Fortinet Security Fabric

Krzysztof Sieniawski

Fortinet Security Fabric

Broad

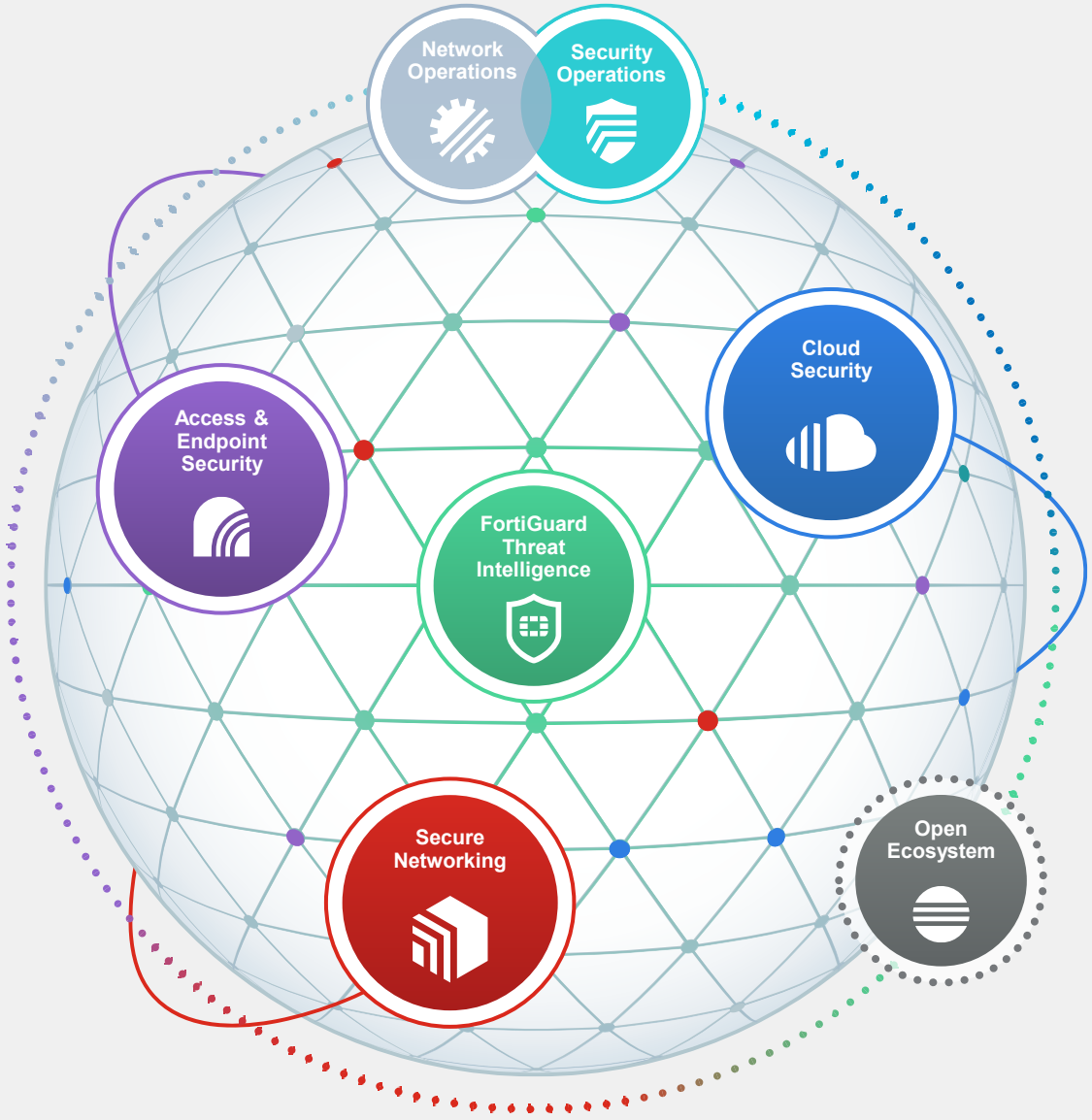
visibility and protection of the entire digital attack surface to better manage risk

Integrated

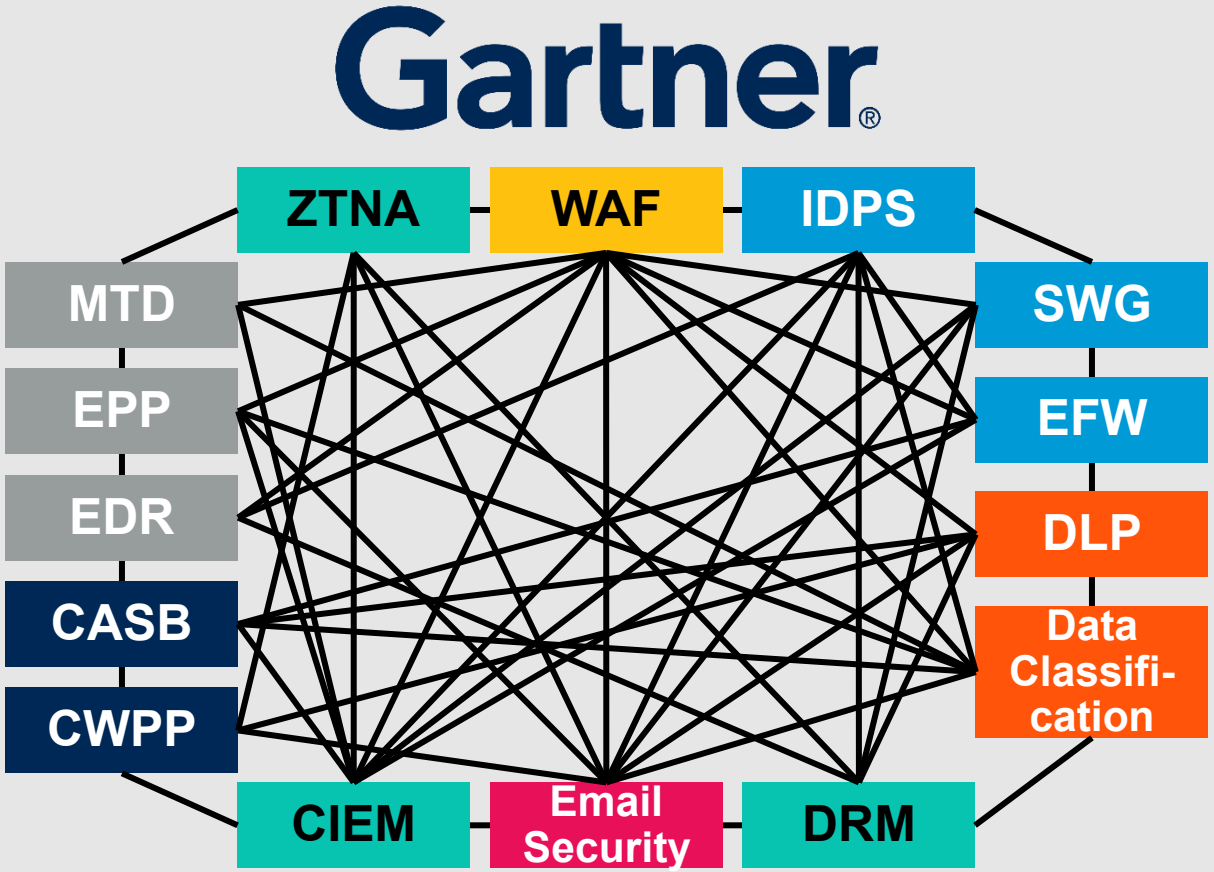
solution that reduces management complexity and shares threat intelligence

Automated

self-healing networks with AI-driven security for fast and efficient operations



Fortinet Security Fabric as CyberSecurity Mesh



Executive Guide to Cybersecurity Mesh, 2022

Felix Gaehtgens, James Hoover, Henrique Teixeira, Claudio Neiva, Michael Kelley, Mary Ruddy, Patrick Hevesi. As of October 2021

Fortinet Security Fabric

The industry's highest-performing integrated cybersecurity mesh platform

Fortinet Brochure
Highlighting our broad, integrated, and automated solutions, quarterly

Free Training
Fortinet is committed to training over 1 million people by 2025

Free Assessment
Perform an assessment in your network to validate your existing controls

FortiOS
The Heart of the Fortinet Security Fabric

Secure Networking

FortiGate
NGFW w/ SOC acceleration and industry-leading secure SD-WAN

FortiGate SD-WAN
Application-centric, scalable, and Secure SD-WAN with NGFW

FortiExtender
Extend scalable and resilient LTE and LAN connectivity

FortiAP
Protected LAN Edge deployments with wireless connectivity

FortiSwitch
Deliver security, performance, and manageable access to data

FortiNAC
Visibility, access control and automated responses for all networked devices

