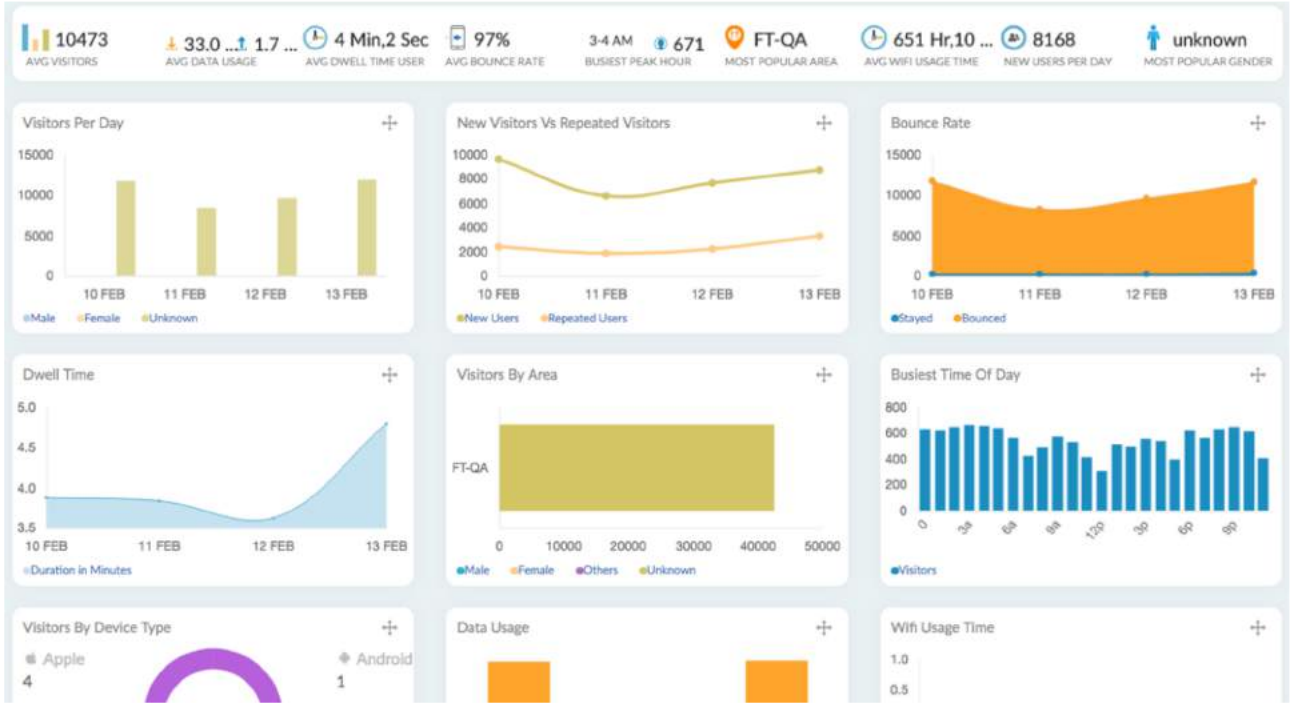
SOCIAL Wifi CAPTIVE PORTAL

CUSTOMIZED REPORTS

FORTINET

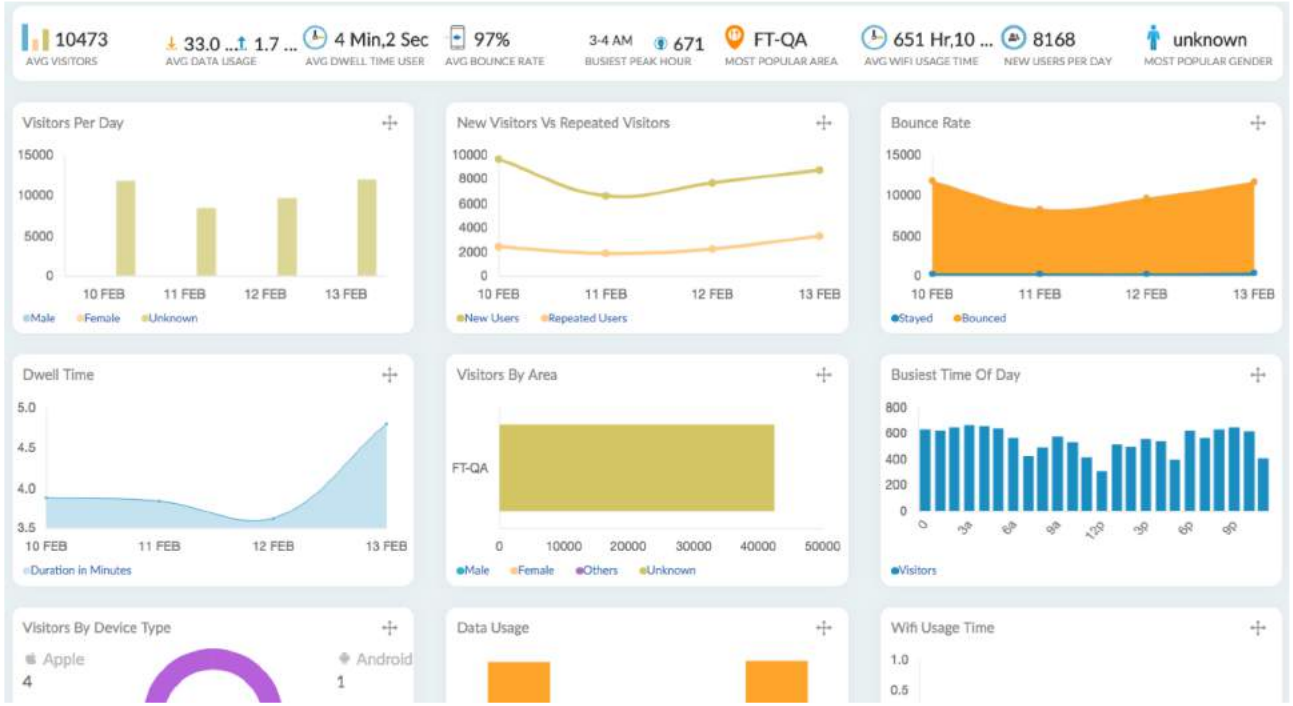
FortiPresence Lite (Free Offering)

