

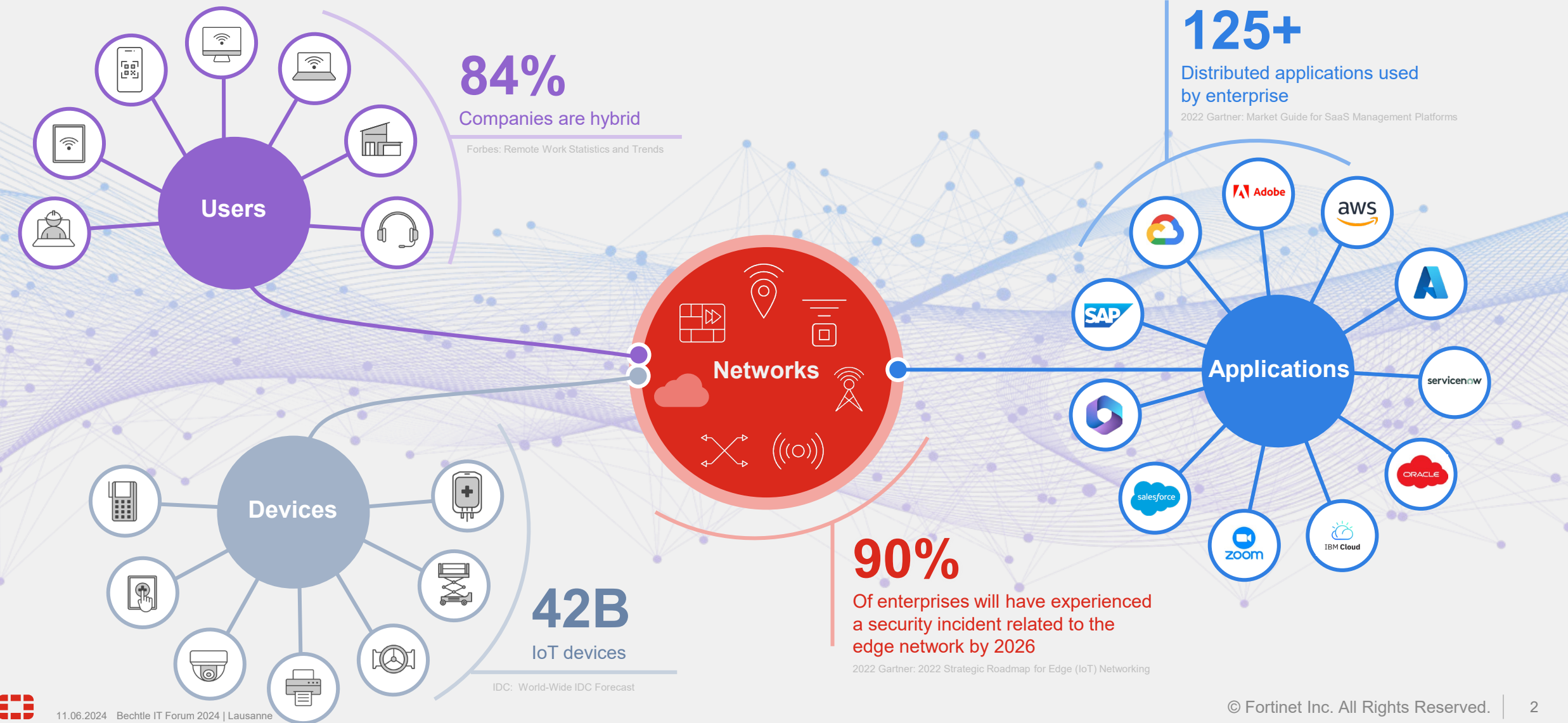
# Construire des fondations de cybersécurité solides, tout en simplifiant vos opérations de Sécurité avec Fortinet.

Bechtle IT Forum | 11.06.2024 | SwissTech Convention Center

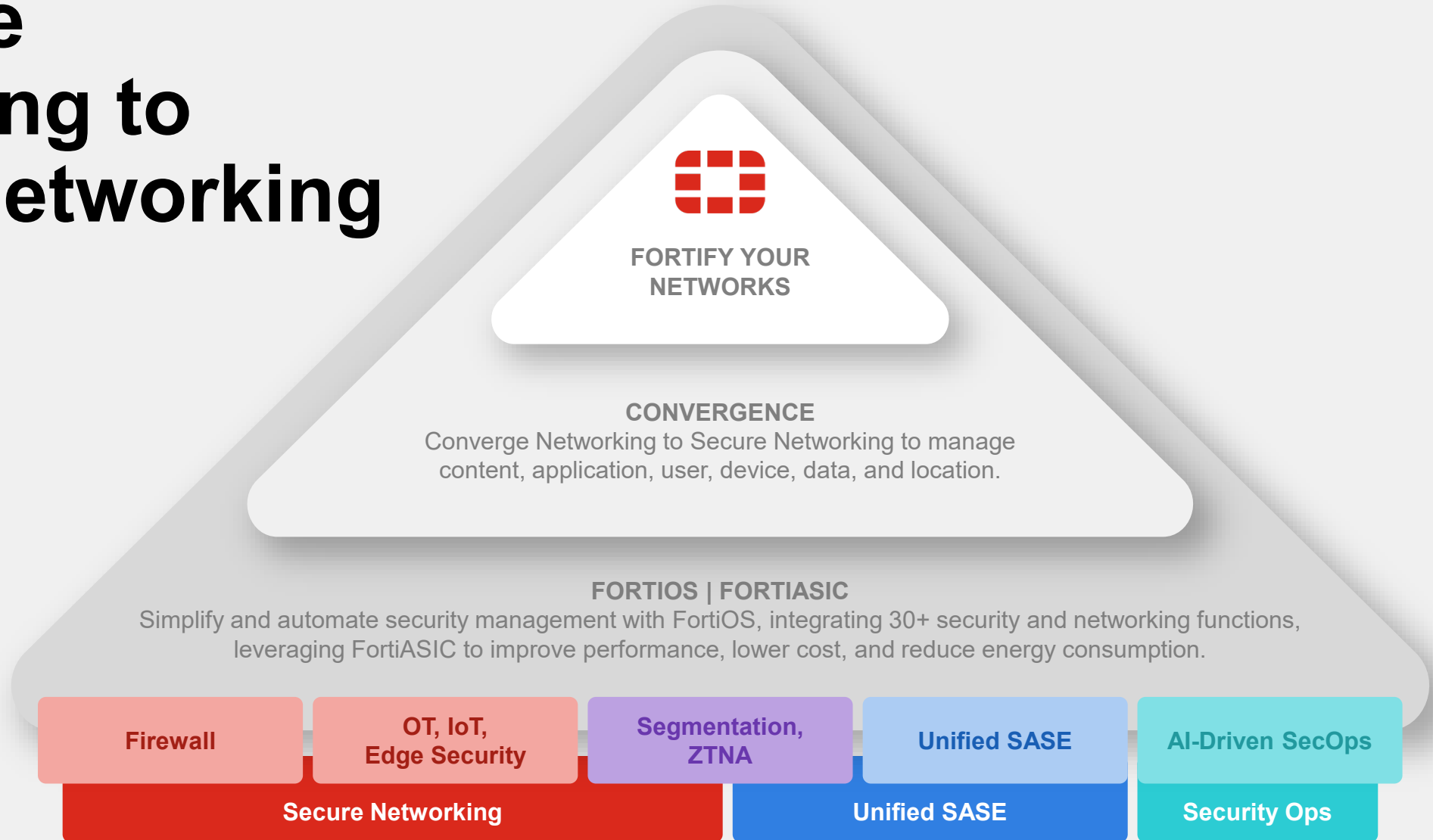
Sébastien Beal, Manager System Engineering, CISSP – Fortinet  
Yoan Cousin, Advanced Team & Network Operation Team Leader, Bechtle Suisse