FortiProxy
Enforce internet, compliance and granular application control

FortiIsolator
Maintain an "air-gap" between browser and web content

Cloud Security

FortiGate VM
NGFW w/ SOC acceleration and industry-leading secure SD-WAN

FortiDDOS
Machine-learning quickly inspects traffic at layers 3, 4, and 7

FortiCNP
Manage risk and compliance through multi-cloud infrastructures

FortiDevSec
Continuous application security testing in CI/CD pipelines

FortiWeb
Prevent web application attacks against critical web assets

FortiADC
Application-aware intelligence for distribution of application traffic

FortiGSLB Cloud
Ensure business continuity during Unexpected network downtime

FortiMail
Secure mail getaway to protect against SPAM and virus attacks

FortiCASB
Prevent misconfigurations of SaaS applications and meet compliance

FortiCNF
Offers enterprise-grade protection on Amazon AWS, with inbound and outbound traffic inspection and insights

Zero Trust Access

FortiSASE
Enforce dynamic network access control and network segmentation

ZTNA Agent
Remote access, application access, and risk reduction

FortiAuthenticator
Identify users wherever they are and enforce strong authentication

FortiToken
One-time password application with push notification

FortiClient Fabric Agent
IPSec and SSL VPN tunnel, endpoint telemetry and more

FortiGuest
Simplified guest access, BYOD, and policy management

FortiPAM
Control & monitoring of elevated & privileged accounts, processes, and critical systems

FortiGuard Threat Intelligence

Powered by FortiGuard Labs

Fabric Management Center: NOC

FortiManager
Centralized management of your Fortinet security infrastructure

FortiGate Cloud
Saas w/ zero touch deployment, configuration, and management

FortiMonitor
Analysis tool to provide NOC and SOC monitoring capabilities

FortiAIOps
Network inspection to rapidly analyze, enable, and correlate

FortiExtender Cloud
Deploy, manage and customize LTE internet access

FNDN
Exclusive developer community for access to advanced tools & scripts

Open Ecosystem

The industry's most extensive ecosystem of integrated solutions

Fabric Connectors
Fortinet-developed

DevOp Tools & Script
Fortinet & community-driven

Fabric API Integration
Partner-led

Extended Ecosystem
Threat sharing w/ tech vendors

Fabric Management Center: SOC

FortiDeceptor
Discover active attackers inside with decoy assets

FortiNDR
Accelerate mitigation of evolving threats and threat investigation

FortiEDR
Automated protection and orchestrated incident response

FortiRecon
Digital Risk Protection (DRP) for early, actionable warning and fast response

FortiSandbox / FortiAI
Secure virtual runtime environment to expose unknown threats

FortiAnalyzer
Correlation, reporting, and log management in Security Fabric

FortiSIEM
Integrated security, performance, and availability monitoring

FortiSOAR
Automated security operations, analytics, and response

FortiTester
Network performance testing and breach attack simulation (BAS)

SOC-as-a-Service
Continuous awareness and control of events, alerts, and threats

Incident Response Service
Digital forensic analysis, response, containment, and guidance

Support & Mitigation Services

FortiCare Essentials*
15% of hardware

FortiCare Premium*
20% of hardware

FortiCare Elite**
25% of hardware

FortiConverter
25% of hardware

* FortiCare Premium is formerly 24x7 Support. Lower support price for Switches and APs

** Response time for High Priority tickets. Available for FortiGate, FortiManager, FortiAnalyzer, FortiSwitch, and FortiAP

Communication and Surveillance

FortiFone
Robust IP Phones w/ HD Audio with centralized management

FortiVoice
Integrated voice, chat, conferencing management, and fax with centralized

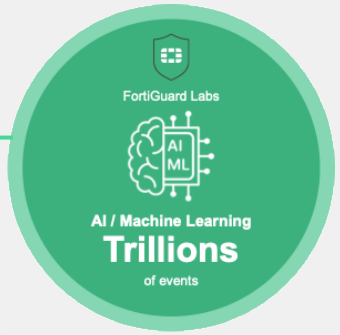
FortiCamera
HDTV-quality surveillance cameras for physical safety and security

