



# Applying Zero Trust to enable a Secure SD-Branch

Anderson Silva C. Freire

Sr. Business Dev. Engineer – Americas International (SAT)

[silvaa@fortinet.com](mailto:silvaa@fortinet.com)

# Agenda (~ 60min)

- 01** Intro and Key Concepts
- 02** Challenges and Trends
- 03** Fortinet Vision and Technologies
- 04** Use cases
- 05** Closing remarks
- 06** DEMO
- 07** Q&A



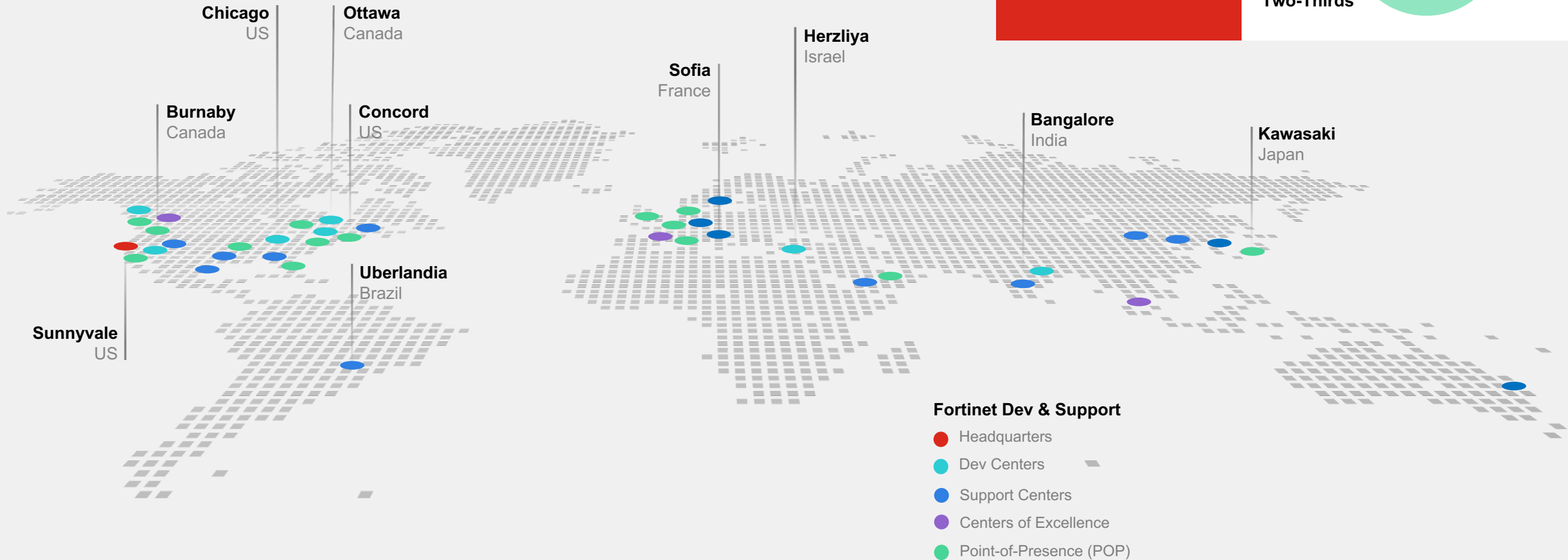
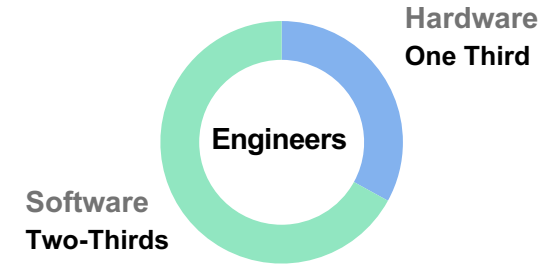
# Intro



# Global Reach & Support

Majority of our R&D is based in North America

**13,200+**  
Employees  
Worldwide



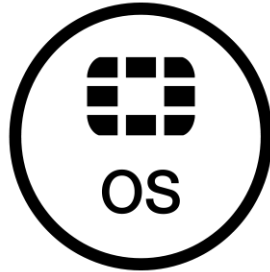


# The Fortinet Advantage



## Security Processors

Superior NGFW and  
SD-WAN performance  
and efficiency



## FortiOS

Ties all the Security Fabric's  
security and networking  
components together



## Security Fabric

Organically developed, highly  
integrated and automated  
cybersecurity platform



## Ecosystem

**300+** partners  
**500+** integrations

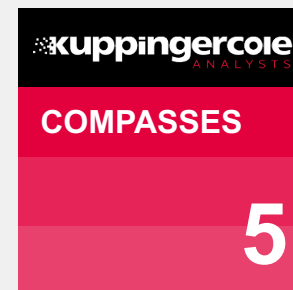
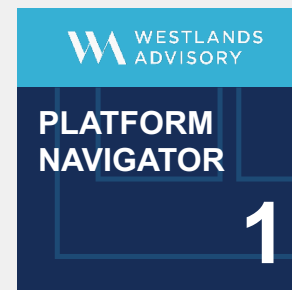
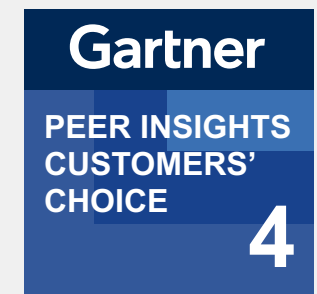


# 37

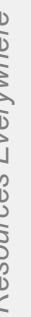
## Enterprise Analyst Reports Validate Fortinet Across Networking & Security

Fortinet is one of the most validated enterprise cybersecurity companies in the world ranking in leadership positions across dozens of analyst reports highlighting the broad application of the Fortinet Security Fabric.

\*Analyst validation includes reports where expert and independent 3<sup>rd</sup> party analysts rank and evaluate vendors: Gartner Magic Quadrants, IDC MarketScapes, Frost & Sullivan Radars, Forrester Waves, Westlands Advisory Platform Navigator, Kuppingercole Compasses, Gigaom Radar.