# Traditional Networking is Built on Trusting Everyone and Connecting Everything

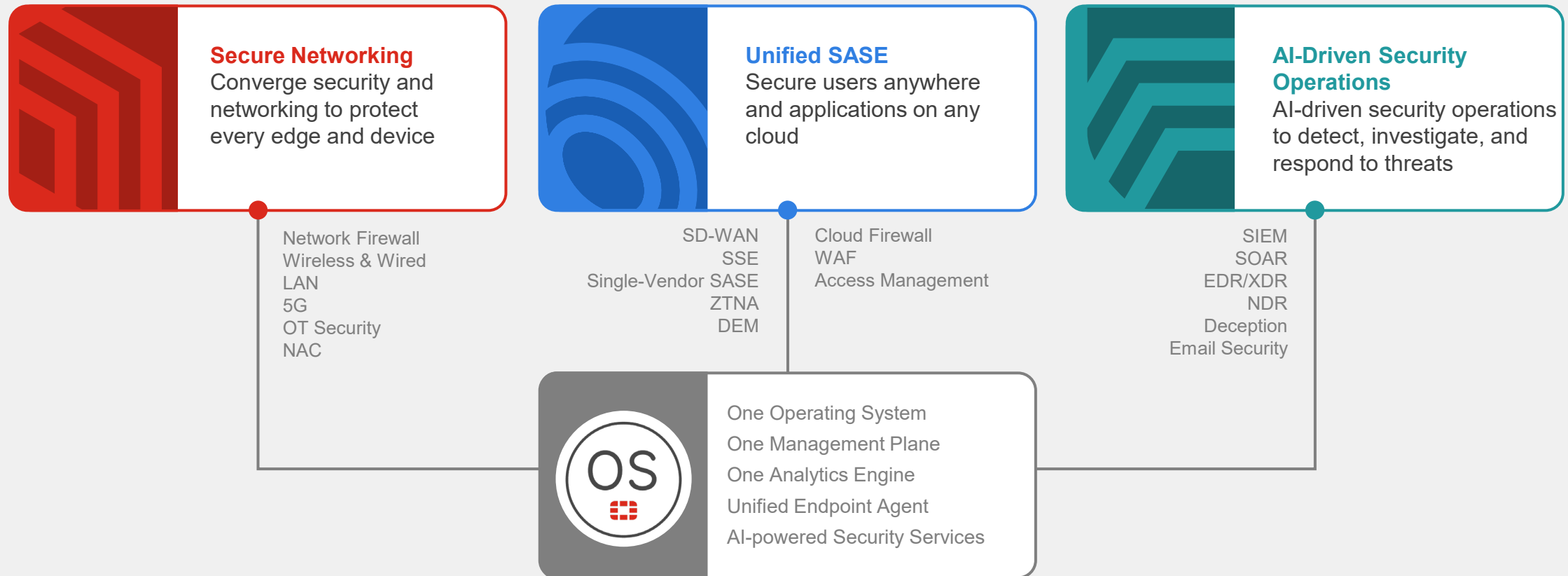


# Converge Networking to Secure Networking



# The Fortinet Security Fabric Platform

The Only Cybersecurity Platform Delivering Unprecedented Integration and Automation



# The Only Cybersecurity Platform Delivering Unprecedented Integration and Automation



## ONE OPERATING SYSTEM



### FortiOS

Network and Cloud Firewall, SD-WAN, Secure WLAN/LAN, Single-Vendor SASE, and SSE

## ONE MANAGEMENT PLANE



### FortiManager

Unified policies for hybrid environments

## ONE ANALYTICS ENGINE



### FortiAnalyzer

Data lake for security operations

## UNIFIED ENDPOINT AGENT



### FortiClient

EPP, EDR, SASE, ZTNA

## AI-POWERED SECURITY SERVICES AND TOOLS



### FortiAI

Generative AI across the platform



### FortiGuard Labs

AI-Driven Security Services



### FortiAI Ops

Self-healing networks end-to-end



# Extend Protection Across the Entire Network with Unified Security



## Secure Networking

### Hybrid Mesh Firewall



Evolution of NGFW to Hybrid Mesh Firewall for unified management that simplifies operations, reduces risk, and ensures compliance at scale



Accelerated ASIC



Branch



Campus



Data Center



Cloud Native



Virtual



FWaaS

### Secure Connectivity



FortiLink converges networking and security for secure WLAN/LAN equipment to provide security and automation, improve visibility and control, and reduce TCO.



FortiLink



FortiAP



FortiSwitch



FortiExtender



FortiNAC

### AI-Driven Technologies



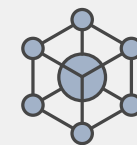
FortiOS



FortiGuard Labs

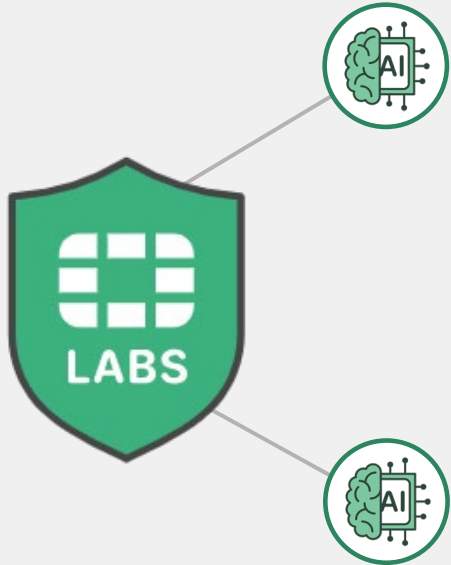


AI for Networking (AIOPS)



Unified Management

# FortiGuard AI-Powered Security Services

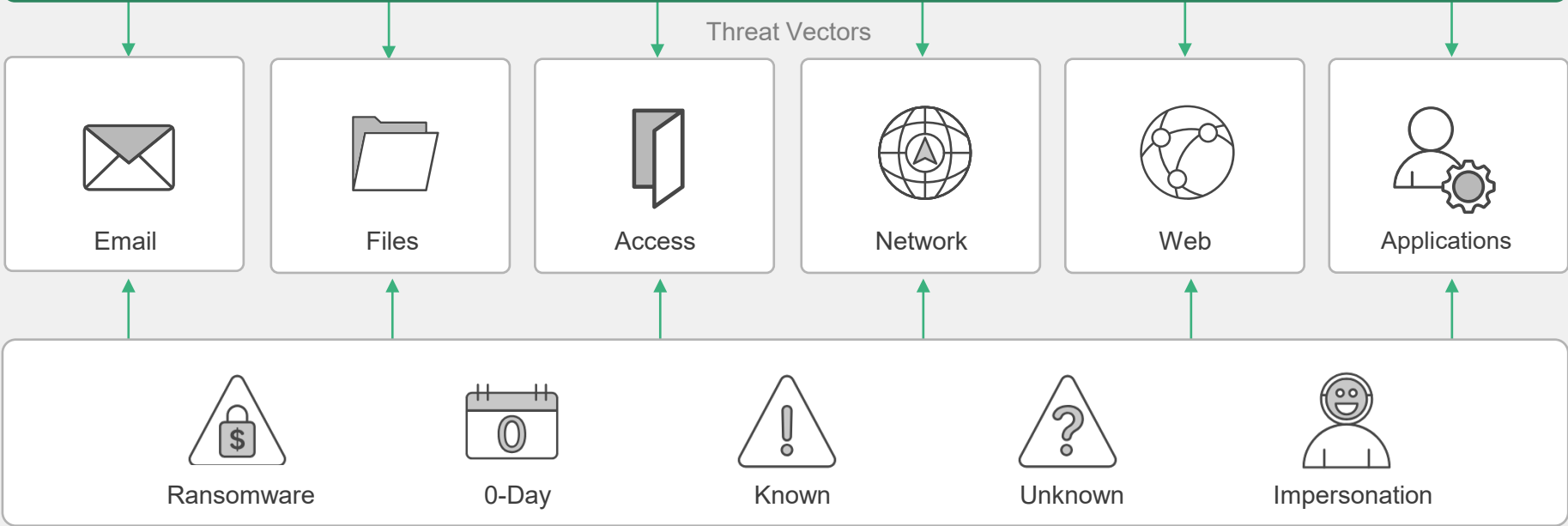


## FortiGuard AI-powered Security Services

AV IL MPS DLP IPS OT ATTK SRFC DNS URL BOT IL CASB APP CTRL ANTI-SPAM

Integrated into FortiGate NGFWs, and Across Fortinet's Broad Portfolio

## Protect Against Known, Unknown, Zero-Day and Emerging AI-based Threats



Firewall

OT, IoT,  
Edge Security

Segmentation,  
ZTNA

Unified SASE

AI-Driven SecOps

**FORTIOS | FORTIASIC**

Simplify and automate security management with FortiOS, integrating 30+ security and networking functions, leveraging FortiASIC to improve performance, lower cost, and reduce energy consumption.