FortiRecorder
High-performance NVR with AI-powered video management software

Fortinet's Network Firewall Solution

New

SecOps



FortiGuard

OS, Management & Analytics

FortiOS | FortiAnalyzer | FortiAI | FortiManager

Branch

ASIC — FortiGate 40-90 Series

Campus

ASIC — FortiGate 100-900 Series

Data Center

ASIC — FortiGate 1000-7000 Series

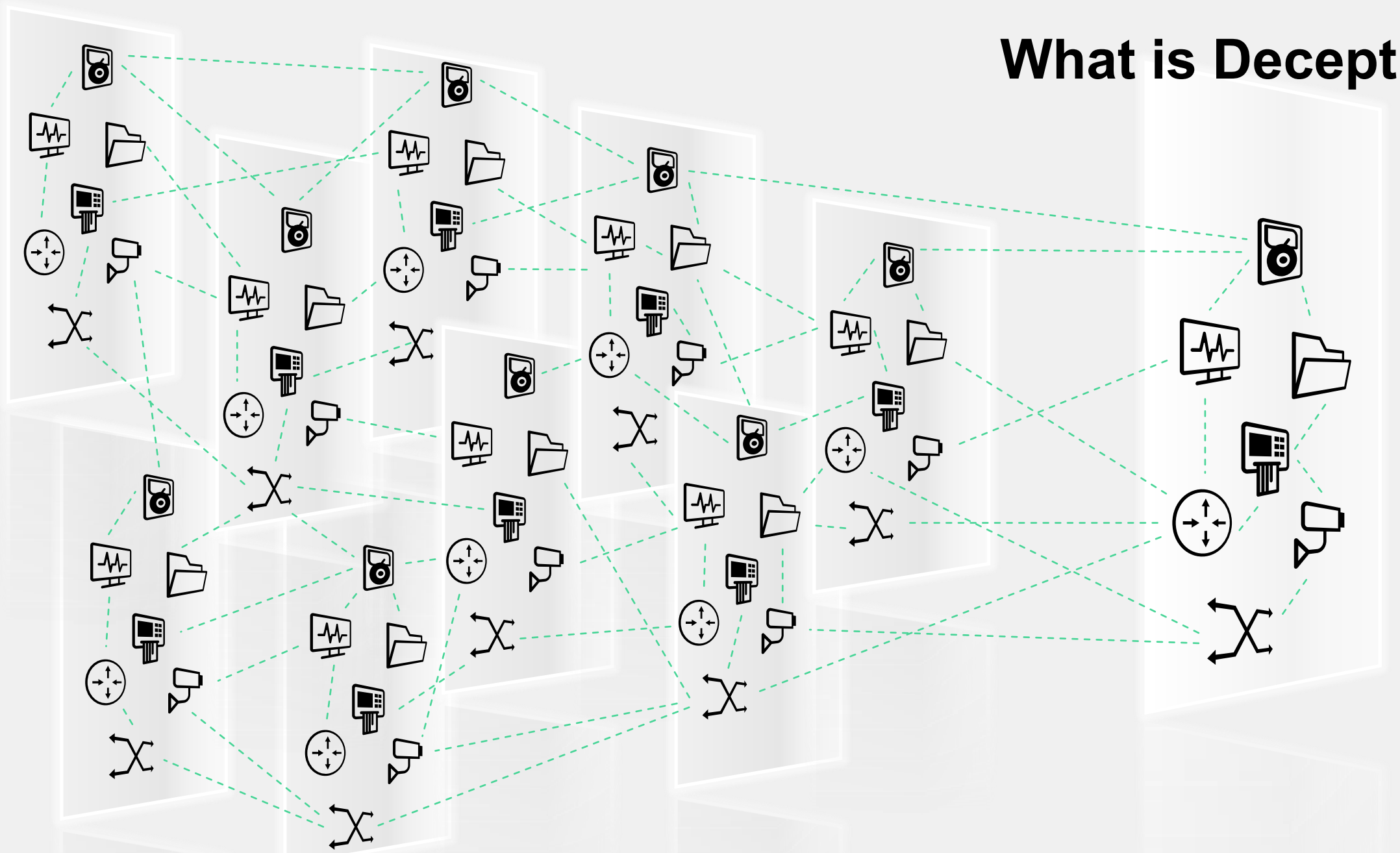
VM / Cloud / FWaaS

FortiGate VM | FortiCNF | FGaaS

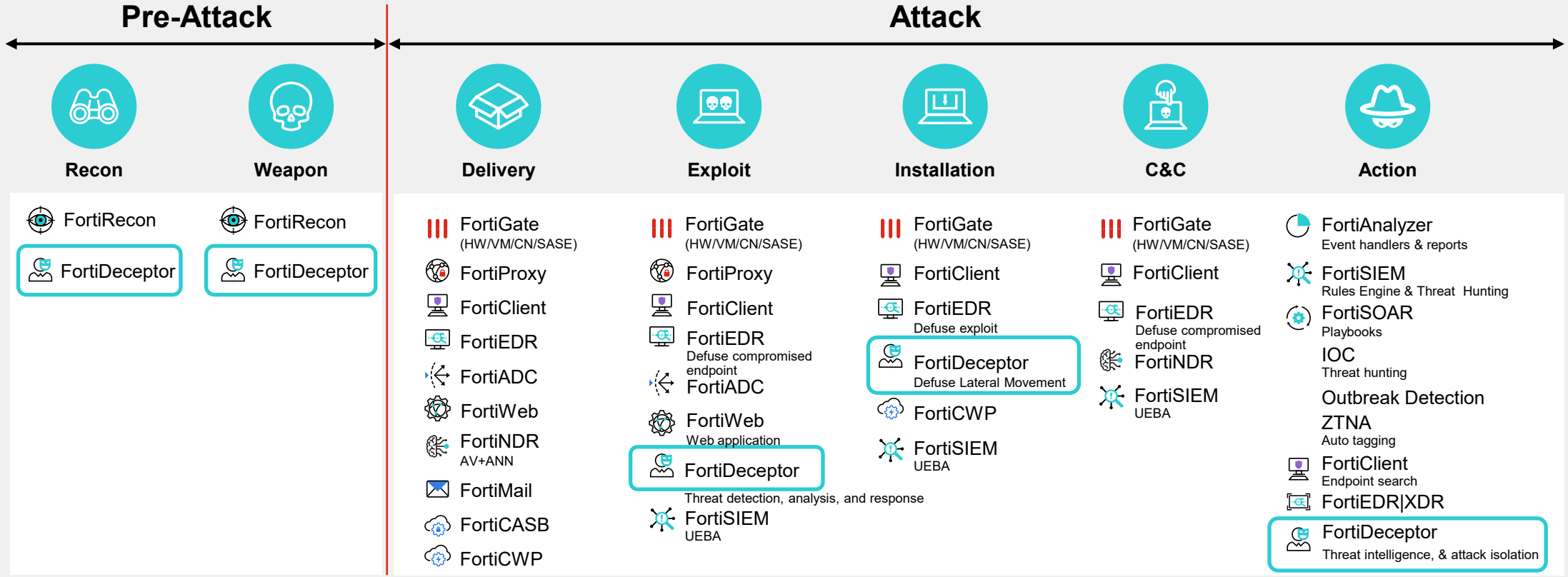
Secure LAN Edge

FortiExtender | FortiAP | FortiSwitch | FortiNAC

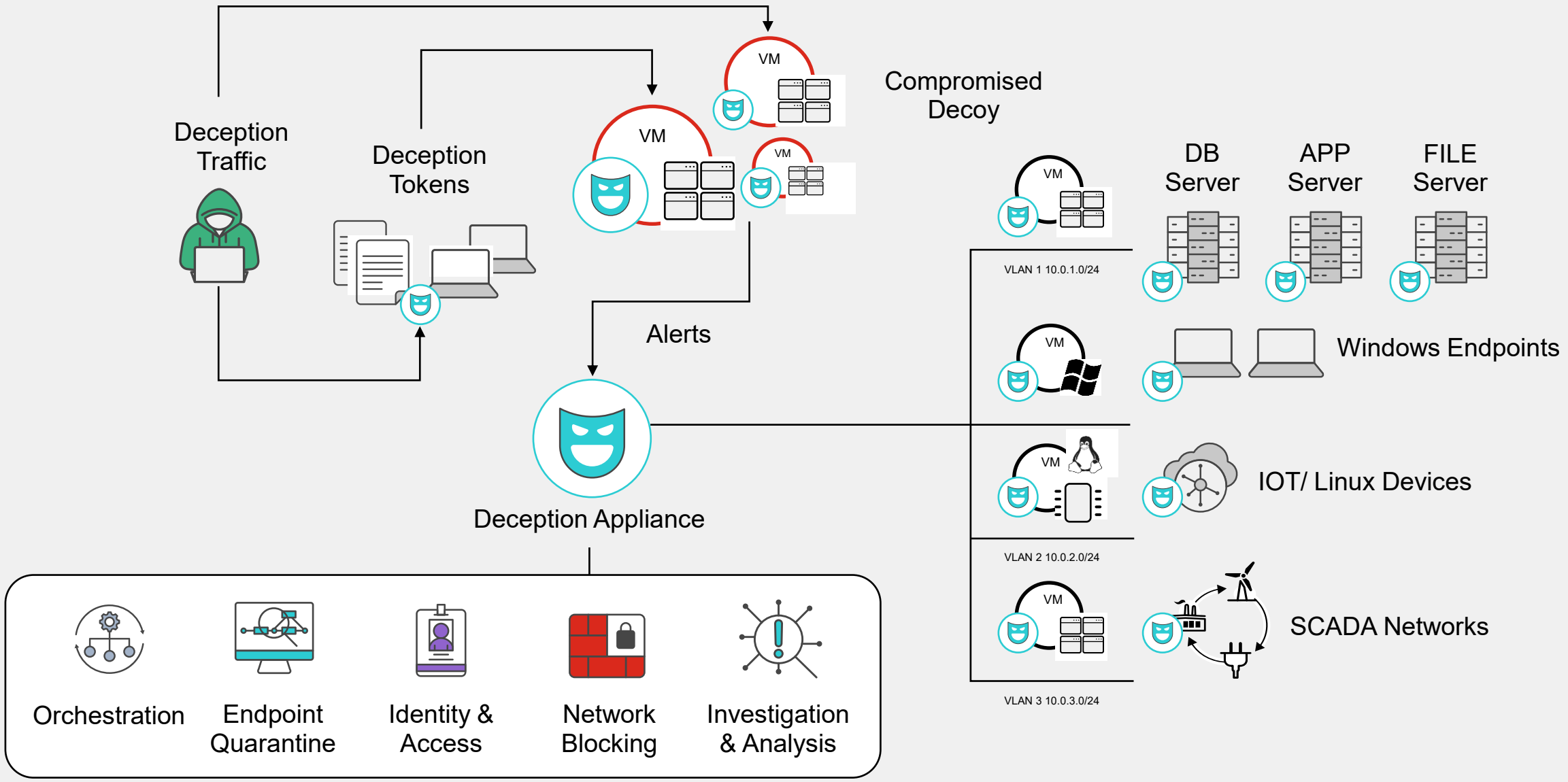
What is Deception?



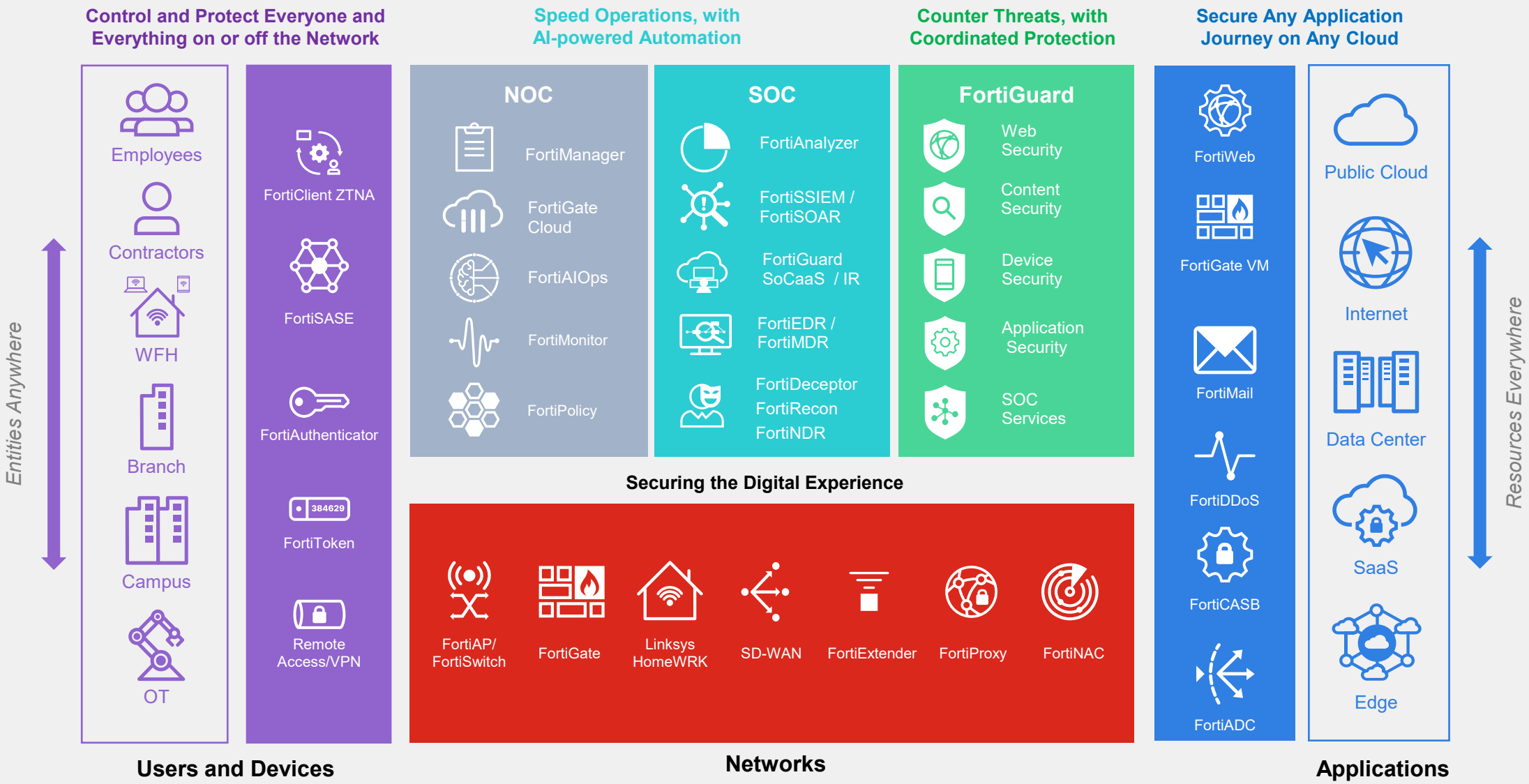
How to Break the Attack Sequence — FortiDeceptor Support