100%









# Key concepts

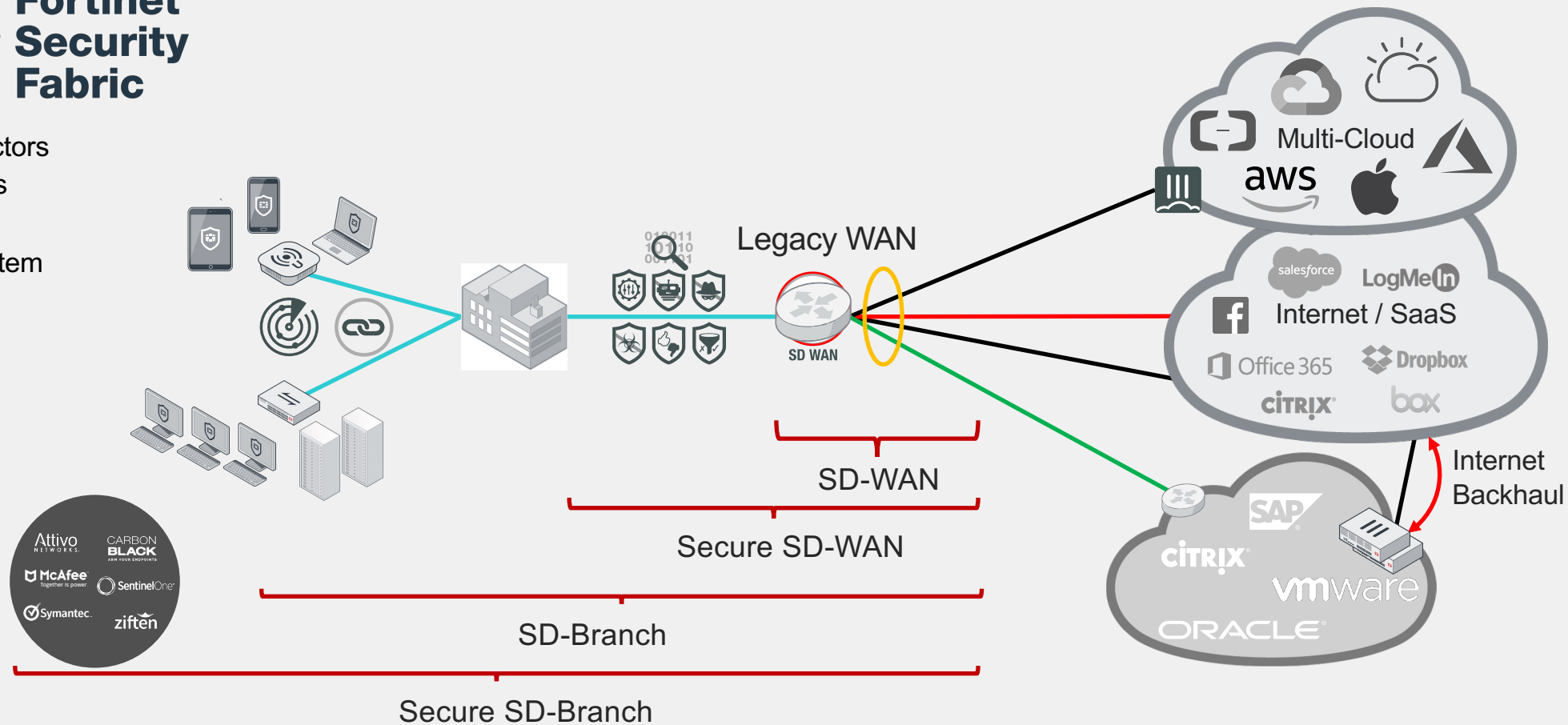


# What's Secure SD-Branch?

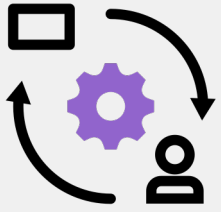
MPLS Overlay	
Internet Overlay	
Internet	
LAN	



-  Connectors
-  DevOps
-  APIs
-  Ecosystem







# Zero Trust Principles:

Never trust, always verify.

Discover

Users, devices, system, data and applications

Control

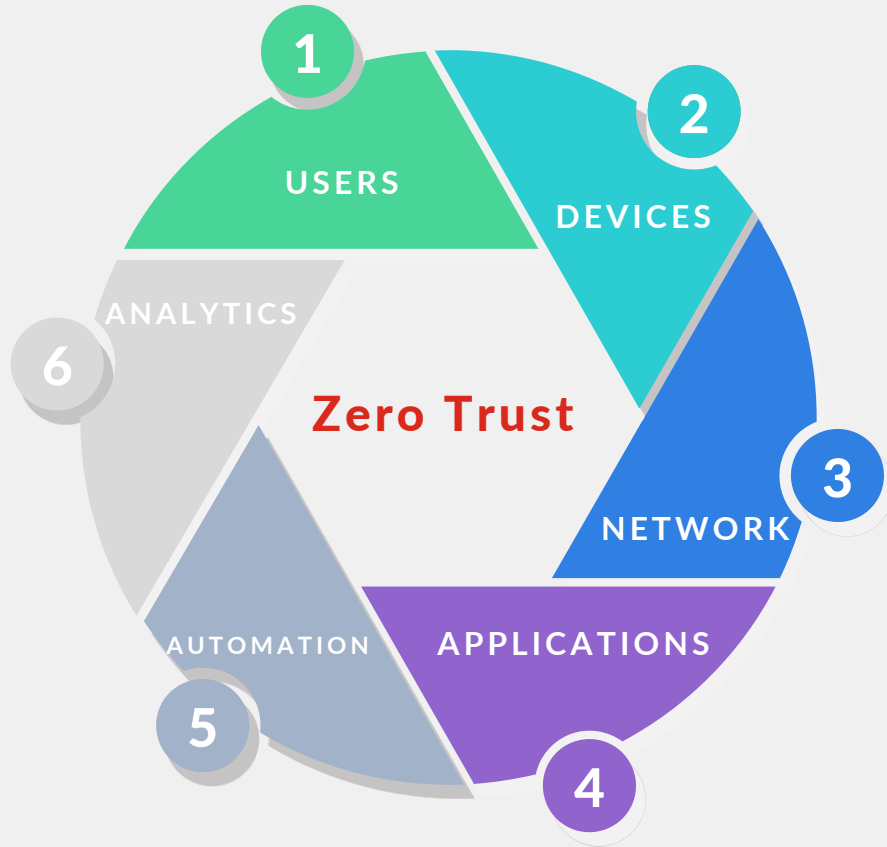
Use policies to grant least privilege, authorize and authenticate everywhere, all the time and on a per-transaction basis.

Monitor

Continuously monitor, re-evaluate and assess cyberhealth. Baseline and adapt

Assume you were breached.

# Fundamental Pillars of Zero Trust



## Users

Identity, Credential, and Access Management

## Network

Control network access, visibility to make dynamic policy and trust decision on network and data traffic

## Automation

Automate event responses across products to reduce reaction time

## Devices

Real-time cybersecurity posture and trustworthiness of devices

## Applications

Securing and properly managing the application layer

## Analytics

Observe in real time what is happening



# Industry Challenges



# New Educational Landscape Drives Digital Transformation

**Today's students come to school technically savvy**

- Expect to be engaged
- Expect technology “should just work”

**Network enabled learning tools**

- Digital “Chalkboard”
- Assignments given and turned in online.
- Interactive applications to engage and enable students.
- Effectively monitor and help students who are having difficulties.

**Security is a key concern**

- Protect information
- Ensure proper use
- Security vs User Experience






# What IT challenges are Educational CIOs facing?

Well...

Why not ask to the new oracle?



## ChatGPT

 Examples	 Capabilities	 Limitations
"Explain quantum computing in simple terms" →	Remembers what user said earlier in the conversation	May occasionally generate incorrect information
"Got any creative ideas for a 10 year old's birthday?" →	Allows user to provide follow-up corrections	May occasionally produce harmful instructions or biased content
"How do I make an HTTP request in Javascript?" →	Trained to decline inappropriate requests	Limited knowledge of world and events after 2021

[ChatGPT Mar 23 Version](#). Free Research Preview. ChatGPT may produce inaccurate information about people, places, or facts



# According to ChatGPT “Researcher Group”...



**Cybersecurity and data privacy**



**Digital Transformation / Hybrid Learning**



**Compliance requirements**



**Budget Constraints**



**User experience and adoption**



**Digital Equity**

# Ok. But what's all about Fortinet Zero Trust?

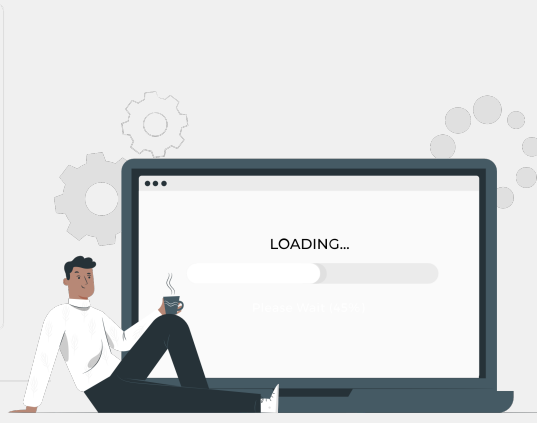
Easy-Peasy: Our Zero Trust solution can help you in