**CONVERGENCE**

Converge Networking to Secure Networking to manage content, application, user, device, data, and location.

**FORTIFY YOUR NETWORKS**



# Integrated Solutions that Solve Customer Problems



# Technology Advancements Enable **Refresh** and **Replace** Opportunities



## Better Performance

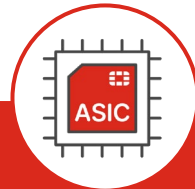


Security Compute Rating

**7x** better than the competition

201G Security Compute Rating

## Better Efficiency



Security Compute Rating - Energy

**29x** better than the competition

90G Security Compute Rating

## Better Security



FortiGuard Labs

**99.88%** security effectiveness

Competitors: <80% security effectiveness

CyberRatings.org Security Effectiveness Report

Data Center Perimeter Firewall



Core Segmentation Firewall



Distributed Firewall



Firewall As a Service



OT Firewall



Cloud Native Firewall



Virtual Machine Firewall



Container Firewall



Expand to **Hybrid Mesh Firewall**

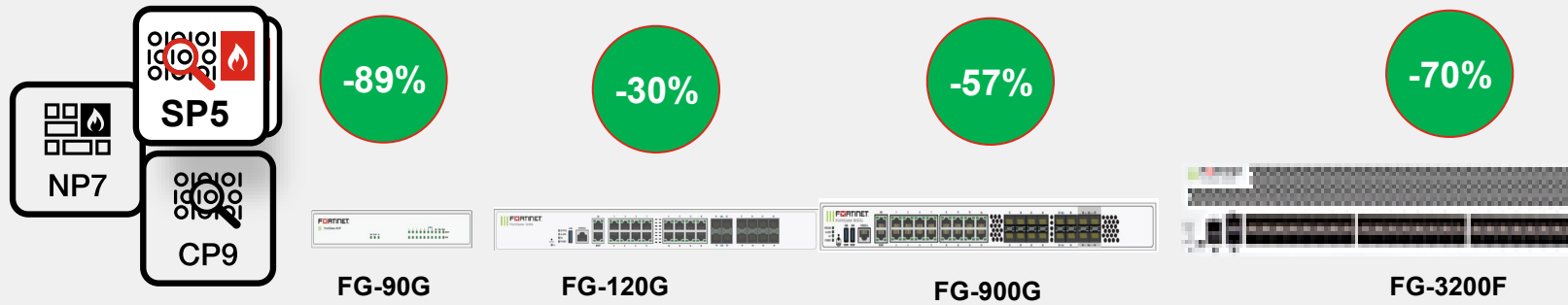


# 2023 Reduced 62% Power Consumption for a Cleaner Future



Continuous Improvement on Energy Consumption Across FortiGate Series Generations

Advanced Threat Protection with Energy Saving



## Key Benefits

Environment Friendly

Cleaner future with most efficient energy consumption

FG Models (Series F vs E) 2022	% saving Power Consumption	% saving Heat Dissipation
FortiGate-90G	-89%	-87%
FortiGate-120G	-30%	-29%
FortiGate-900G	-57%	-57%
FortiGate-3200F	-70%	-70%
<b>Average</b>	<b>-62%</b>	<b>-61%</b>

- Improvements in maximum power consumption use in top 4 products sold (FortiGate G/F Series versus FortiGate E/D Series) in 2023.



# FortiAnalyzer Benefits

Centralized, Automated & Augmented



## Quick Start Your SecOps

Keep pace with attackers by simplifying & amplifying security operations without adding complexity



## Increase Operational Effectiveness

Manage risks efficiently while maintaining agility and responsiveness



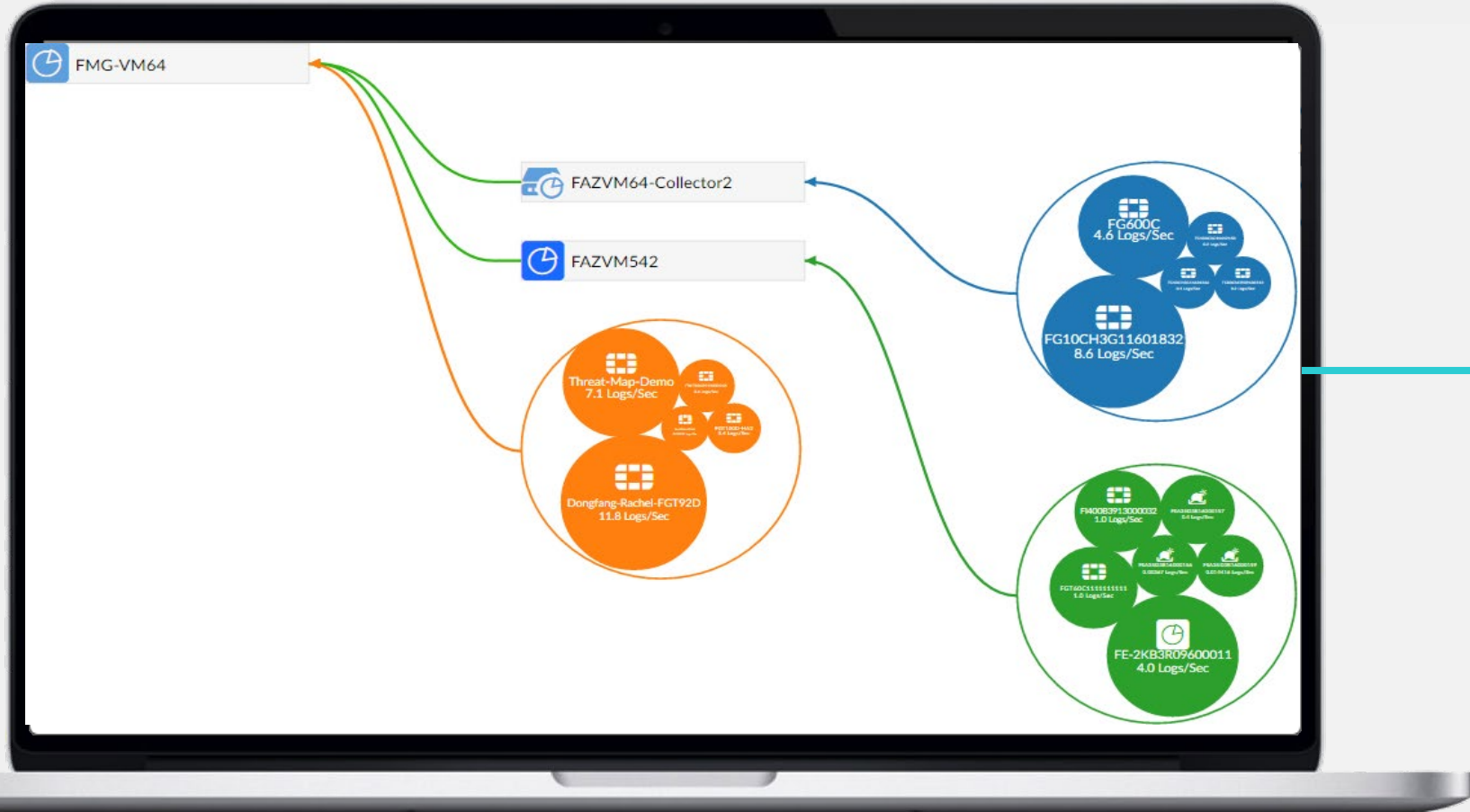
## Strengthen Security Posture

Constrict the threat actors window of opportunities with layers of centralized Automation & Augmentation