- **Features:**
  - Locationing
  - Demographics (requires Captive Portal login)
- **Limitations:**
  - 5 sites per account
  - Only 7 days data stored
- **Not available:**
  - E-mail & SMS Marketing
  - CRM Integration



FortiPresence (New Paid Tier)

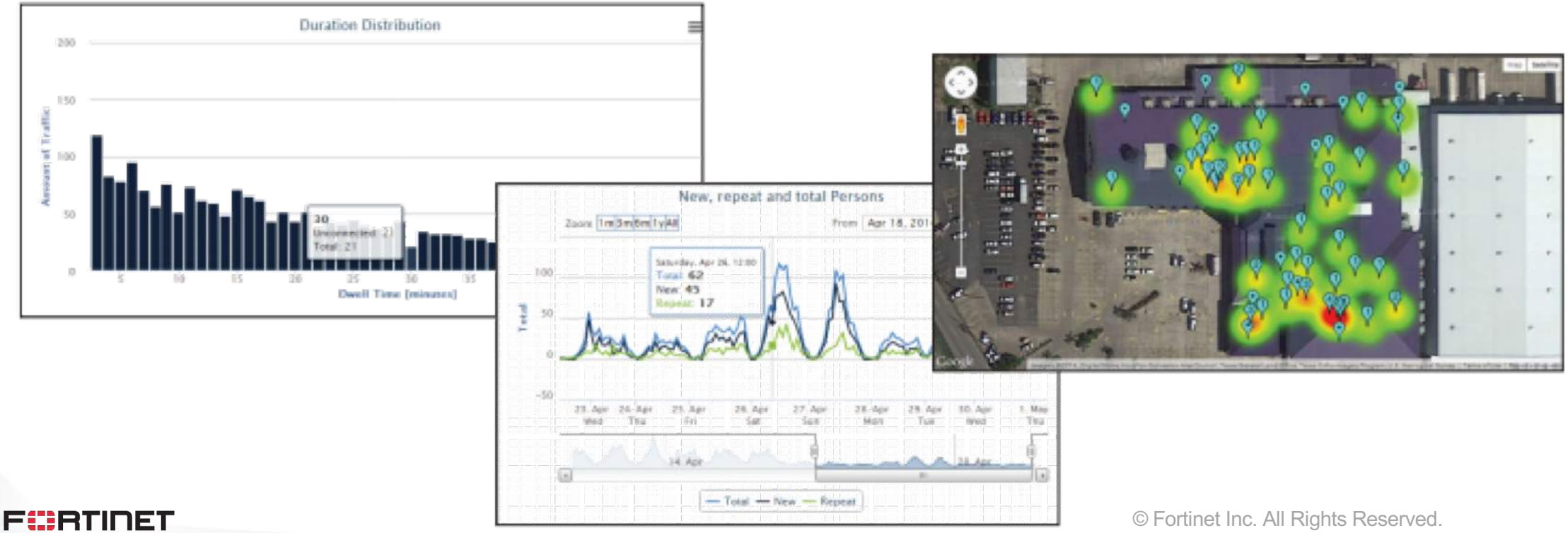
- **Capability Increases:**
  - Unlimited sites per account
  - Up to 365 days data stored
  - Unlimited Captive Portal connections
  - Reporting by Site or across Deployment



- **License details:**
  - Licenses are on a per-AP basis
  - Paid tier access included in FortiAP Cloud licenses

FortiPresence PRO

- **Additionally offers:**
  - Marketing Integration
  - 1 year historical storage




FORTINET