Improving security



Simplifying management



Delivering greater agility



Improving user experience



Increasing efficiency  
and reducing costs

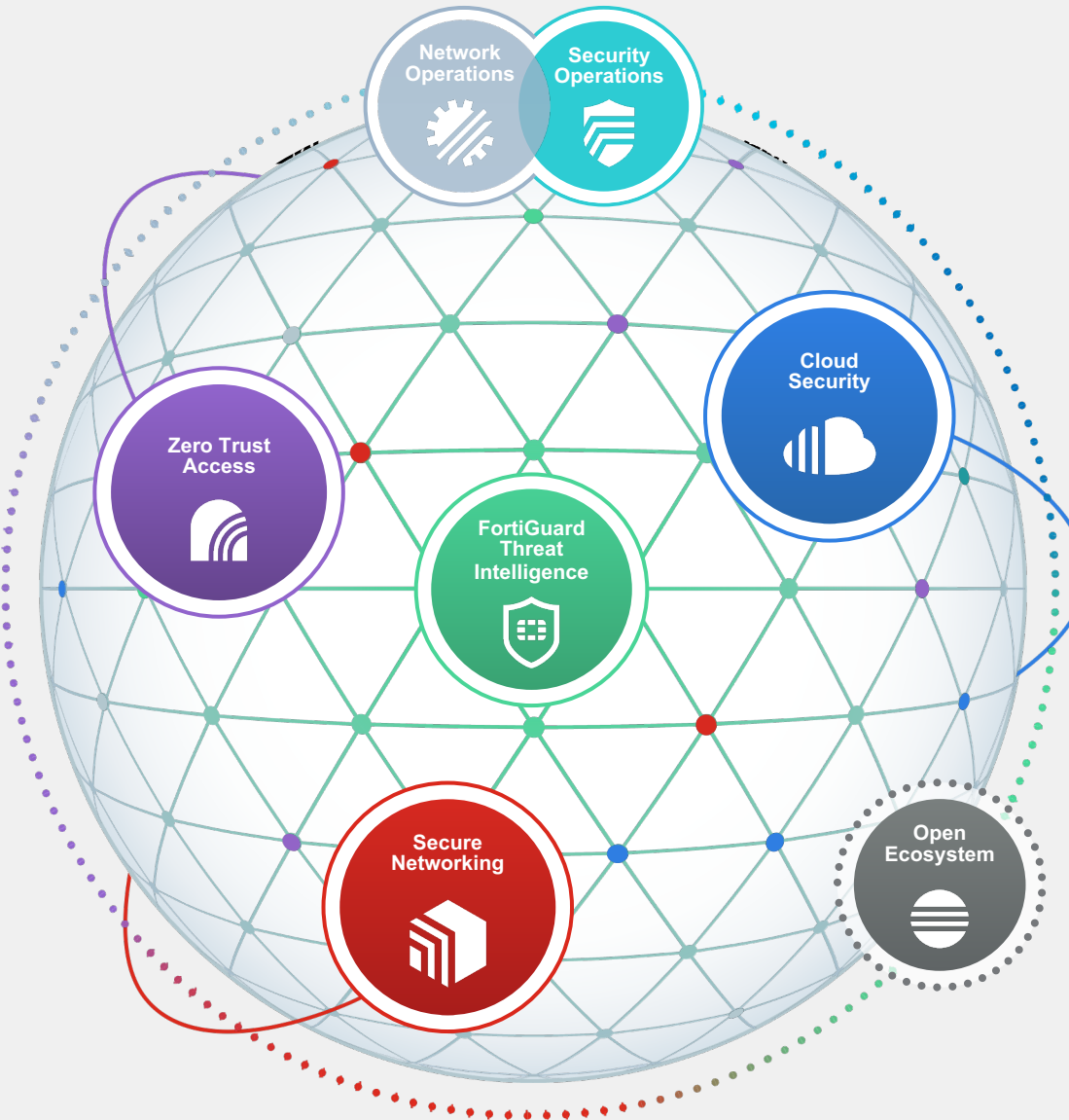
## But... HOW?

Glad you asked...



# Implementing a consolidated network

The Fortinet approach  
by gaining control from few  
vendors (not a single vendor)  
Network structure  
- Multiple products from a few  
vendors vendors  
- No complex integration  
capabilities



# Why Architecture?

---





# Create a mature and efficient security strategy

---







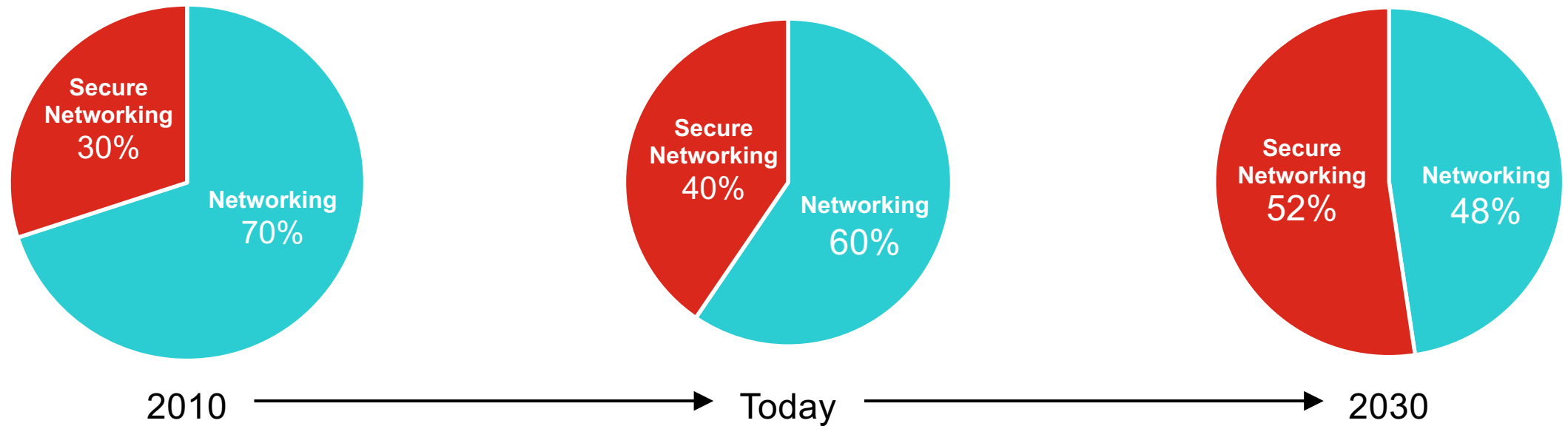
# Fortinet Vision

Network Convergence and Consolidation



# Convergence

Secure networking will be larger than networking by 2030



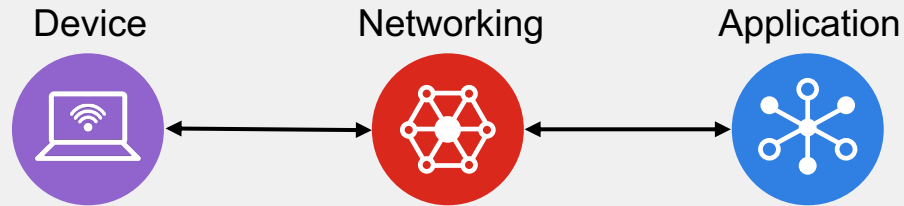
<sup>1</sup> Gartner, Forecast: Enterprise Network Equipment, Worldwide, 2022-2026, 3Q22 Update (December 2022). <sup>2</sup> Gartner, Forecast: Information Security and Risk Management, Worldwide, 2022-2026, 3Q22 Update (December 2022). <sup>3</sup> Fortinet estimates.



# Old vs New Network Landscape

## Connectivity

Trust Everything

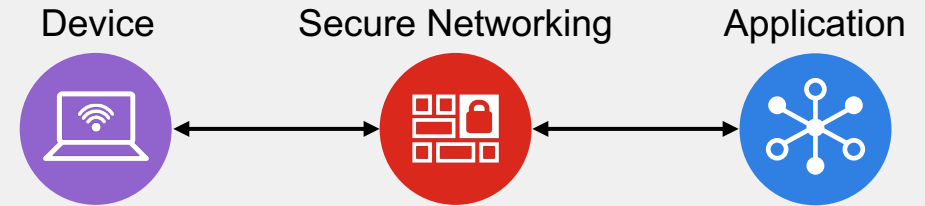


Connection based on IP

Small amount of  
compute required

## Secure Connectivity

Zero Trust

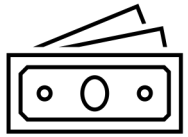


Connection based on application, content,  
users, devices and location



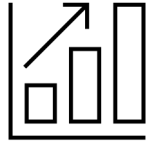
More compute  
required

# Effectiveness of converged networks



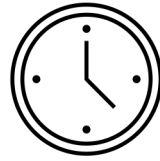
## Cost Reduction

According to Forrester, organizations that adopt converged networks can achieve **cost reductions** of up to **25%**.



## Improved Efficiency

According to IDC, converged networks can improve network **efficiency** by up to **40%**



## Reduced Downtime

Gartner reports that organizations that adopt converged networks can **reduce network downtime** by up to **70%**.



## Increased Productivity

According to IDC, converged networks can **improve** employee **productivity** by up to **20%**.