# What Centralized Analytics, Automation, & AI looks like



# Single Pane for Visibility



**Topology** of the Fortinet security fabric from a single console

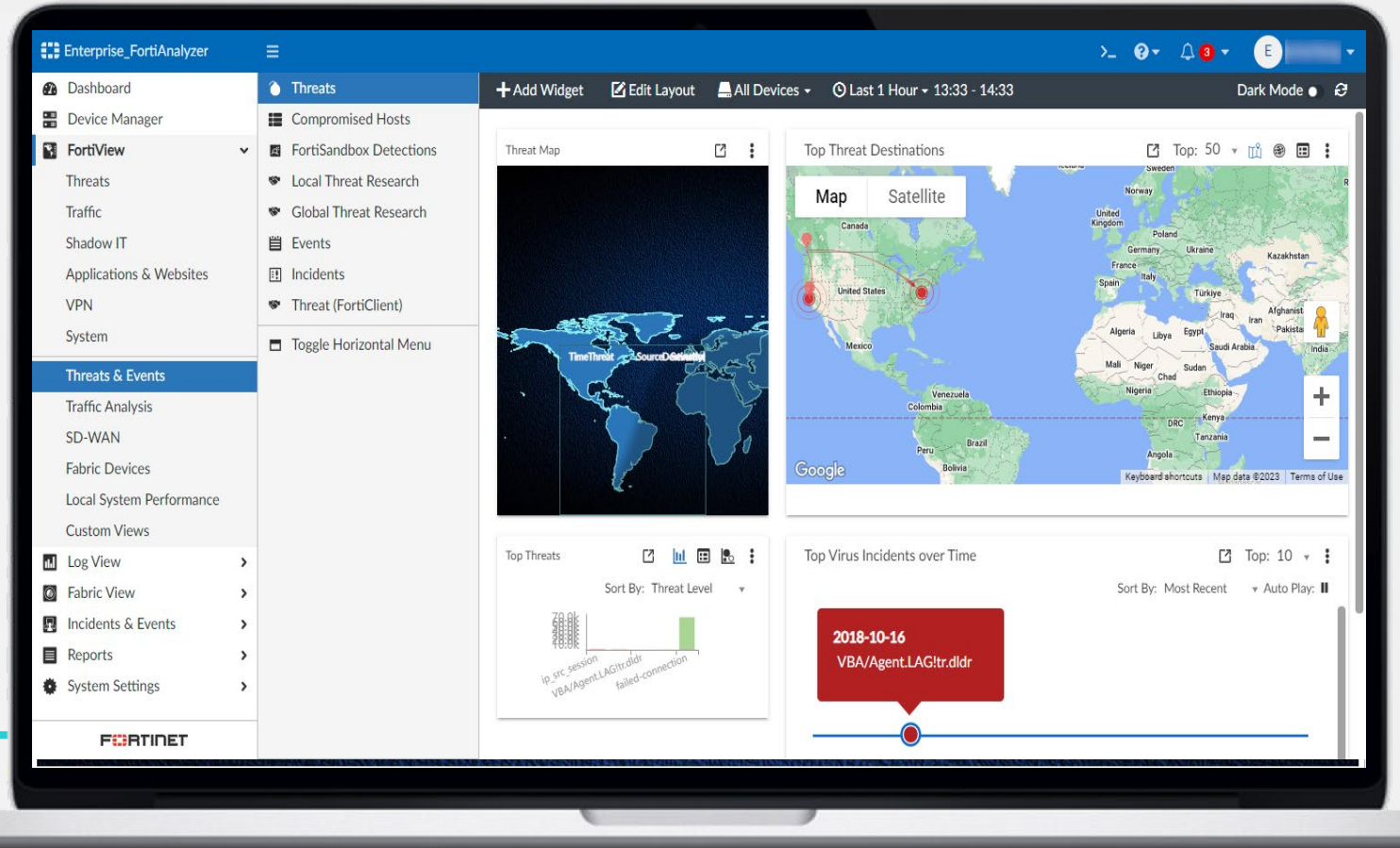
# FortiAnalyzer Threat Monitoring with FortiGuard Indicators of Compromise



Benefit from intuitive monitoring & detection of compromised hosts with real-time context of network activity, risks, vulnerabilities, attack attempts, and **\*FortiGuard indicators of compromise (IOC)**



- IOC Threat scoring & prioritization
- Drill down threat visualizations
- Real-time & historic IOC rescans
- Automatic FortiGate response actions on FortiAnalyzer threat detections



[Search the latest FortiGuard Labs IOCs](#)

\*FortiGuard IOC for FortiAnalyzer appliances requires Hardware Enterprise Protection or al la carte SKUs



# Event & Incident Management

**Incident ID:** IN00002422 (High) | **Status:** Uncategorized, Not Assigned, New | **Created on:** 2020-01-31 18:26:18-08:00 | **Last Modified on:** N/A

**Affected Endpoint/User:**  
Topology: FGVM04TM19000838  
Addresses: MAC: 00:0c:29:6e:9e:16, IP: 192.168.22.5/32  
Operating System: Windows 7  
Status: Registered - Online  
Online Interfaces: Guest Network (vsw.port5)  
Last Seen: Now

**Executed Playbooks:**

PLAYBOOK	STATUS
Compromised Host Incident	Running
Run AV Scan	Success
Run Vulnerability Scan	Success
Get process & connection List	Success
Get Vulnerabilities	Success
Update C&C Blacklist on Edge FortiGate	Success
Quarantine Endpoint	Queued...

**Audit History:** NOW

- VULNERABILITY List Attached (2019.06.28.09:49:54)
- REPORT ATTACHED (2019.06.28.09:49:54)
- EVENT ATTACHED (2019.06.28.09:49:54)
- PROCESS LIST REQUESTED (2019.06.28.09:49:54)
- VULNERABILITY SCAN REQUESTED (2019.06.28.09:49:54)
- AV SCAN REQUESTED (2019.06.28.09:49:54)
- LOOKING UP EVENTS (2019.06.28.09:49:54)
- REPORT SCHEDULED (2019.06.28.09:49:54)
- EVENT ATTACHED (2019.06.28.09:49:54)
- INCIDENT CREATED (2019.06.28.09:49:54)

**Timeline:** From 2020-01-30 17:11:03 To 2020-01-31 18:25:34 (Total 839 Events)

#	Event	Count	Severity	Additional Info	Tags
1	Compromised host detected	1	critical	infected-ip: 103.226.154.43 :80, Traffic path: Shawn-FW-93-FCT (Policy ID:3) port3	IP, C&C
2	Compromised host detected	1	critical	infected-ip: 103.226.154.43 :80, Traffic path: Shawn-FW-93-FCT (Policy ID:3) port3	IP, C&C
3	Compromised host detected	1	critical	infected-ip: 103.226.154.43 :80, Traffic path: Shawn-FW-93-FCT (Policy ID:3) port3	IP, C&C
4	Compromised host detected	1	critical	infected-ip: 103.226.154.43 :80, Traffic path: Shawn-FW-93-FCT (Policy ID:3) port3	IP, C&C
5	Web request to Malicious Websites de	1	high		Risky URL
6	DNS traffic to Botnet C&C daicoaero.f	10	critical		IP, C&C
7	Malware VBA/Agent.LAG/tr.dldr down	2	high		Malware
8	Traffic anomaly: icmp_sweep blocked	5	critical		IP, C&C

**Streamlined lifecycle management with incidents automatically showing affected assets, endpoints, users, and timelines, simplifying complex investigations**

- Easily investigate suspicious traffic patterns and employ filters in predefined or custom event handler



FortiAI

*“Analyze this incident and tell me what action to take”*

# FortiGuard Outbreak Detection Baked-in FortiAnalyzer



Integrated in the user experience, **FortiGuard Labs \*Outbreak detection** automatically alerts & downloads content packages for the latest malware detection, offering summaries and kill chain mapping.