How Deception Works

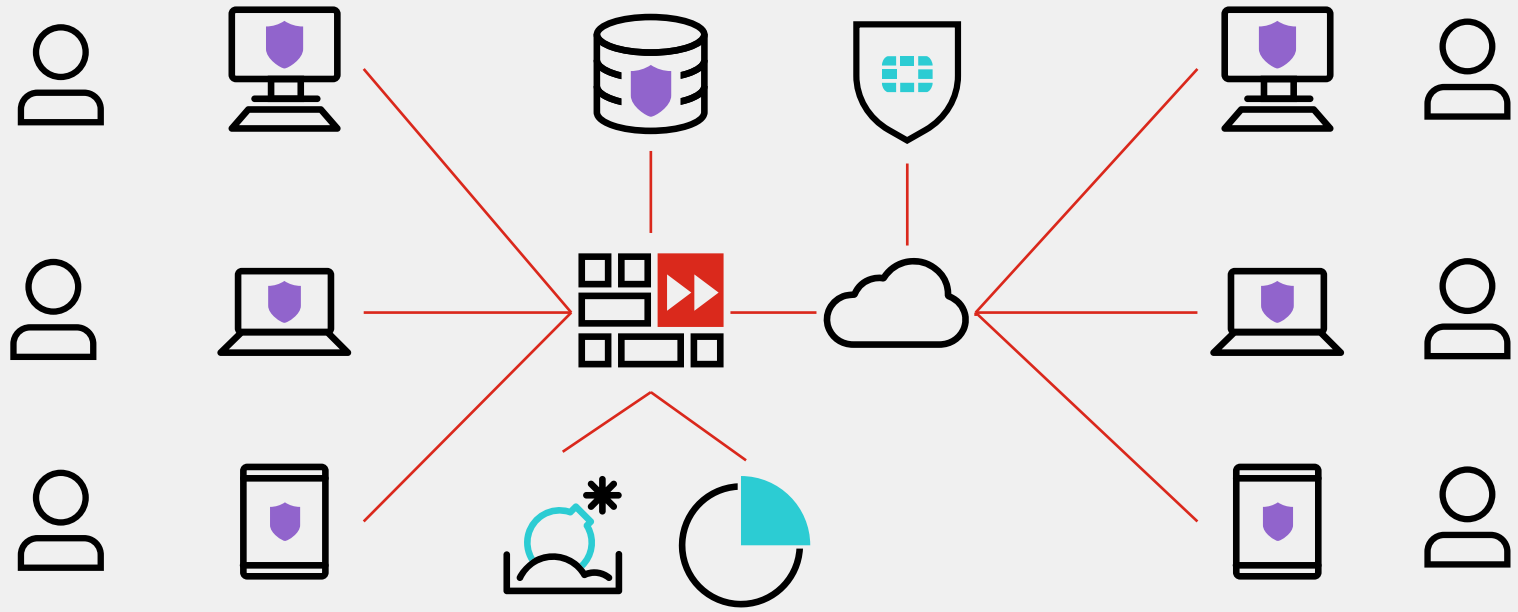


Fortinet Security Fabric Expansion



Zero Trust Access—Device Visibility & Control

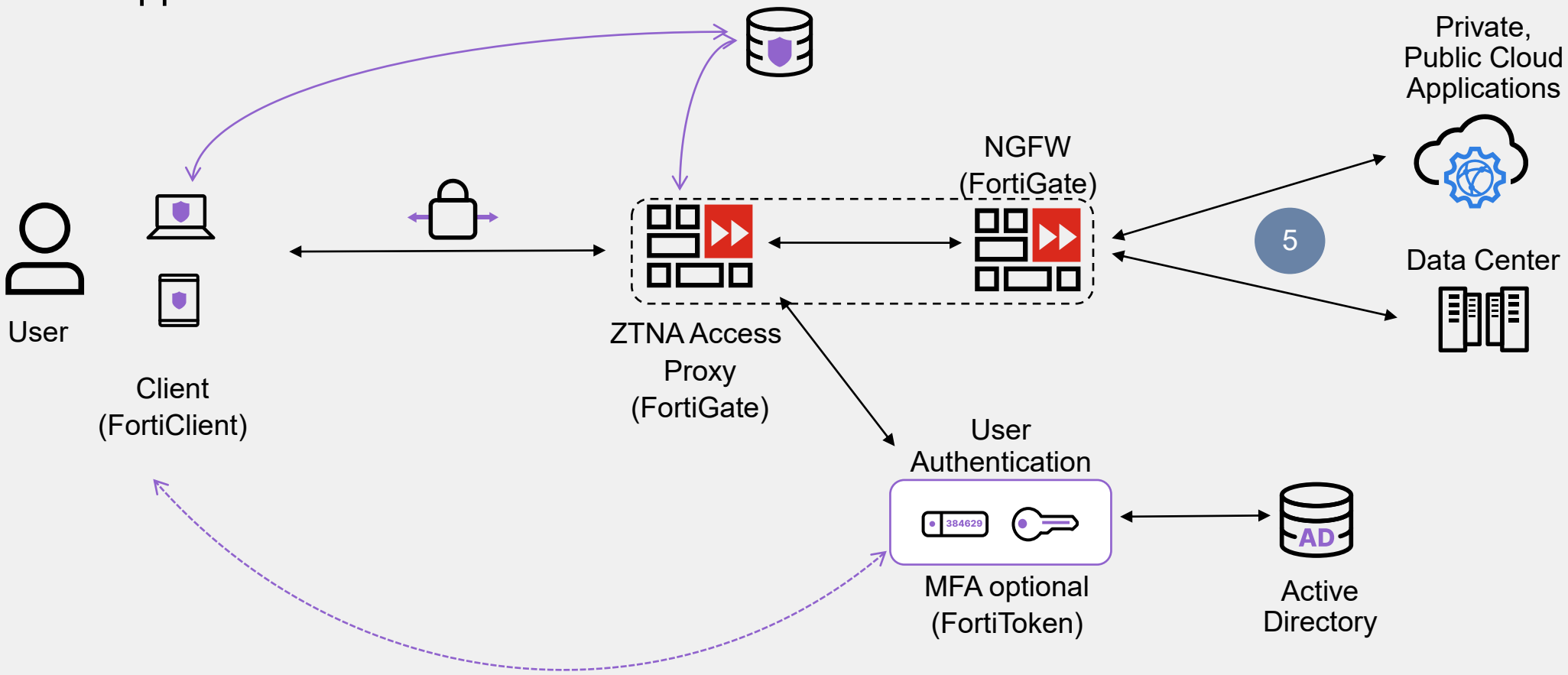
FortiClient for Fabric Agent, Remote Access, and Endpoint Protection



Hygiene Control	Secure Remote Access	Endpoint Protection
Vulnerability scanning FortiGuard Web Filtering Patching Policy Dynamic grouping	Zero Trust Network Access (ZTNA) VPN (IPSec & SSL) Single Sign On (SSO)	FortiGuard ML-based AV Sandbox integration Anti-exploit Automated containment