## Increased Security

According to Forrester, organizations that adopt converged networks can **reduce** the number of security **incidents** by up to **30%**.

\* Forrester: "Converged Infrastructure: Benefits Beyond the Data Center" / Gartner: "The Top Six Benefits of Converged Infrastructure"





# Fortinet Technologies

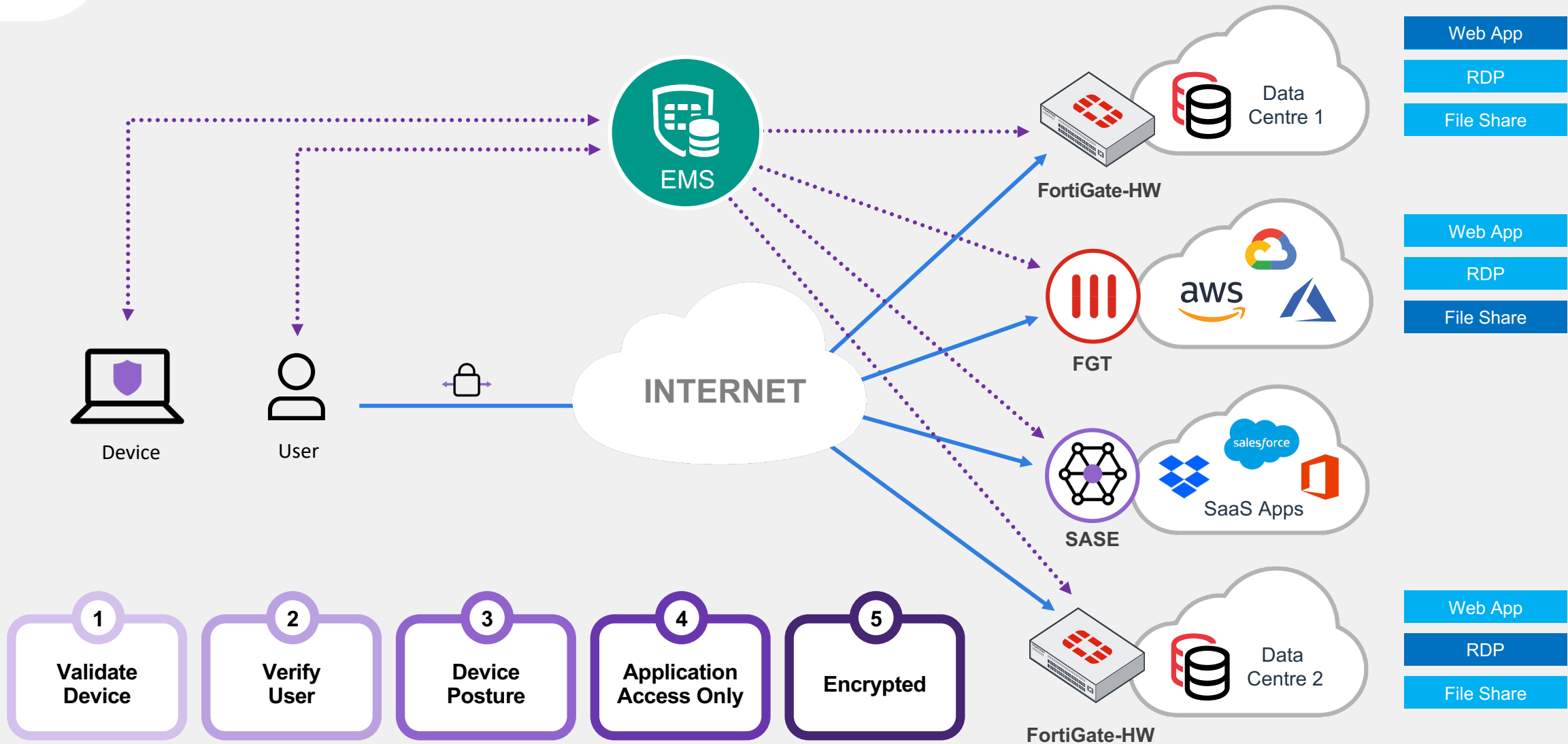
Convergence and Consolidation

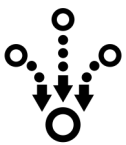






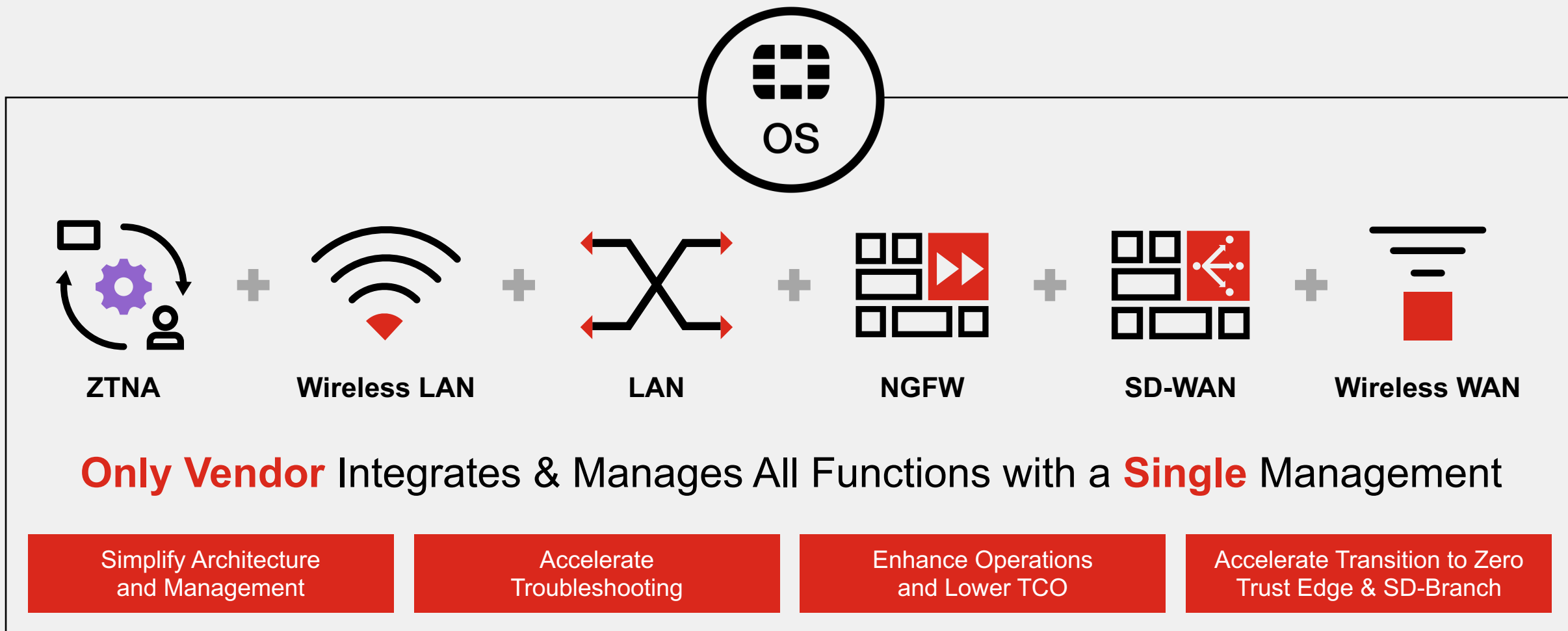
# Fortinet Zero Trust Architecture





# Tight Integration With LAN, WLAN, WWAN, ZTNA

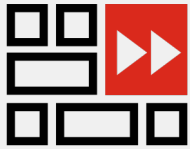
Transition to support SD-Branch, SASE and Zero Trust Edge