- Filter & group alerts by date or severity
- FortiGuard Outbreak Detection content packs with event handlers, correlation rules, & reports
- Mapped to MITRE ATT&CK® Domain & ID

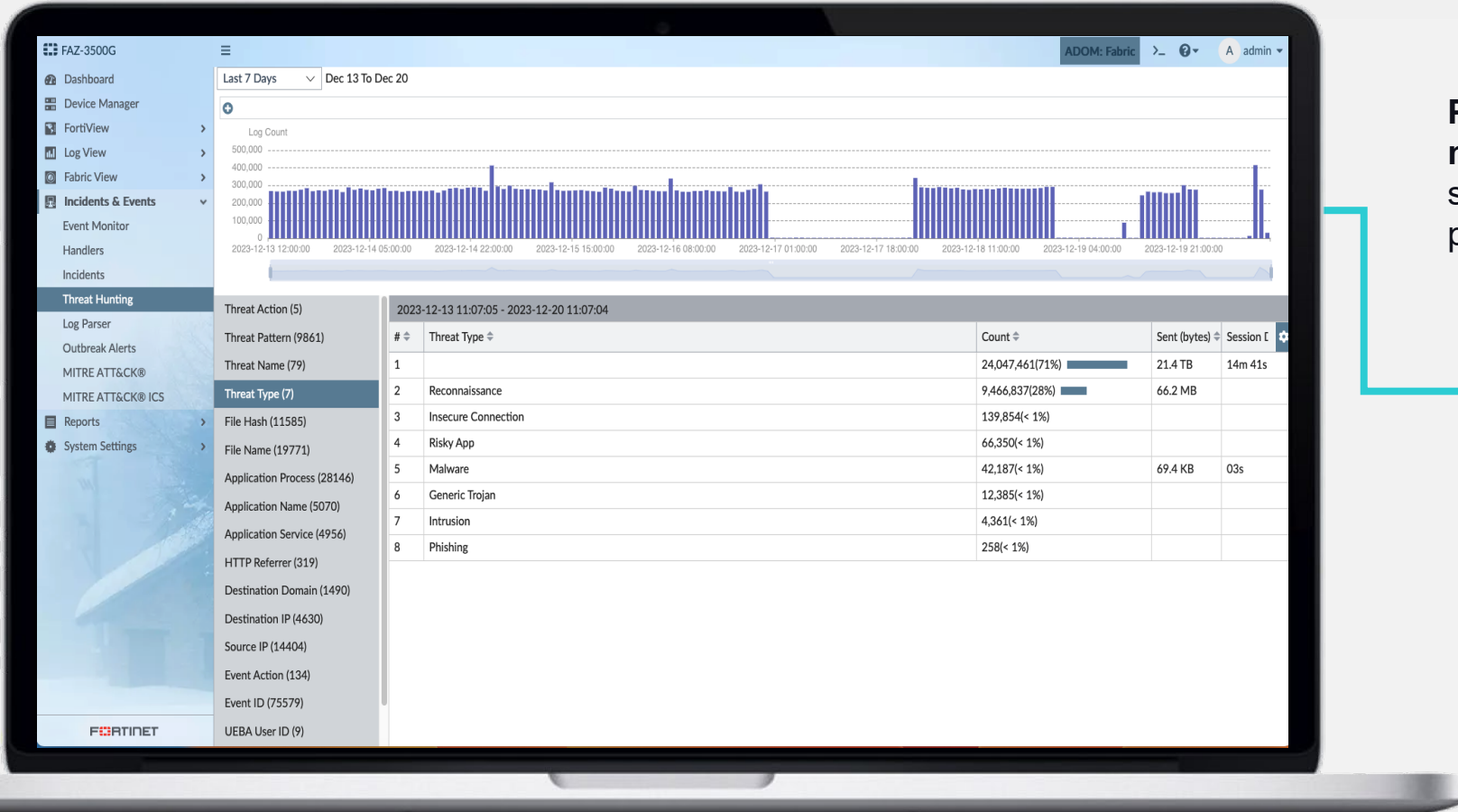


\*FortiGuard Outbreak Detection & IOC for FortiAnalyzer appliances requires Hardware Enterprise Protection or a la carte SKUs – [view the latest content packs](#)





# Become the Hunter with Analysis & SIEM Correlation



Proactively search for hidden threats within your network and unearth subtle signs of compromise, such as unusual endpoint behavior or network patterns indicative of an advanced persistent threat

# FortiAnalyzer Attack Surface Security Rating & Compliance



Continuously assess your security posture, including unpatched vulnerabilities & critical security settings. Benefit from real-time monitoring & analysis of your Security Fabric deployment with scores for posture, Fabric coverage, and optimization.

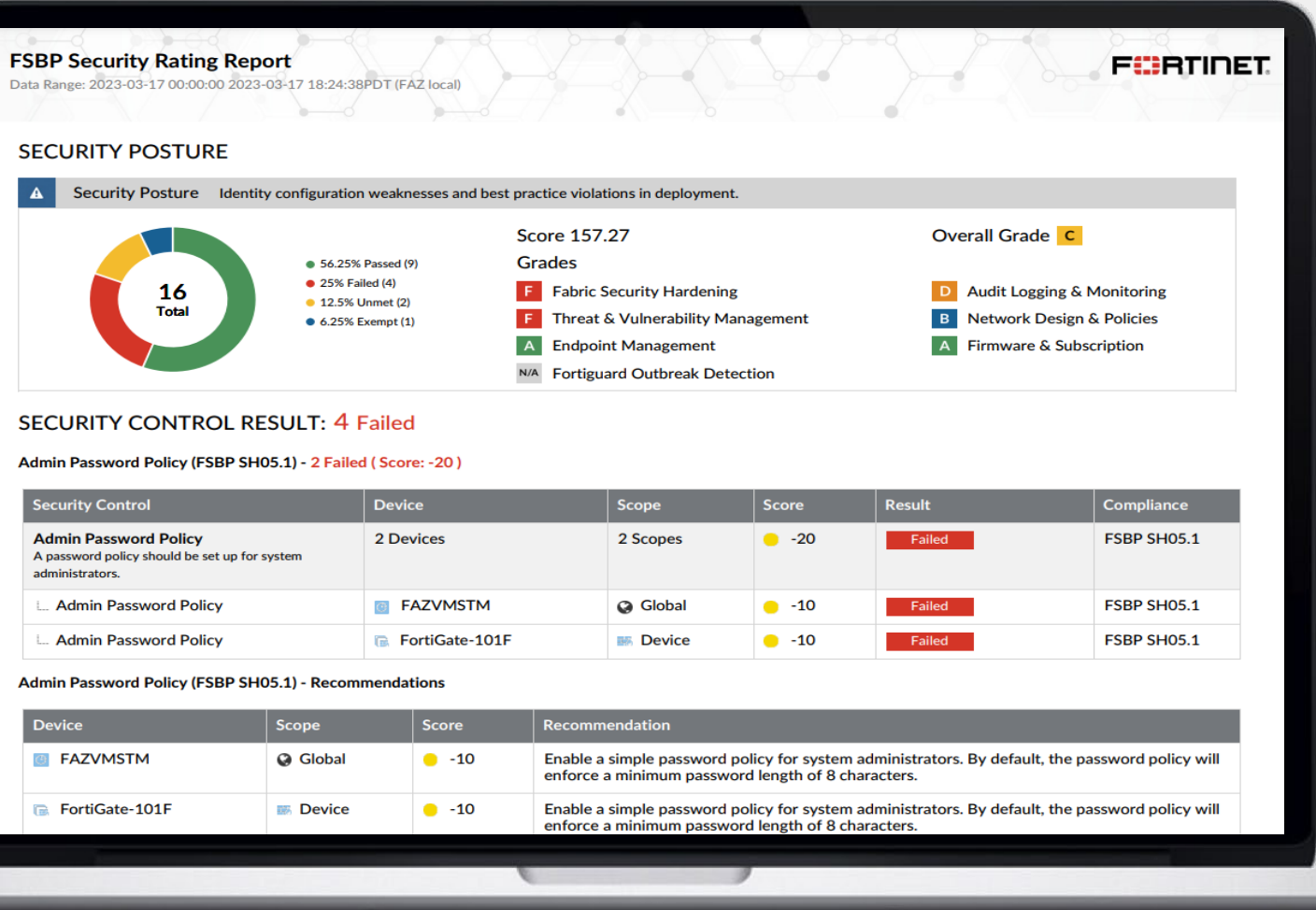
- Attack surface visualization
- Security Rating & best practice recommendations
- Industry specific compliance reporting
- Historical trend analysis



The screenshot displays the FortiAnalyzer Security fabric rating report for a device named FAZ-3500G. The interface includes a sidebar menu with options like Dashboard, Device Manager, FortiView, Threats, Traffic, Shadow IT, Applications & Websites, VPN, System, Threats & Events, Traffic Analysis, SD-WAN, Fabric Devices, Local System Performance, Custom Views, Log View, Fabric View, Incidents & Events, Reports, and System Settings. The main content area is titled "Security fabric rating report" and features a "Maturity Milestones" section with three levels: LEVEL 1: LIMITED (Protection against common external threats, 30221/30267 Completed), LEVEL 2: DEVELOPING (Control over what's on the network, and device lockdown, 48/55 Completed), and LEVEL 3: DEFINED (Heightened awareness of network activity, and ability to recover, 62/78 Completed). A note states: "To get a Security Rating all FortiGates in the Security Fabric must have a valid Security Rating License." Below this, it lists "The top 5 things to improve your score are" with five recommendations: 1. Define a role for the following interfaces (+120), 2. Upgrade firmware version to 7.0.5 (+75), 3. Upgrade firmware version following interfaces (+120), 4. Upgrade firmware version to 7.0.5 (+75), and 5. Upgrade firmware version. The bottom section shows a "Security fabric topology" diagram with nodes for NGFW\_PRI, Demo-FortimalGateway, LANEdge-CampusFW, and FortiAP\_ISFW-E connected by green lines.