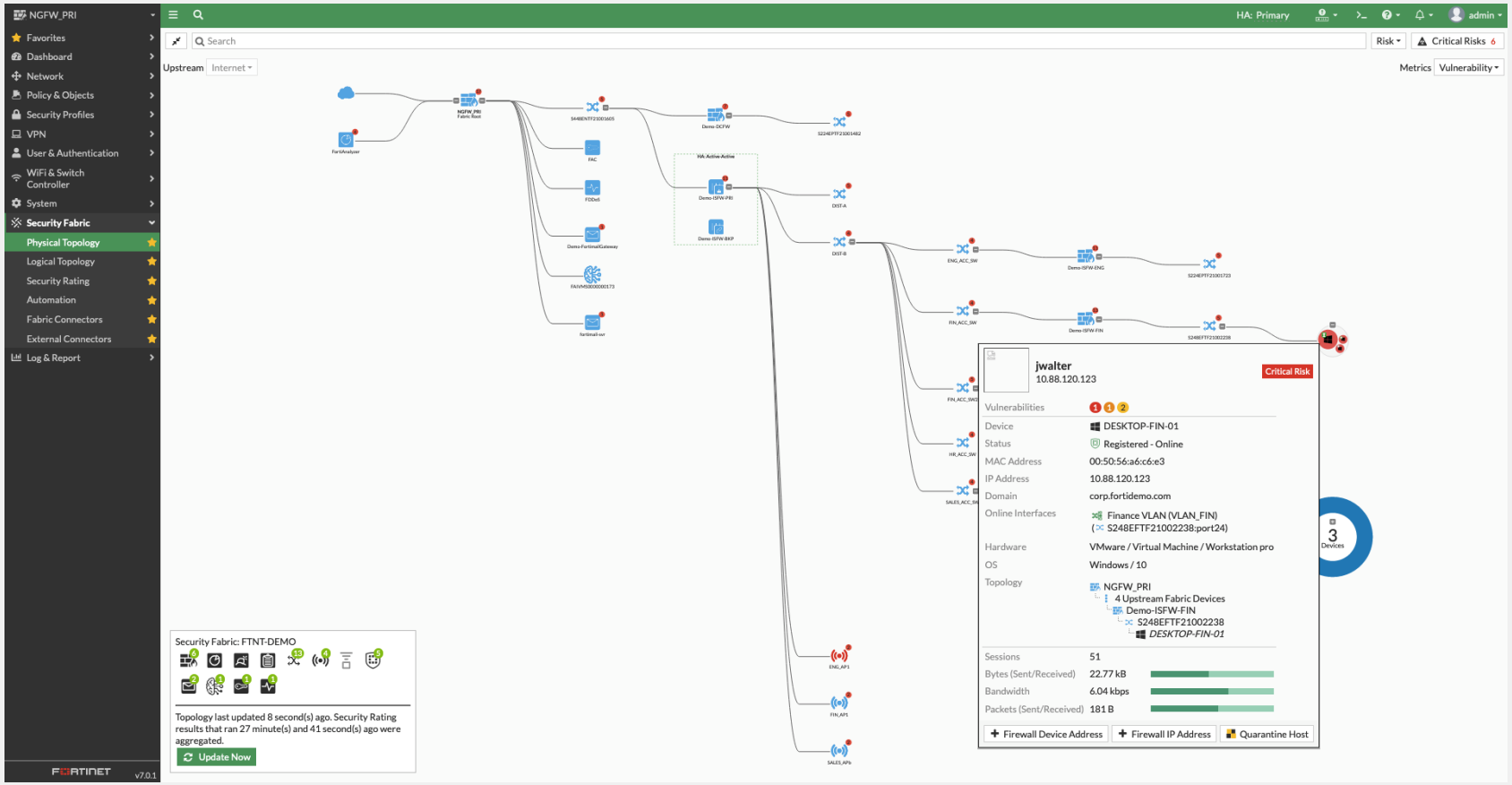
Zero Trust Network Access (ZTNA) Technology

Granular Application Access



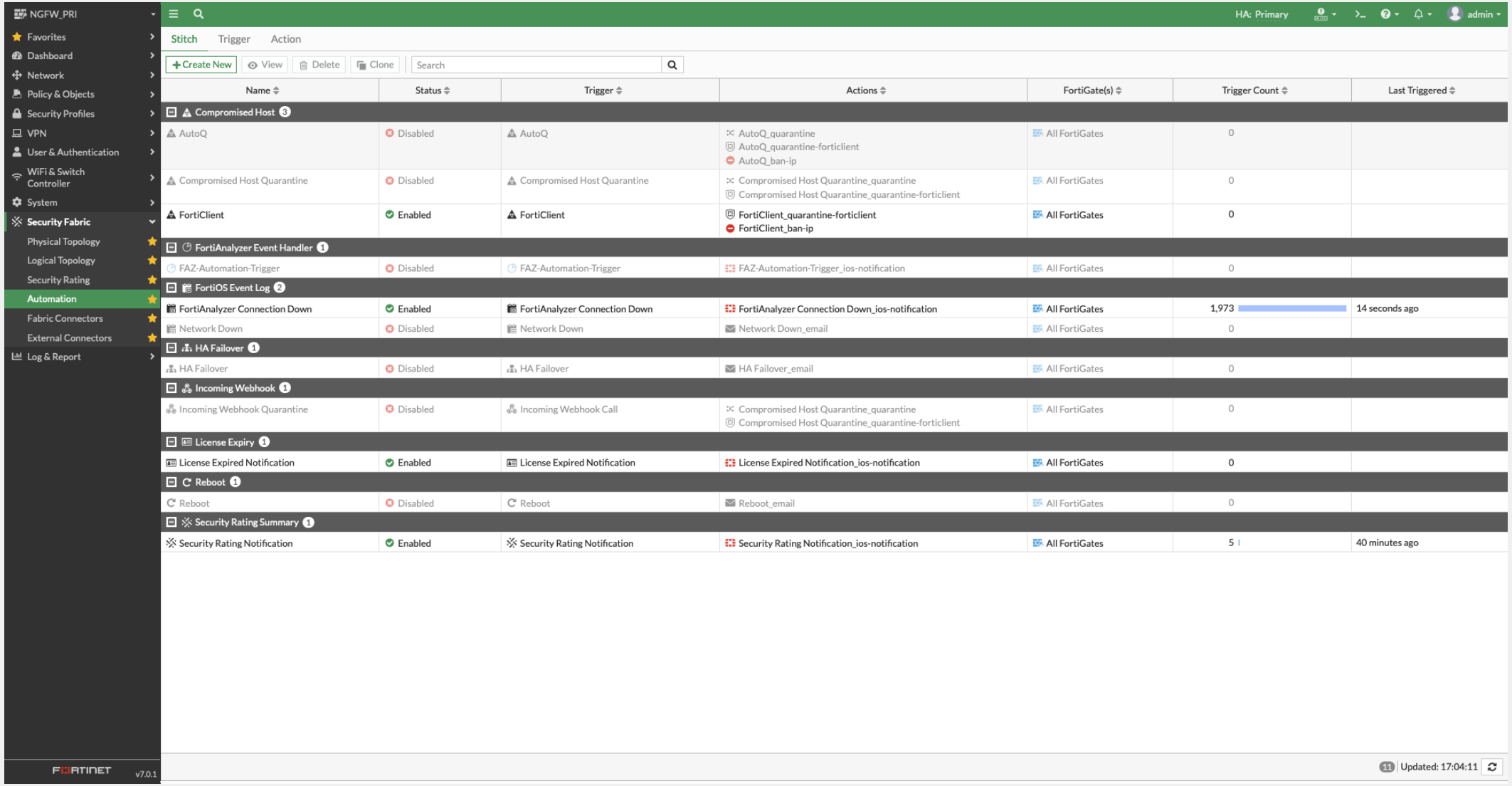
- Automatic, transparent encrypted tunnels
- Split tunneling
- Per Session verification & identification
- Additional layers of security with MFA
- Single-Sign-on agent supports FortiAuthenticator

Risk Visibility In The Network Context Endpoint Telemetry

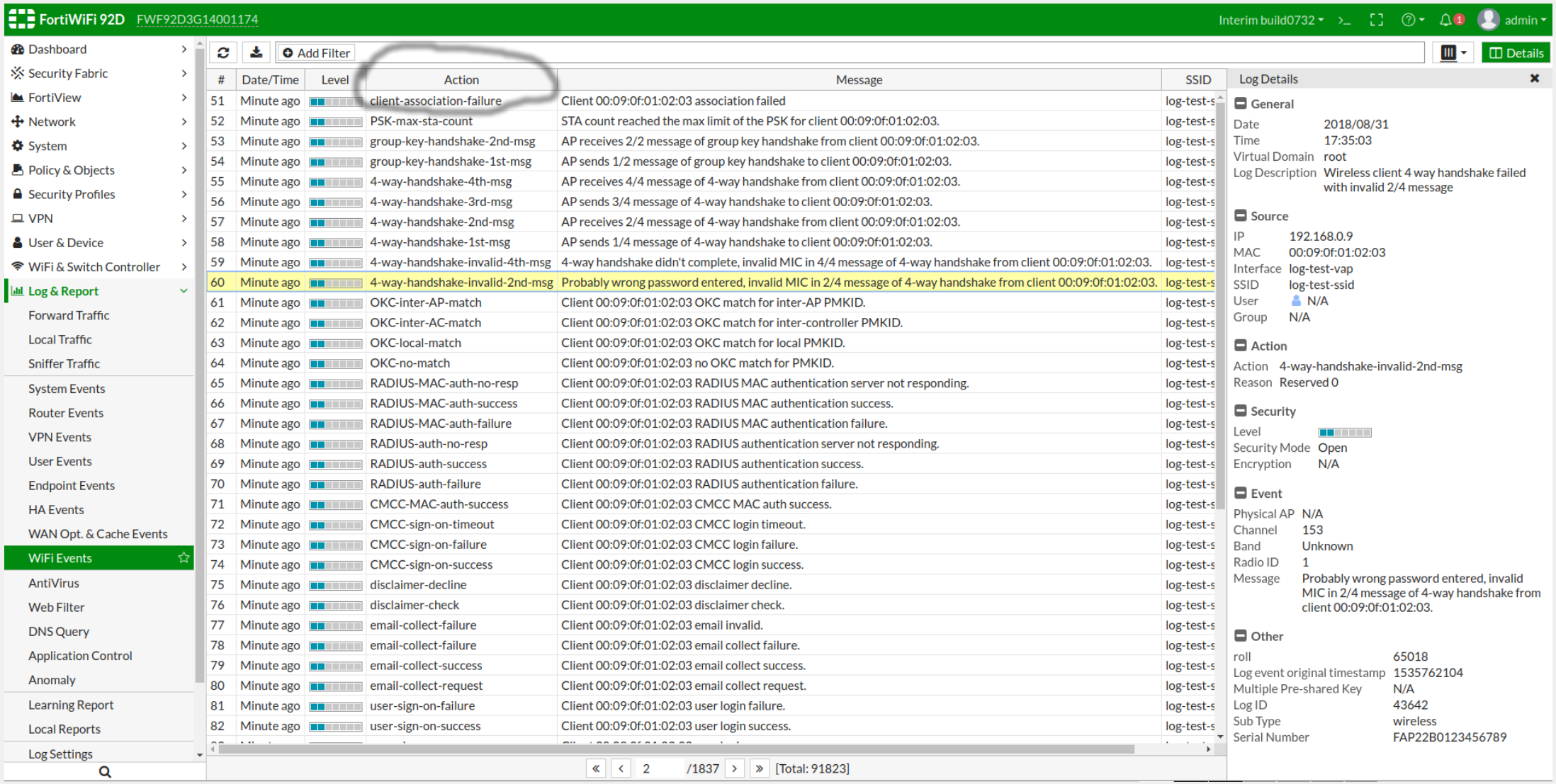


- Device information
  - OS
  - Co-relate multiple MAC
- FortiClient Status
- Endpoint Vulnerabilities
- Logged-in User
- User Avatar
- Social IDs
- Online/Off-line
- Endpoint events and logs