# Fortinet LAN Edge Difference

## LAN Requirements

NGFW



Wireless



Switching



NAC



## Convergence

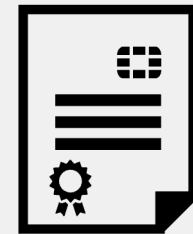


One Console



One Config

## High ROI & Low TCO



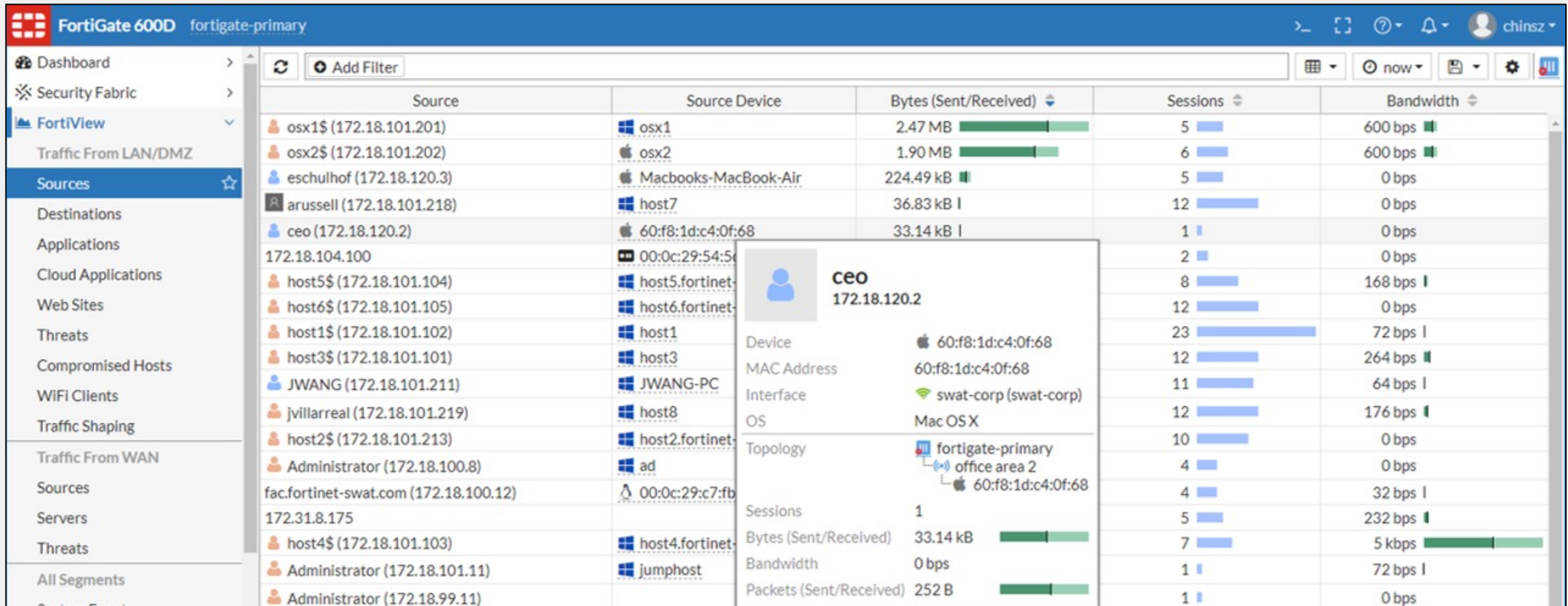
Fewer Licenses  
Simplified Operations





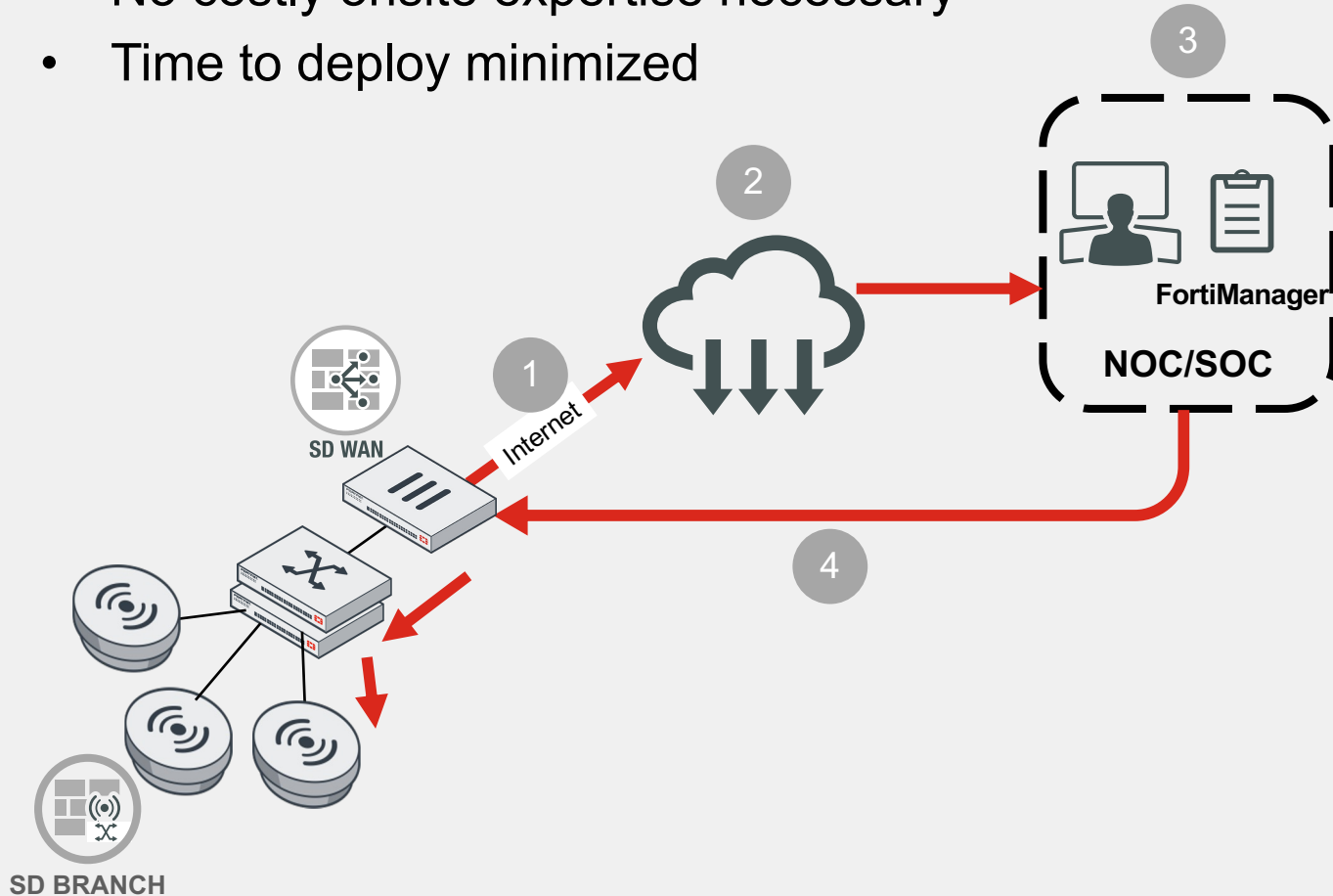
# Tracked Identity for regulatory compliance

It's no longer about what a device is doing, it's about what a specific **user** is doing



# Zero Touch Deployment

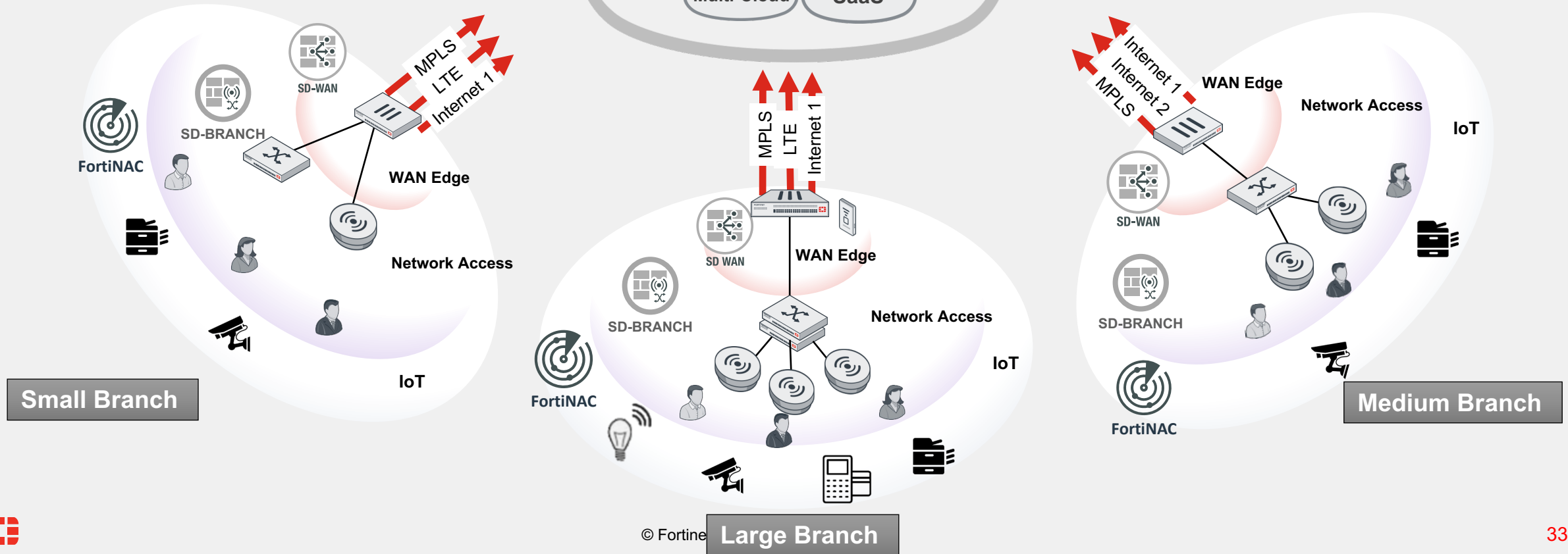
- Ship equipment directly to site
- No costly onsite expertise necessary
- Time to deploy minimized