# Maximize Your Investments with Best Practice Reporting

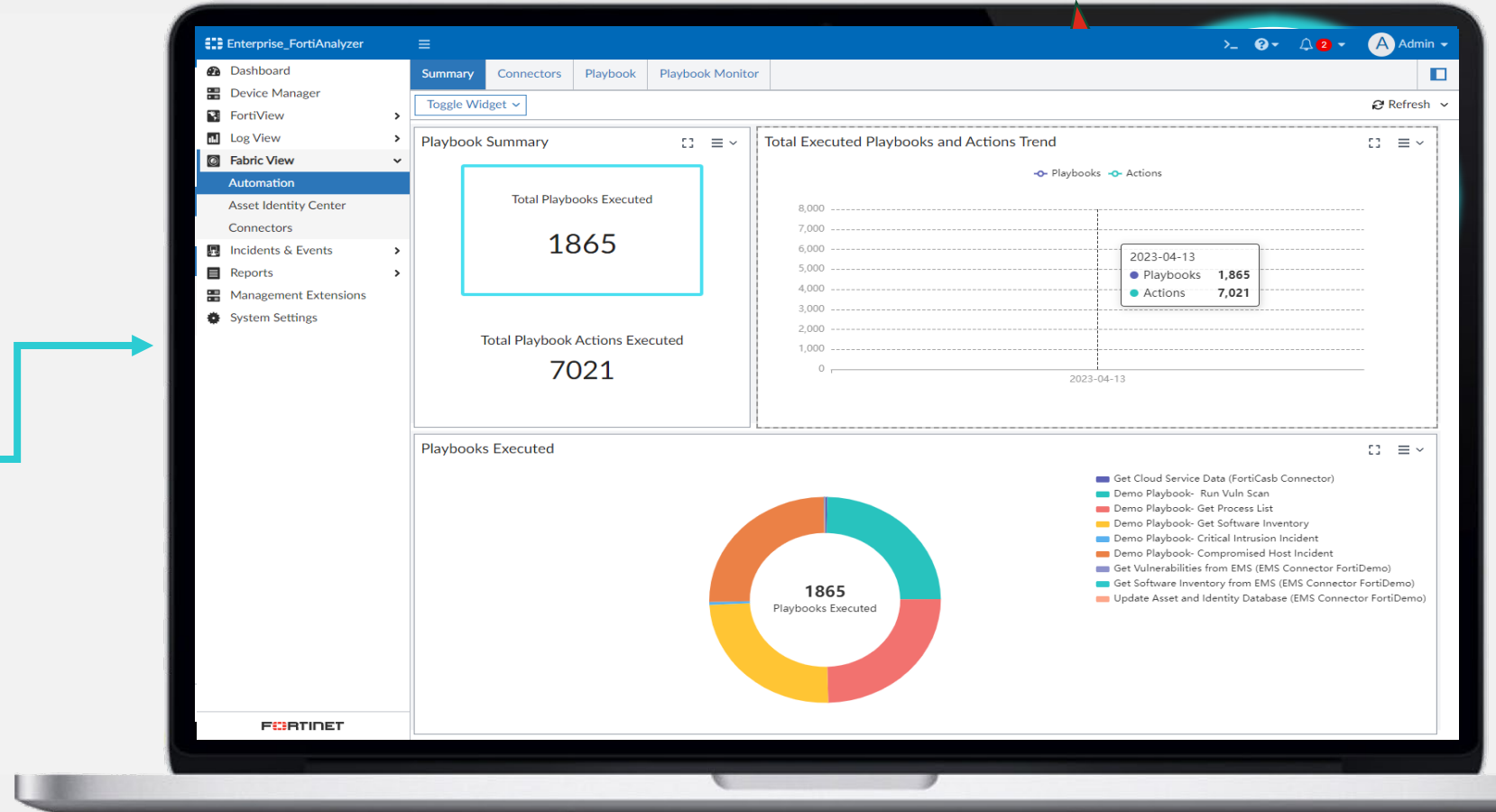


Maximize the deployed FortiGates in terms of Security Posture, Fabric Coverage, and Optimization. This report consolidates security ratings performed on fabric deployments.

# Connect, Automate, & Optimize

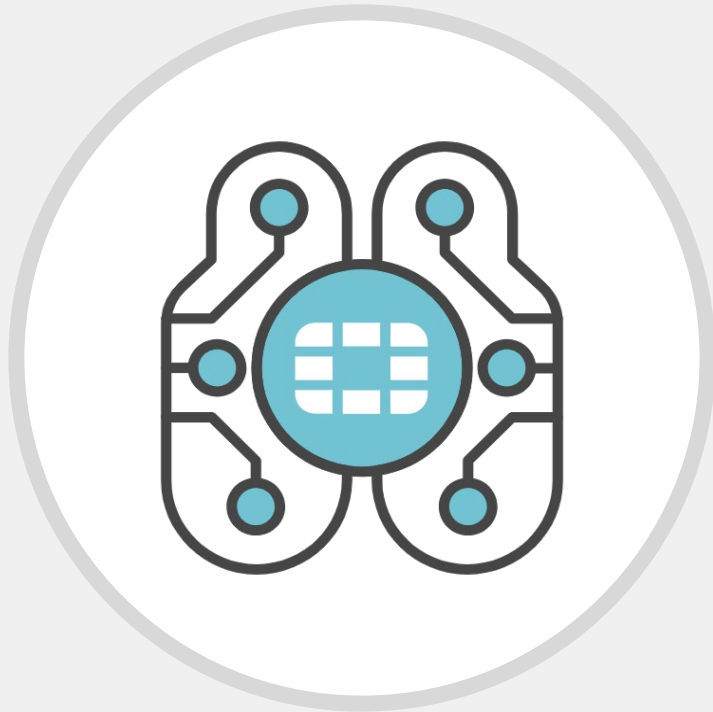


Speed incident analysis and response with one-click config connectors, continuously updated playbook templates, and countless event handlers