Automation



Detailed event logging

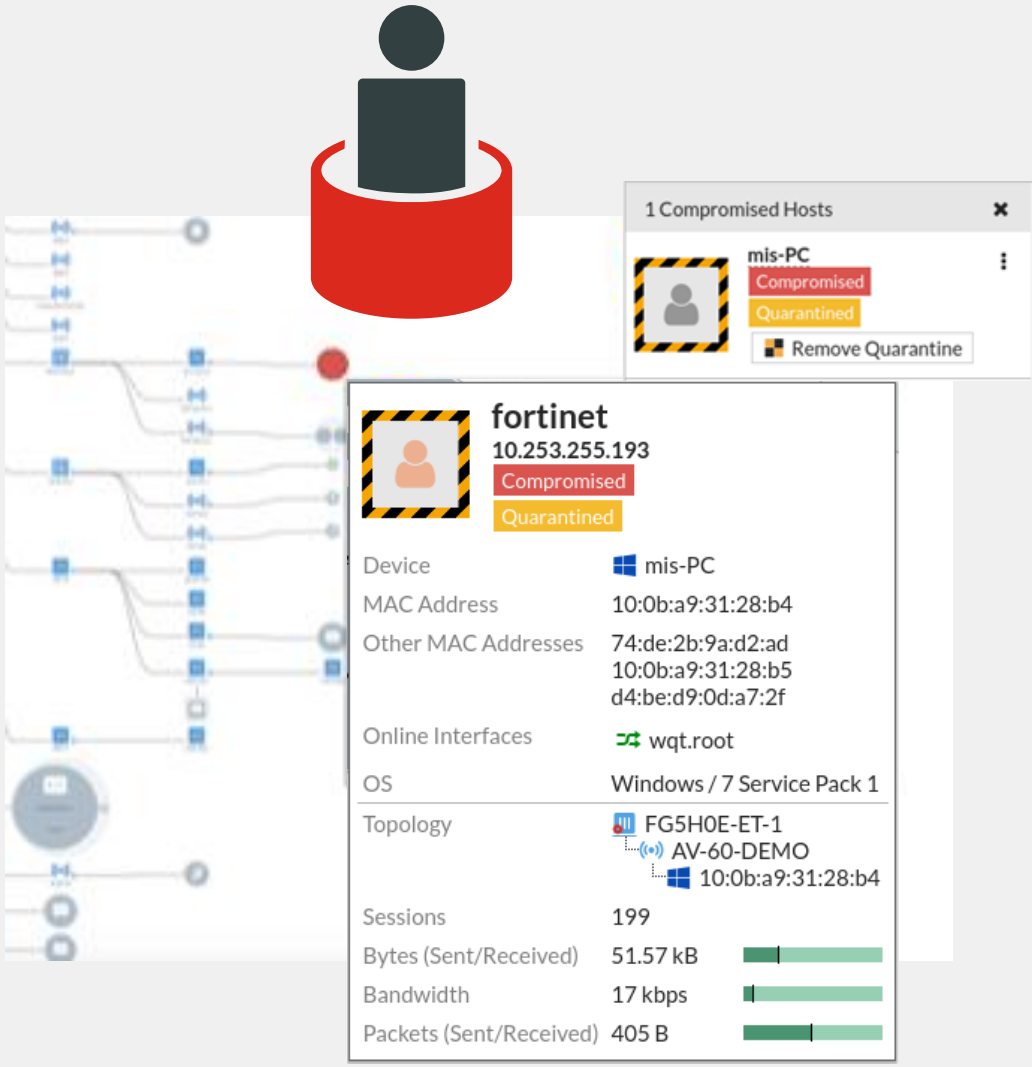


Automated response to compromised devices

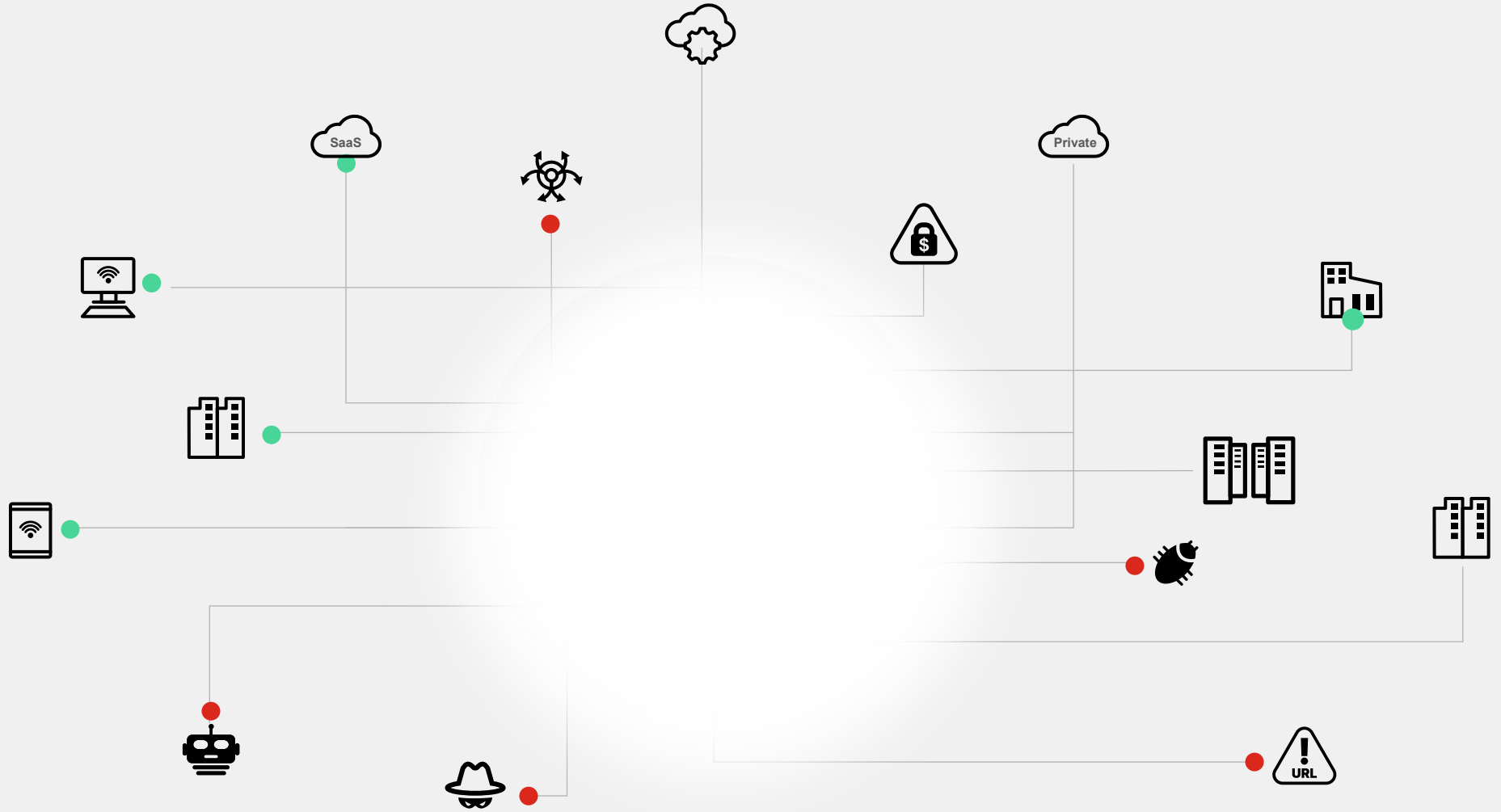
TAKING RESPONSE TIME OUT OF THE EQUATION

- How it works
  - A devices is detected as compromised by one element of the fabric
  - Switches and APs can automatically **quarantine** the device at the access layer

- Why it's important
  - Compromised IoT devices are no longer a threat to the wider network
  - Guest devices (if infected) will be dealt with automatically