1. Connect FortiGate to internet
2. FortiGate sends out discovery to FortiDeploy
3. FortiDeploy pre-populated with serial Id of FortiGate, forwards to assigned FortiManager
4. FortiManager pushes configuration to FortiGate FortiSwitch and FortiAP.

# Secure SD-Branch Deployment

Simplified Management  
Integrated Security  
Lower TCO

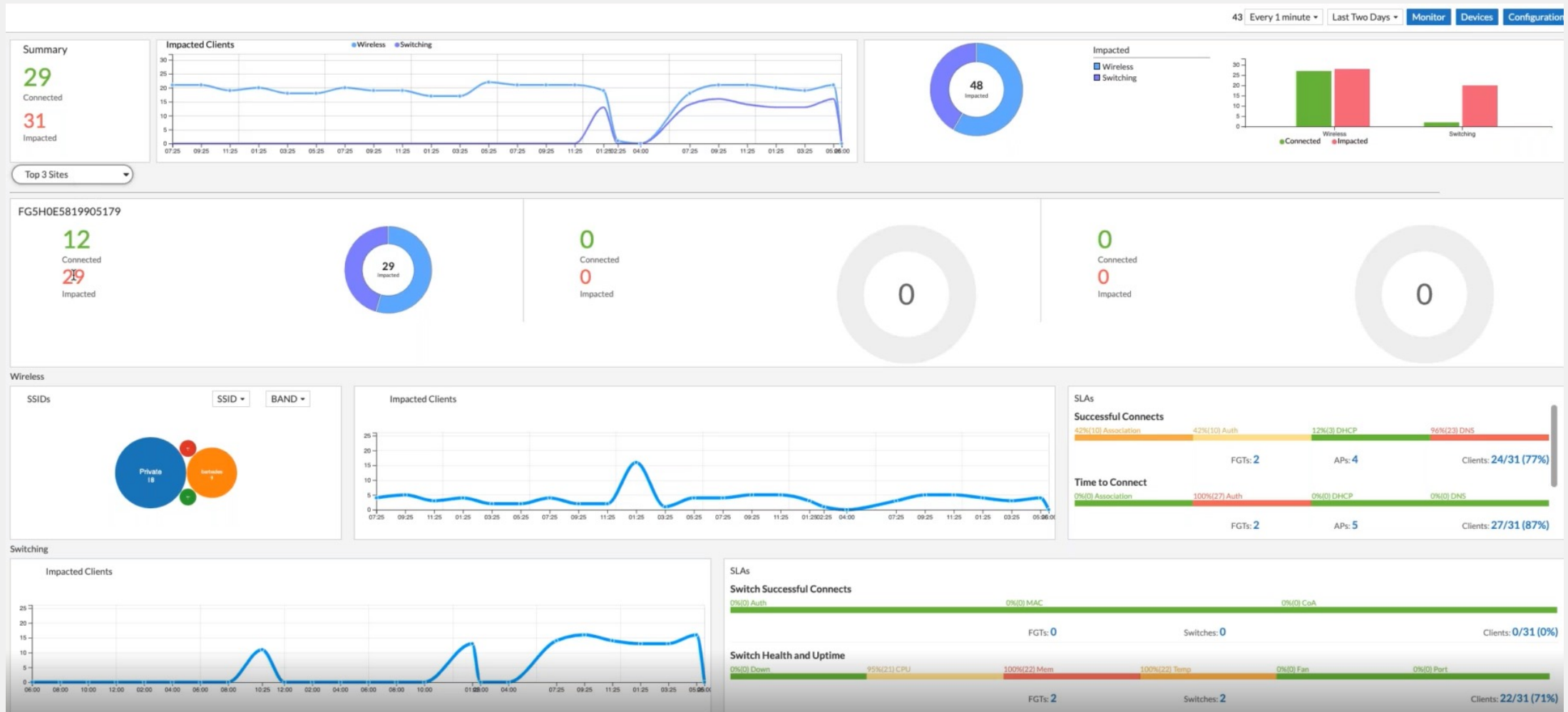




# FortiAIOPs

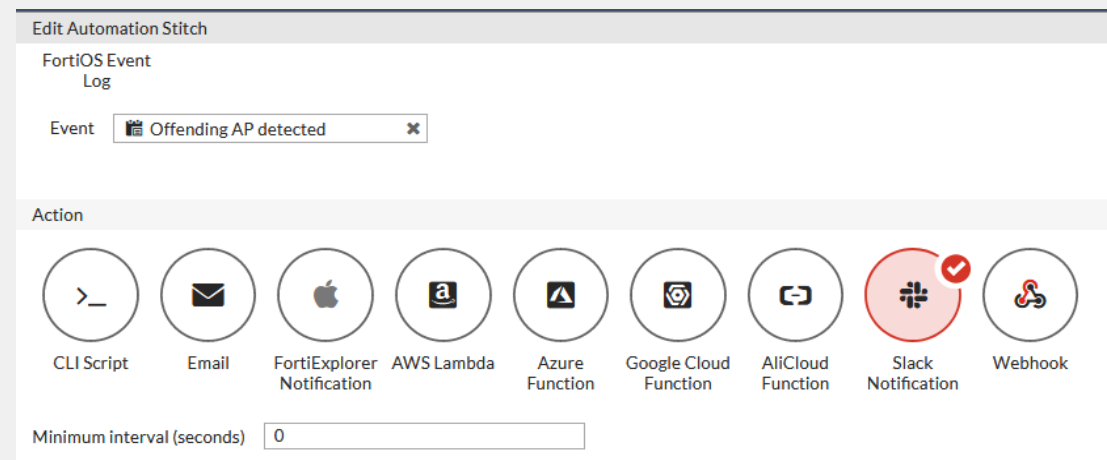
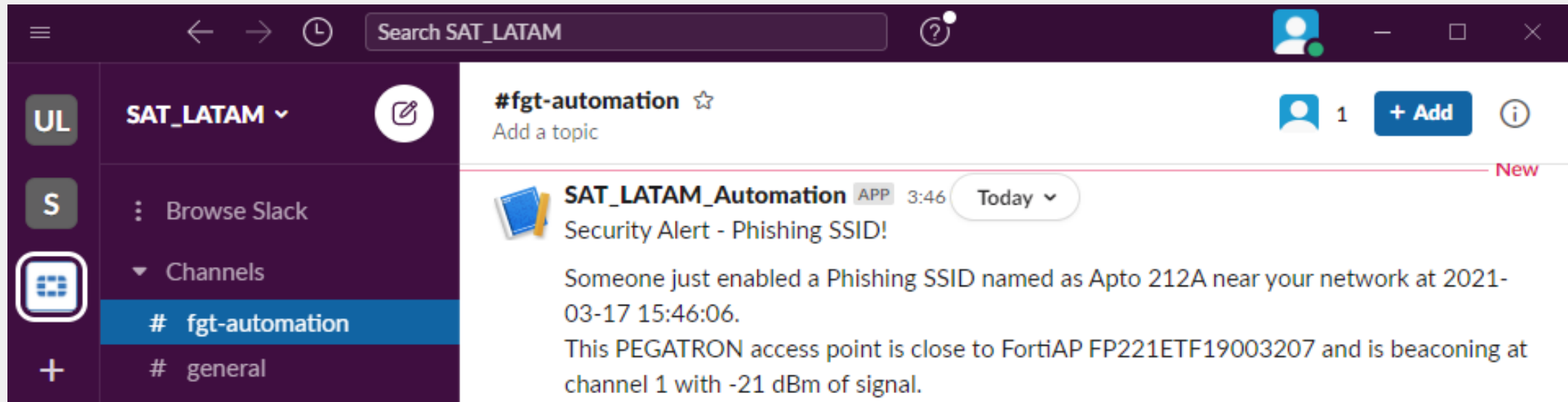