# Unify Management & Response with an AI Advantage

Analytics-powered log management for the Security Fabric



**Detect in Minutes  
Not Days**



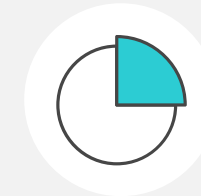
**Streamline, Reduce  
Your Workload**



**Eliminate  
Blind spots**



**Scale When You're  
Ready**



# Do More with Less

## Visibility

---

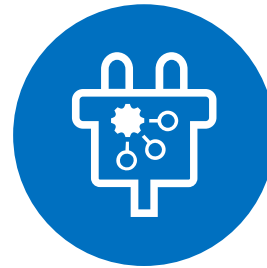


### Single Pane of Glass

Save time from having to access each system

## Better Security

---

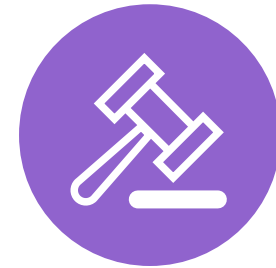


### Automation

Move away from whitelisting  
Detect Anomalies

## Compliance

---



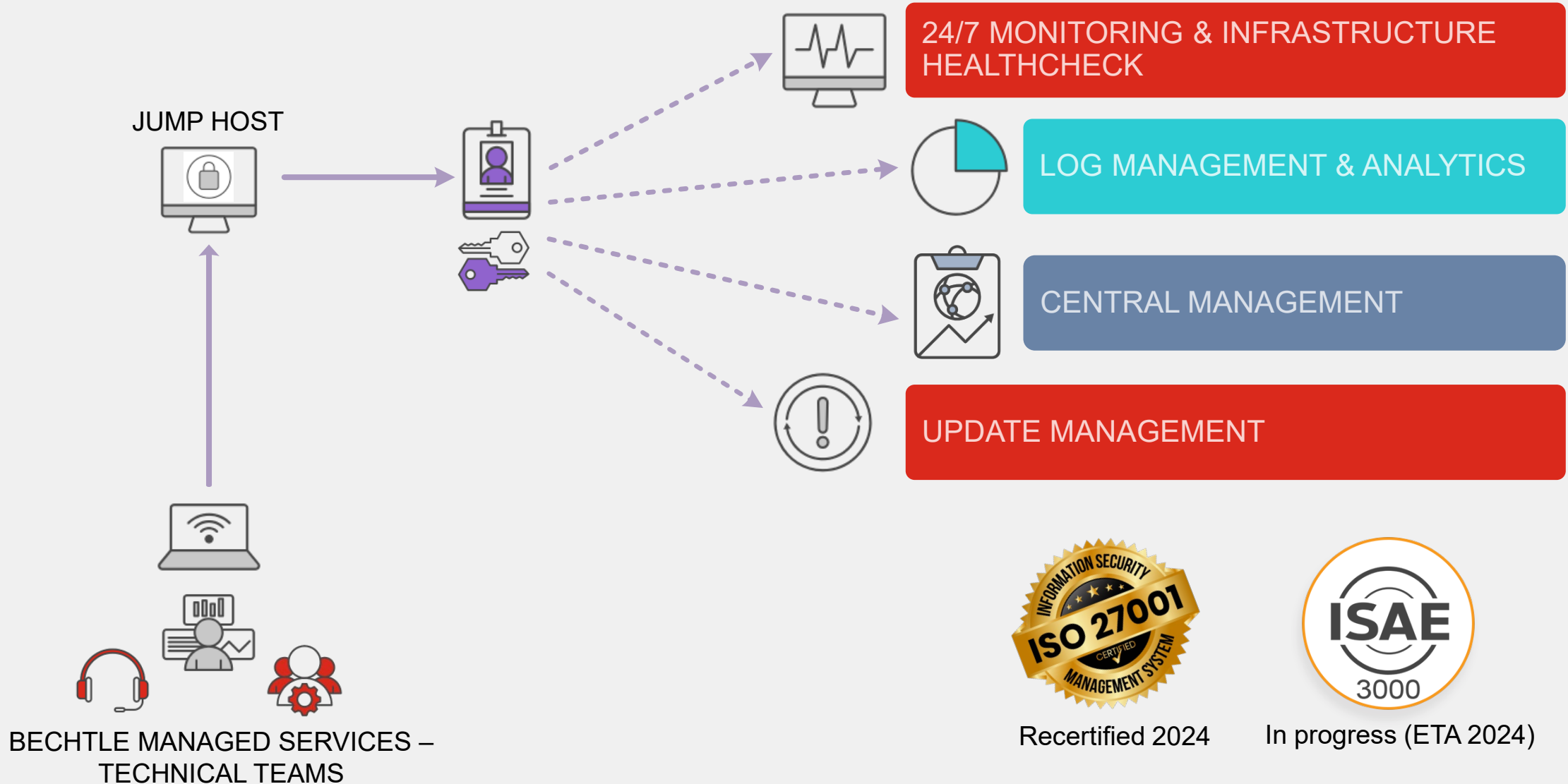
### Auditable

An audit heavy environment,  
made easy

# What Bechtle Security Managed Services looks like



# What about Bechtle Managed Services ?



Recertified 2024

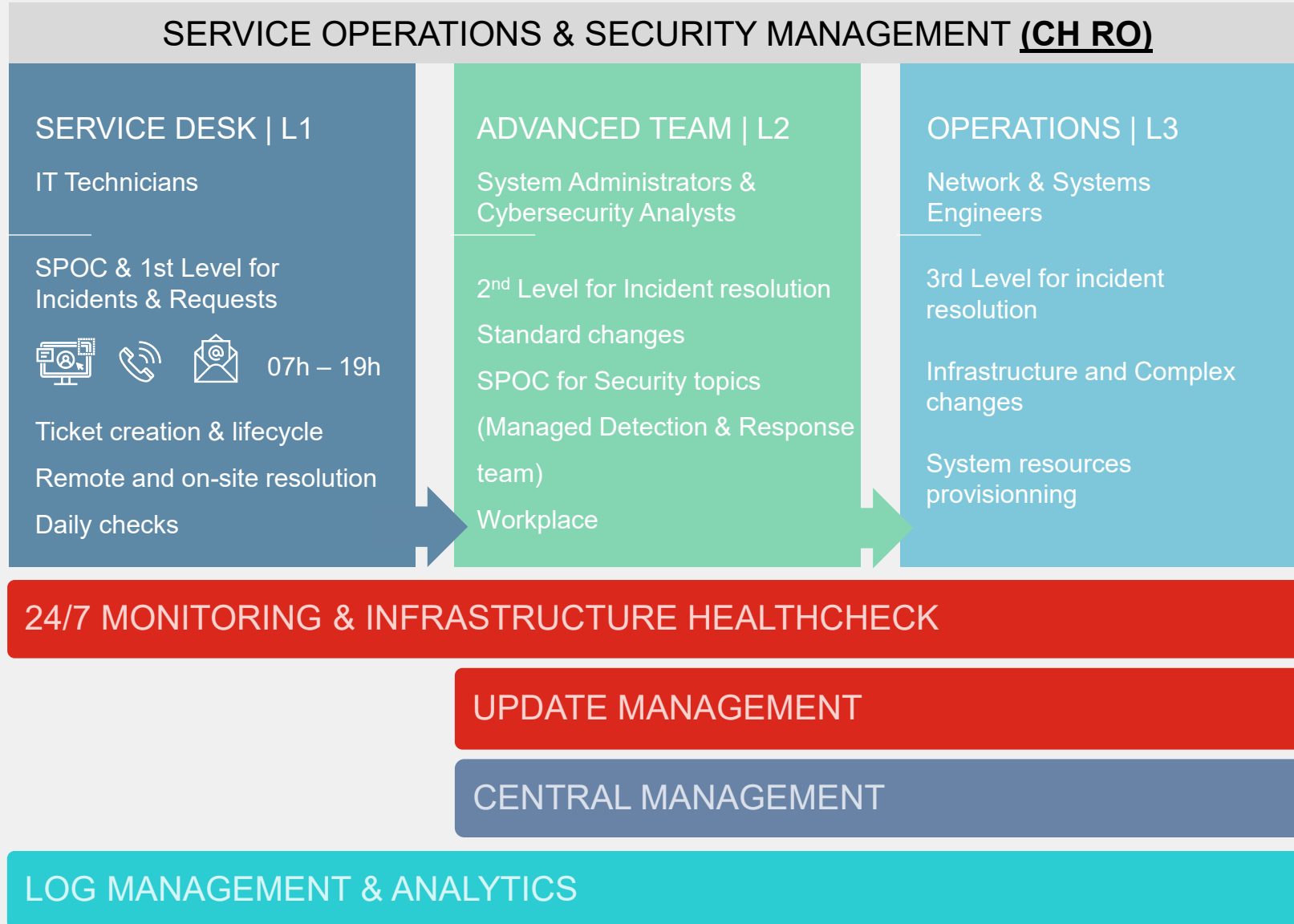


In progress (ETA 2024)