You Can’t Monitor and Respond to What’s not Seen



Take end-to-end control of the attack surface and visibility

Security Fabric Analytics with FortiAnalyzer

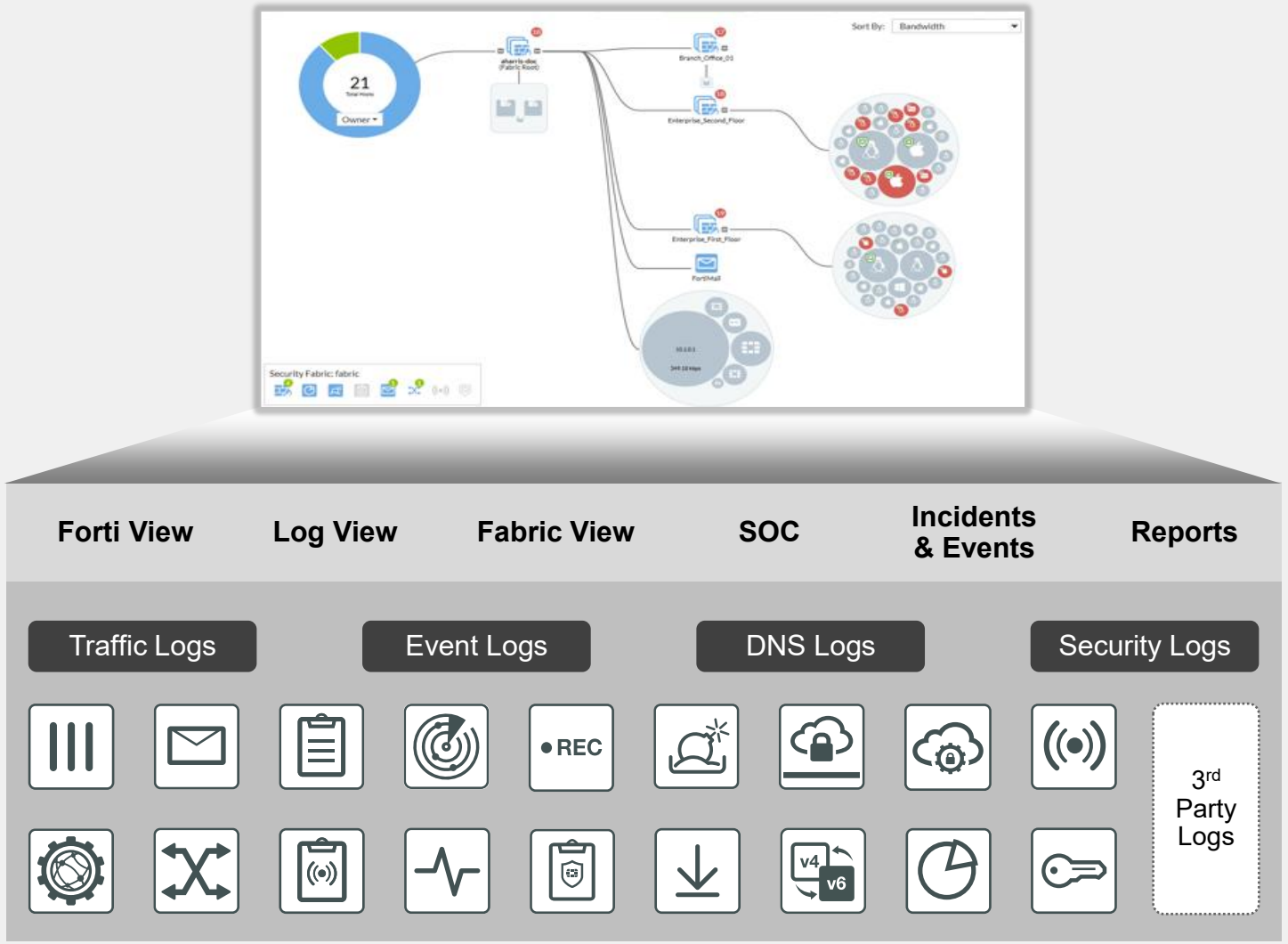
Real-time Network Insights

BUSINESS DRIVERS

Combat Advanced Threats by Identifying Network & Security Risks in Real-time

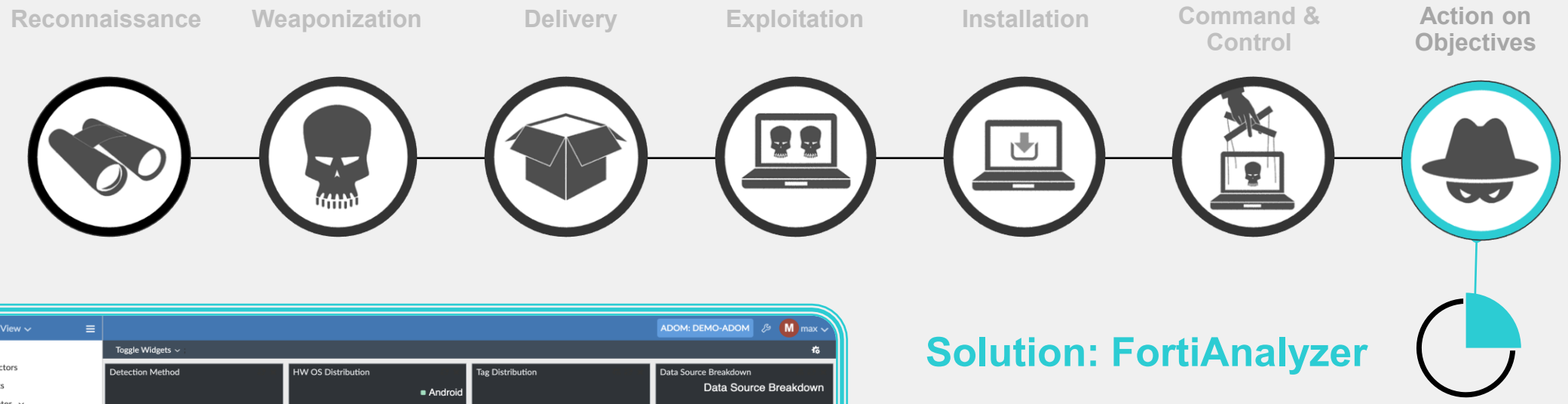
KEY CAPABILITIES

- Network Health Visibility
- Realtime SLA Reporting
- Historic SLA Reporting
- Application Usage Reports & Dashboards
- Adaptive Response Handlers



What is FortiAnalyzer?

Security Fabric Log management, analytics and reporting



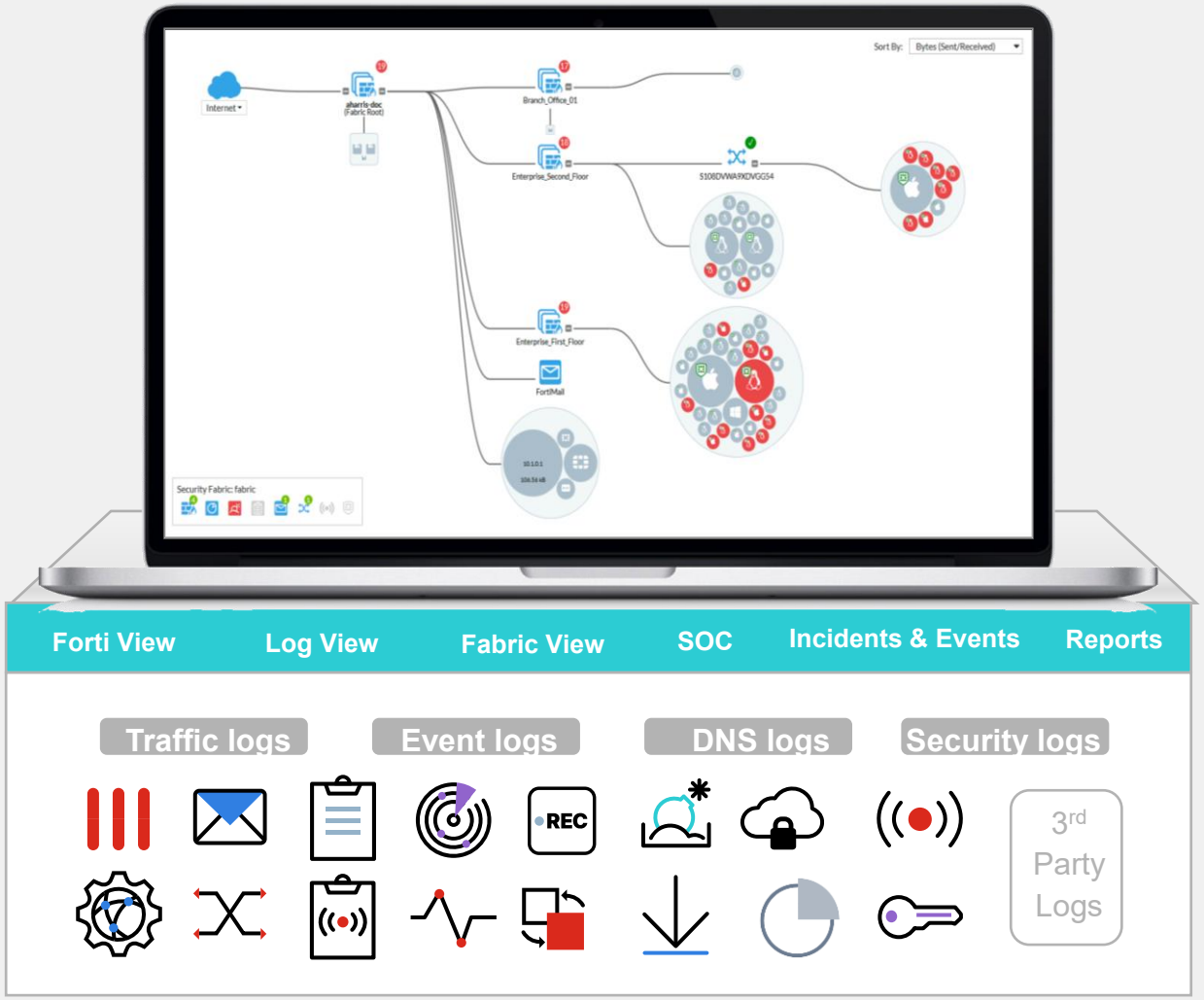
Solution: FortiAnalyzer

- ✓ End to end security management + security loggings with real time detection/analytics
- ✓ Single platform for IT, NOC & SOC visibility
- ✓ Advanced Threat Protection with Security Fabric Automation capabilities