Powered by AI





# Native Automation



# Use Cases



# Use Cases



**Network Access  
Control**



**Securing Work  
From Anywhere**



**Automate  
incident response**

# Use Case – Network Access Control

## Advanced Segmentation

- Accurate endpoint Information
  - OS
  - Logged-in user / social ID / avatar
  - FortiClient status
  - Endpoint vulnerabilities
  - Correlate multiple MAC
  - Online / offline
- Provide endpoint risk score to the Security Rating
  - Risk-based awareness
  - Unpatched vulnerabilities.

Name **Block\_Vulnerable\_IoT**

Status ☒ Enabled ☐ Disabled

FortiSwitches **All** Specify

Description  0/63

---

**Device Patterns** ⓘ

Category **Device** User EMS Tag **Vulnerability**

Match **Severity is at least** Specify

**SEV** High ☒ ☐ ☐ ☐ ☐ ☐

---

**Switch Controller Action** ⓘ

Assign VLAN ☒ **qtn.internal8**

Bounce port ☐

Assign device to dynamic address ⓘ ☐

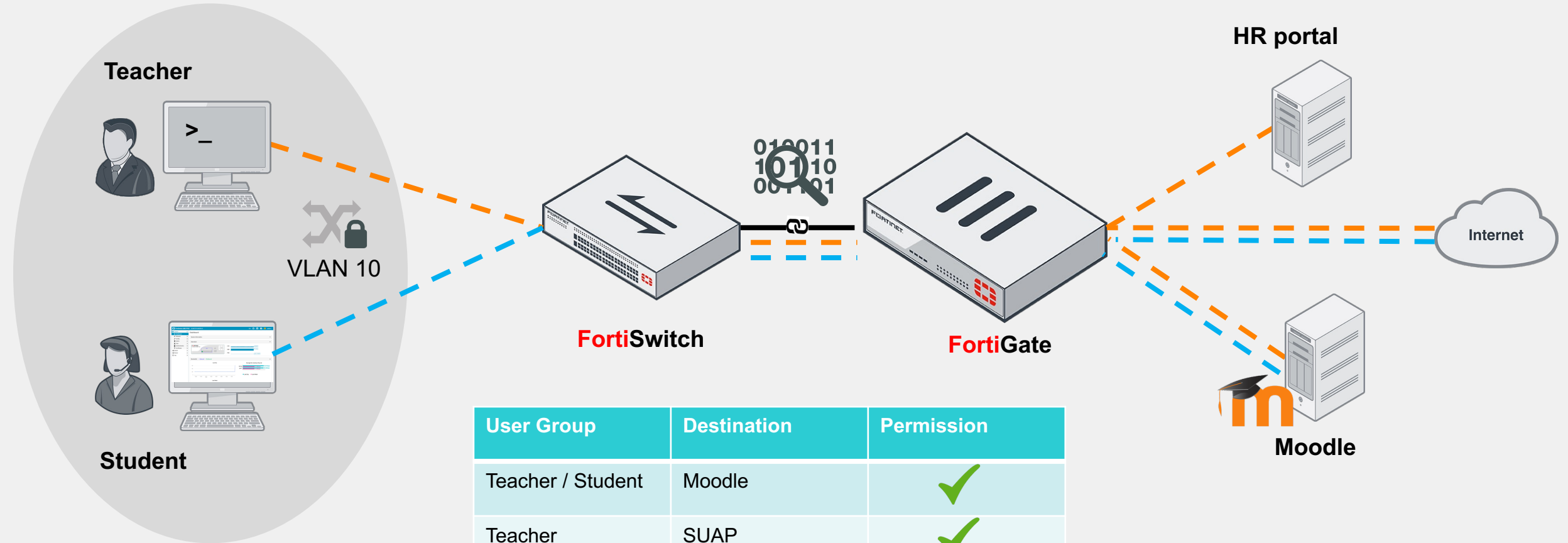
---

**Wireless Controller Action**


Assign VLAN ☒ **wqtn.20.fac**

# Use Case – Network Access Control

## Intent-based Segmentation



User Group	Destination	Permission
Teacher / Student	Moodle	✓
Teacher	SUAP	✓
Student	Portal RH	✗
Teacher / Student	Internet	✓



silvaa

ZERO TRUST TELEMETRY

REMOTE ACCESS

ZTNA DESTINATION

MALWARE PROTECTION

**VULNERABILITY SCAN**

Notifications

Settings

About

OS (1)

OS	SEVERITY	RECOMMENDED ACTION
> MacOS X System Update 13.1 (1)	Critical	Auto-Patch

+ Browser (0)

+ MS Office (0)

+ 3rd Party App (0)

+ Service (0)


+ User Configuration (0)

+ Others (0)

Install Selected

ZTNA Access Denied

https://userportal.myfortinet.com



## Oops, ZTNA doesn't let you in

Note:

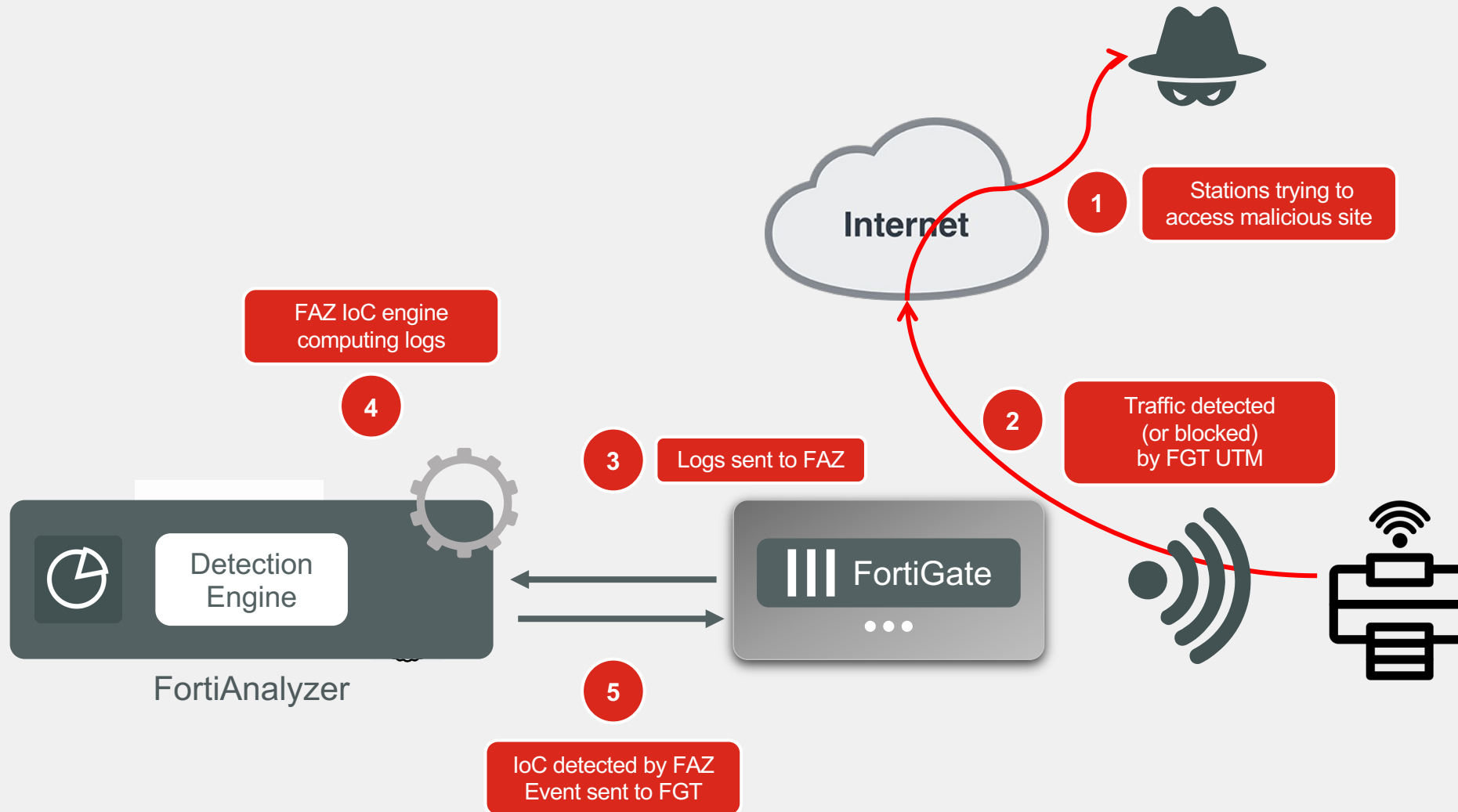
- Mobile users, please use a Fortinet issued computer instead.
- For desktop/laptop users, please try the following debug process.
  1. make sure your Forticlient is running 7.0.6 GA or later
  2. Clean the cache of your browser, restart your browserFor the different browsers, please try to use the below links to find how to clear your cache:  
[Chrome](#)  
[Safari](#)  
[Edge](#)  
[Firefox](#)
  3. Disconnect EMS from FortiClient, connect back to EMS, and wait for 5 seconds