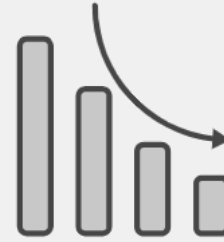
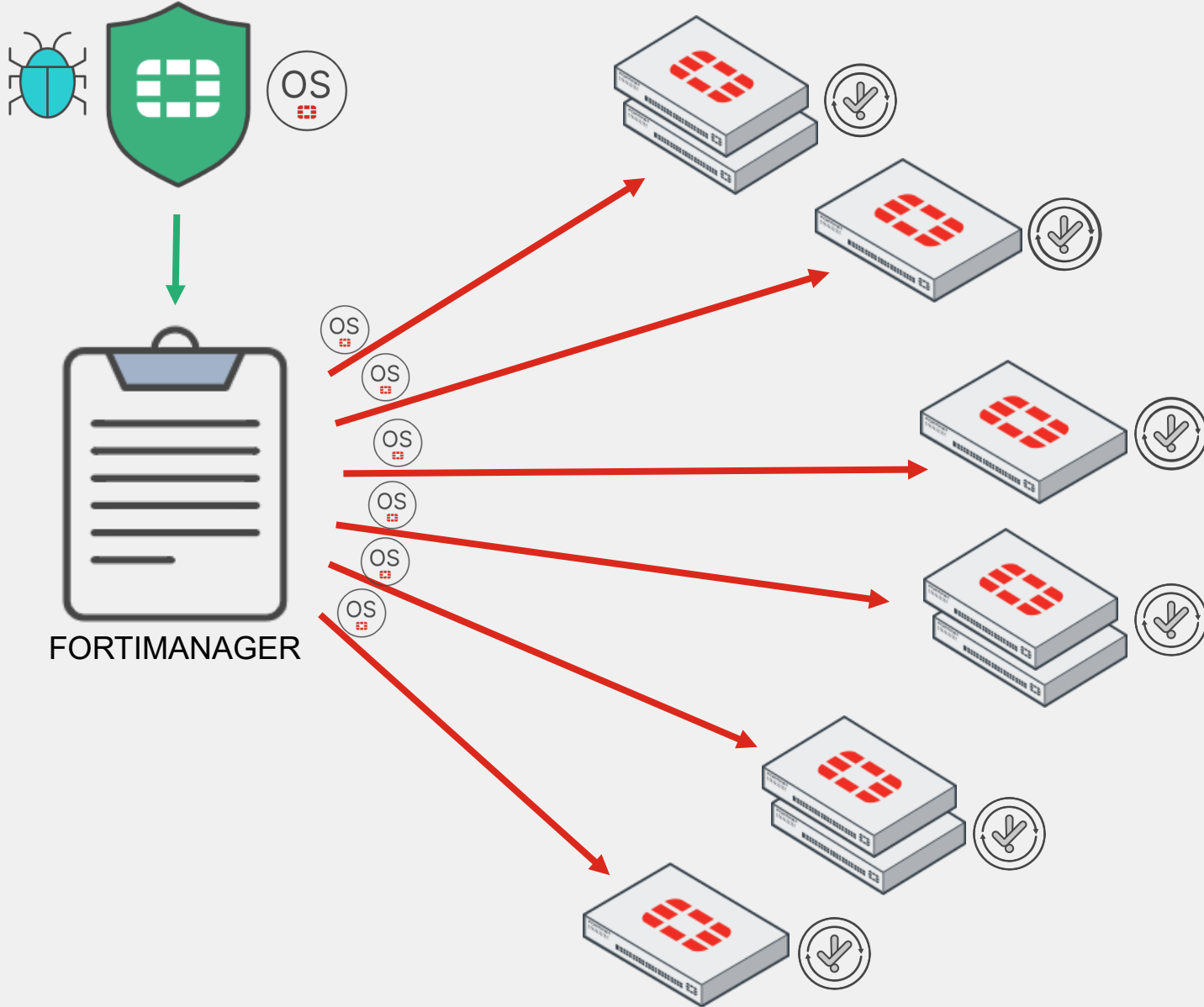
# What about Bechtle Managed Services ?



# How Fortinet helps Bechtle in operations simplification



# FortiManager – Update and Secure



REDUCE  
SECURITY RISK



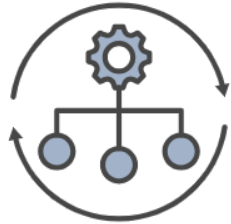
OPERATIONS  
OPTIMIZATION



REACTIVITY  
IMPROVMENT

## Orchestration

---



### Security Baseline

Deploy in a large scale Bechtel Managed Services integrations & Security baselines and improve them simply

## More efficient

---



### ... and more secure

Devices updated regularly & 0-Day breaches patched more quickly  
Safe update & rollback process

## Standardization

---



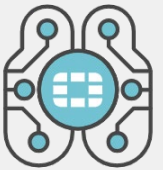
### ... and simplification

Help technical teams in their day-to-day operations and understanding to identify anomalies easily

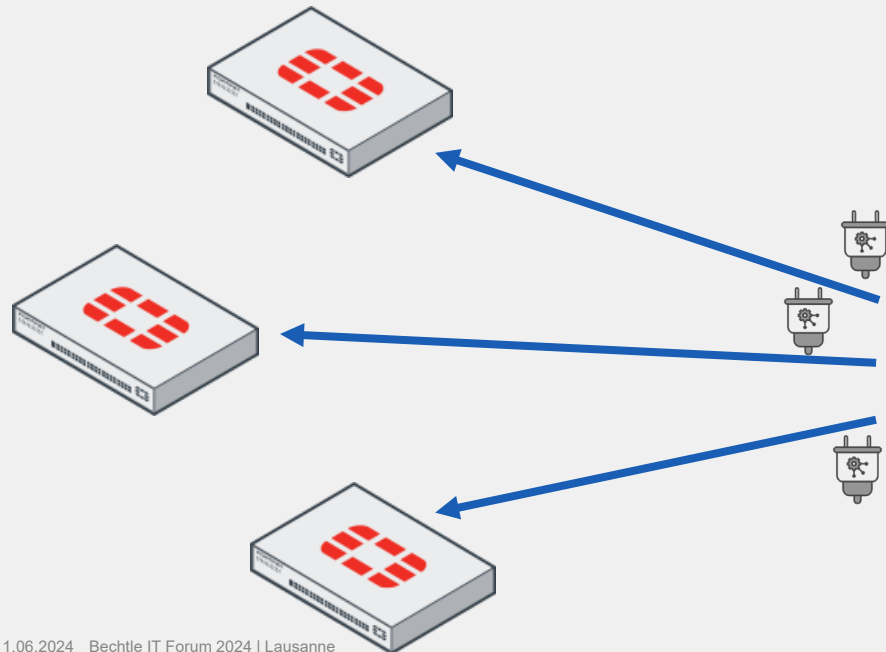
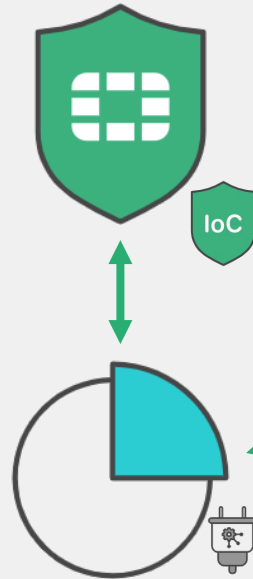
# FortiAnalyzer – Security through Visibility



Single platform for Alerting, Visibility & Remediation



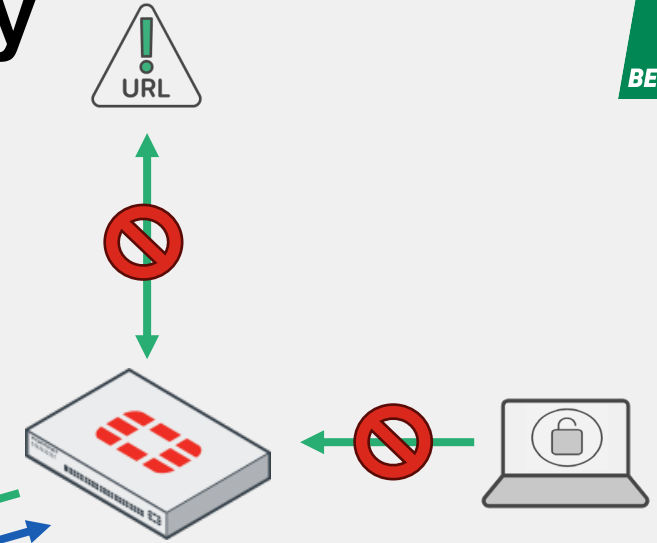
Architecture based on AI from FortiGuard Labs



Predefined playbooks provided by FortiGuard and fully customizable



Foundation for Managed Detection & Response (MDR) service



# Merci!

Des questions? Contactez-nous: [it-forum.ch@bechtle.com](mailto:it-forum.ch@bechtle.com)