SOC and NOC teams can use FortiAnalyzer for IOC, event handling and reporting

Security Fabric Analytics

Central Logging and Reporting for Fortinet



Strategically Consolidate Operations

- Real-Time Network & Anomaly Visibility

Capabilities

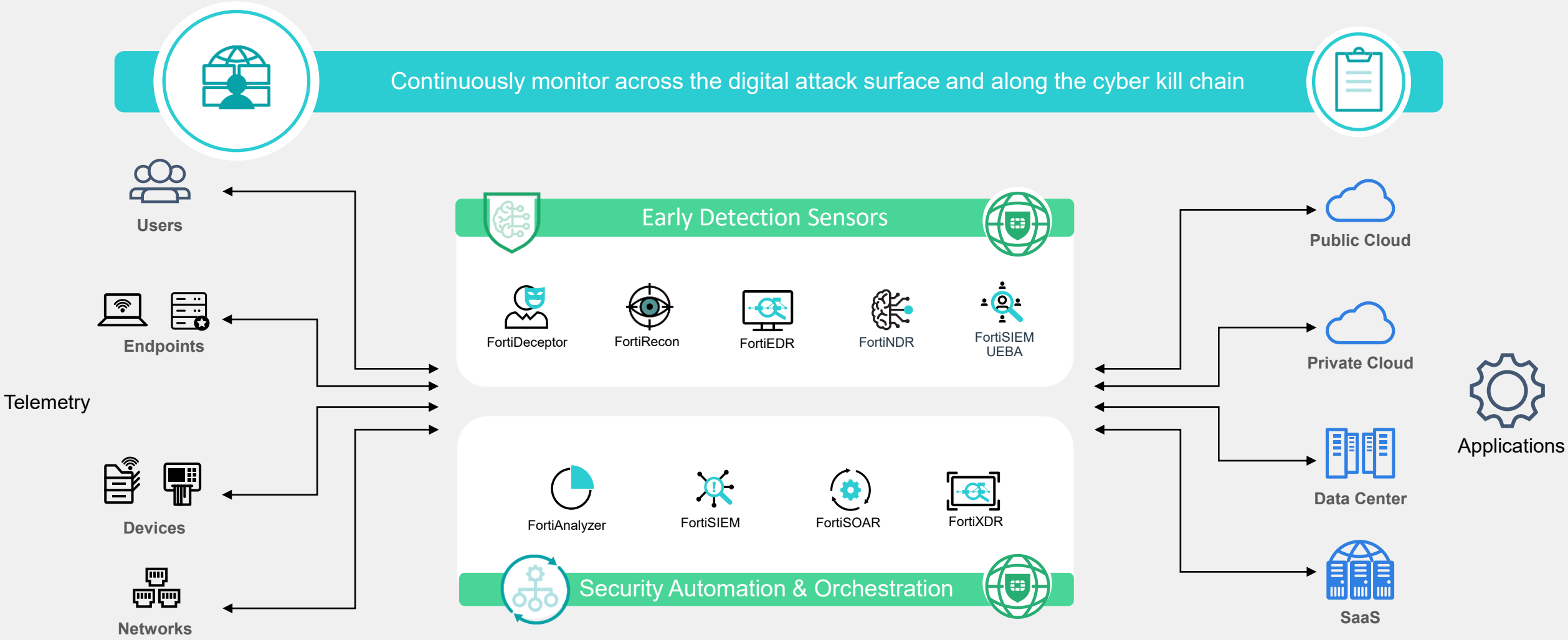
- Security Fabric Analytics & Reporting
- Policy, Events, & additional Data Correlation
- 800 Datasheet and reports

Benefits & Results

Improve Network Visibility, Risk Assessment & Eliminate Blind spots

Solution: Automated Security Operations

Speed Threat Detection and Response with AI and Automation



Fortinet Security Fabric

The industry's highest-performing integrated cybersecurity mesh platform

Product Matrix

Click on icons in this document for additional information

Fortinet Brochure
Highlighting our broad, integrated, and automated solutions, quarterly

Free Training
Fortinet is committed to training over 1 million people by 2025

Free Assessment
Perform an assessment in your network to validate your existing controls

FortiOS
The Heart of the Fortinet Security Fabric

Secure Networking

FortiGate
NGFW w/ SOC acceleration and industry-leading secure SD-WAN

FortiGate SD-WAN
Application-centric, scalable, and Secure SD-WAN with NGFW

FortiExtender
Extend scalable and resilient LTE and LAN connectivity

FortiAP
Protected LAN Edge deployments with wireless connectivity

FortiSwitch
Deliver security, performance, and manageable access to data

Linksys HomeWRK
Secure Work-from-Home solution for remote and hybrid workers

FortiNAC
Visibility, access control and automated responses for all networked devices

FortiProxy
Enforce internet, compliance and granular application control

FortiIsolator
Maintain an "air-gap" between browser and web content

Cloud Security

FortiGate VM
NGFW w/ SOC acceleration and industry-leading secure SD-WAN

FortiDDOS
Machine-learning quickly inspects traffic at layers 3, 4, and 7

FortiCNP
Manage risk and compliance through multi-cloud infrastructures

FortiDevSec
Continuous application security testing in CI/CD pipelines

FortiWeb
Prevent web application attacks against critical web assets

FortiADC
Application-aware intelligence for distribution of application traffic

FortiGSLB Cloud
Ensure business continuity during Unexpected network downtime

FortiMail
Secure mail getaway to protect against SPAM and virus attacks

FortiCASB
Prevent misconfigurations of SaaS applications and meet compliance

Zero Trust Access

FortiSASE
Enforce dynamic network access control and network segmentation

ZTNA Agent
Remote access, application access, and risk reduction

FortiAuthenticator
Identify users wherever they are and enforce strong authentication

FortiToken
One-time password application with push notification

FortiClient Fabric Agent
IPSec and SSL VPN tunnel, endpoint telemetry and more

FortiGuest
Simplified guest access, BYOD, and policy management

FortiGuard Threat Intelligence

Powered by FortiGuard Labs

Fabric Management Center: NOC

FortiManager
Centralized management of your Fortinet security infrastructure

FortiGate Cloud
Saas w/ zero touch deployment, configuration, and management

FortiMonitor
Analysis tool to provide NOC and SOC monitoring capabilities

FortiAIOps
Network inspection to rapidly analyze, enable, and correlate

FortiExtender Cloud
Deploy, manage and customize LTE internet access

FNDN
Exclusive developer community for access to advanced tools & scripts

Open Ecosystem

The industry's most extensive ecosystem of integrated solutions

Fabric Connectors
Fortinet-developed

DevOp Tools & Script
Fortinet & community-driven

Fabric API Integration
Partner-led

Extended Ecosystem
Threat sharing w/ tech vendors

Fabric Management Center: SOC

FortiDeceptor
Discover active attackers inside with decoy assets

FortiNDR
Accelerate mitigation of evolving threats and threat investigation

FortiEDR
Automated protection and orchestrated incident response

FortiSandbox / FortiAI
Secure virtual runtime environment to expose unknown threats

FortiAnalyzer
Correlation, reporting, and log management in Security Fabric

FortiSIEM
Integrated security, performance, and availability monitoring

FortiSOAR
Automated security operations, analytics, and response

FortiTester
Network performance testing and breach attack simulation (BAS)

SOC-as-a-Service
Continuous awareness and control of events, alerts, and threats

Incident Response Service
Digital forensic analysis, response, containment, and guidance

Support & Mitigation Services

FortiCare Essentials*
15% of hardware

FortiCare Premium*
20% of hardware

FortiCare Elite**
25% of hardware

FortiConverter
25% of hardware

* FortiCare Premium is formerly 24x7 Support. Lower support price for Switches and APs

** Response time for High Priority tickets. Available for FortiGate, FortiManager, FortiAnalyzer, FortiSwitch, and FortiAP

Communication and Surveillance

FortiFone
Robust IP Phones w/ HD Audio with centralized management

FortiVoice
Integrated voice, chat, conferencing management, and fax with centralized

FortiCamera
HDTV-quality surveillance cameras for physical safety and security

FortiRecorder
High-performance NVR with AI-powered video management software


FORTINET