Please contact regional helpdesk if you continue to have problems

ZTNA Access Denied Policy restriction! No policy matched! End-point SN miss matched. SN: 3751E

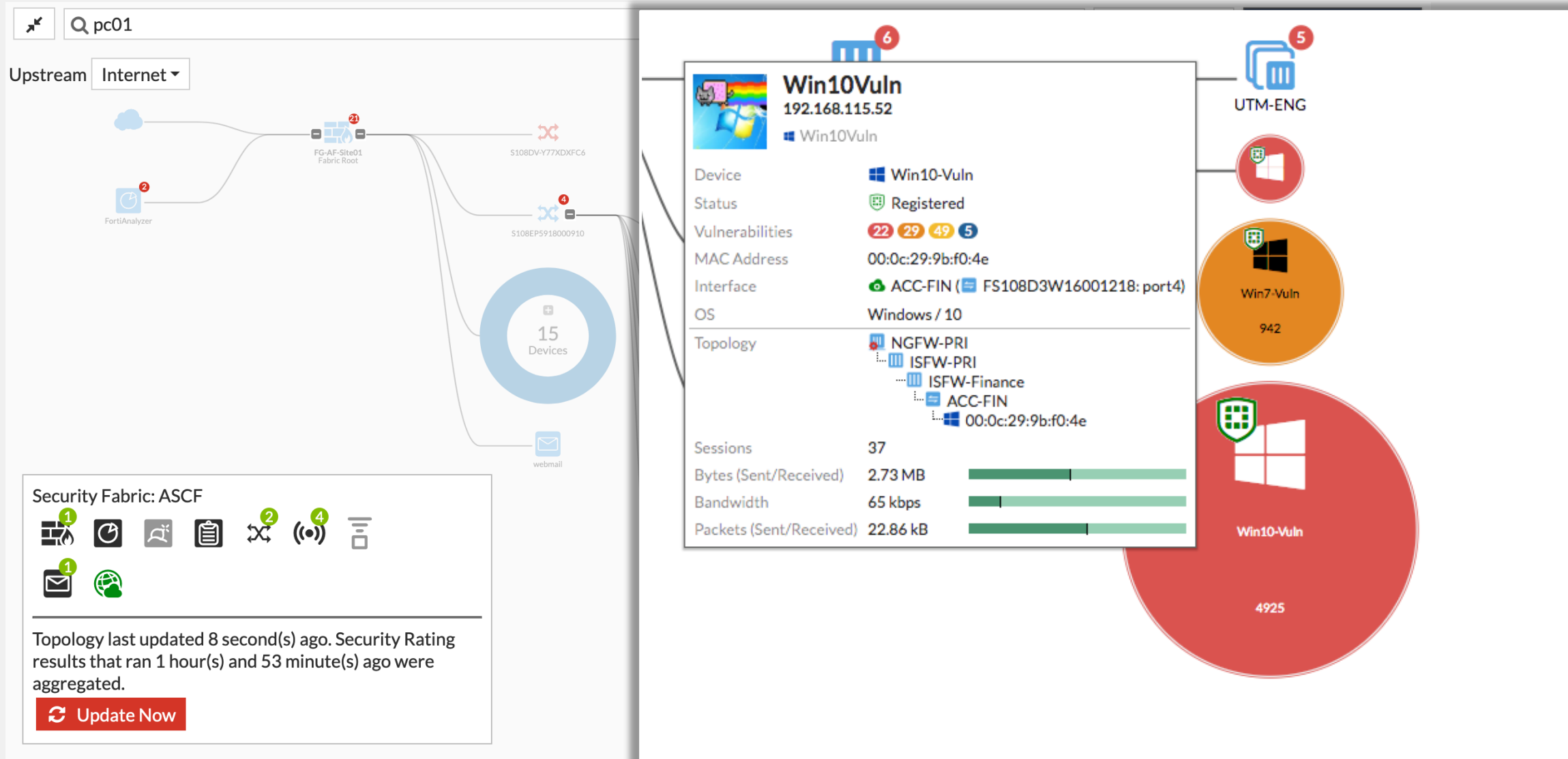
# Use case – Automate incident response

Automation via IOC



# Use case – Automate incident response

Automation via IOC







# Closing remarks



# Summary



Zero Trust is a philosophy/culture, not a solution. So...



Follow Fortinet recommendations



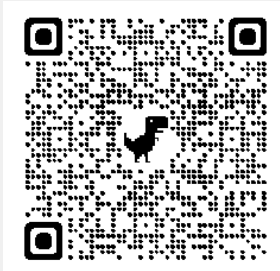
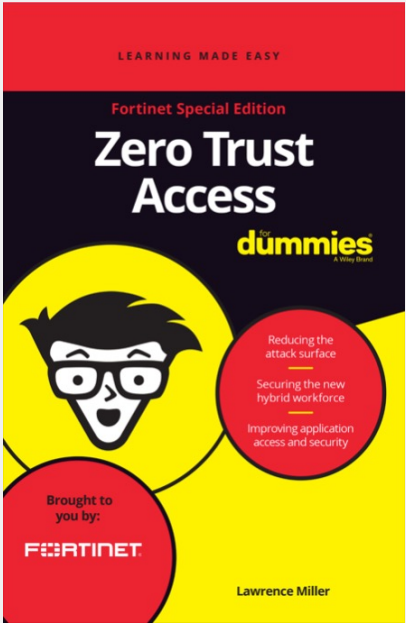
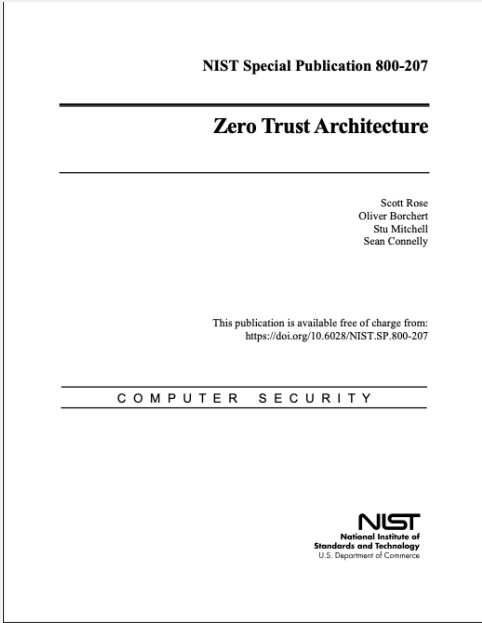
Take the FTNT Maturity Level Evaluation



Trust no ONE else, but us.



# Improving your Zero Trust Skills



**FORTINET®**