

Fortinet Security Fabric

Krzysztof Sieniawski

CROWDSTRIKE

ExtraHop

FORTINET



HPE JUNIPER
networking

infoblox

Trellix

nomios

ARROW

ectacom

EXCLUSIVE
NETWORKS

CLICO



Fortinet Security Fabric

Broad

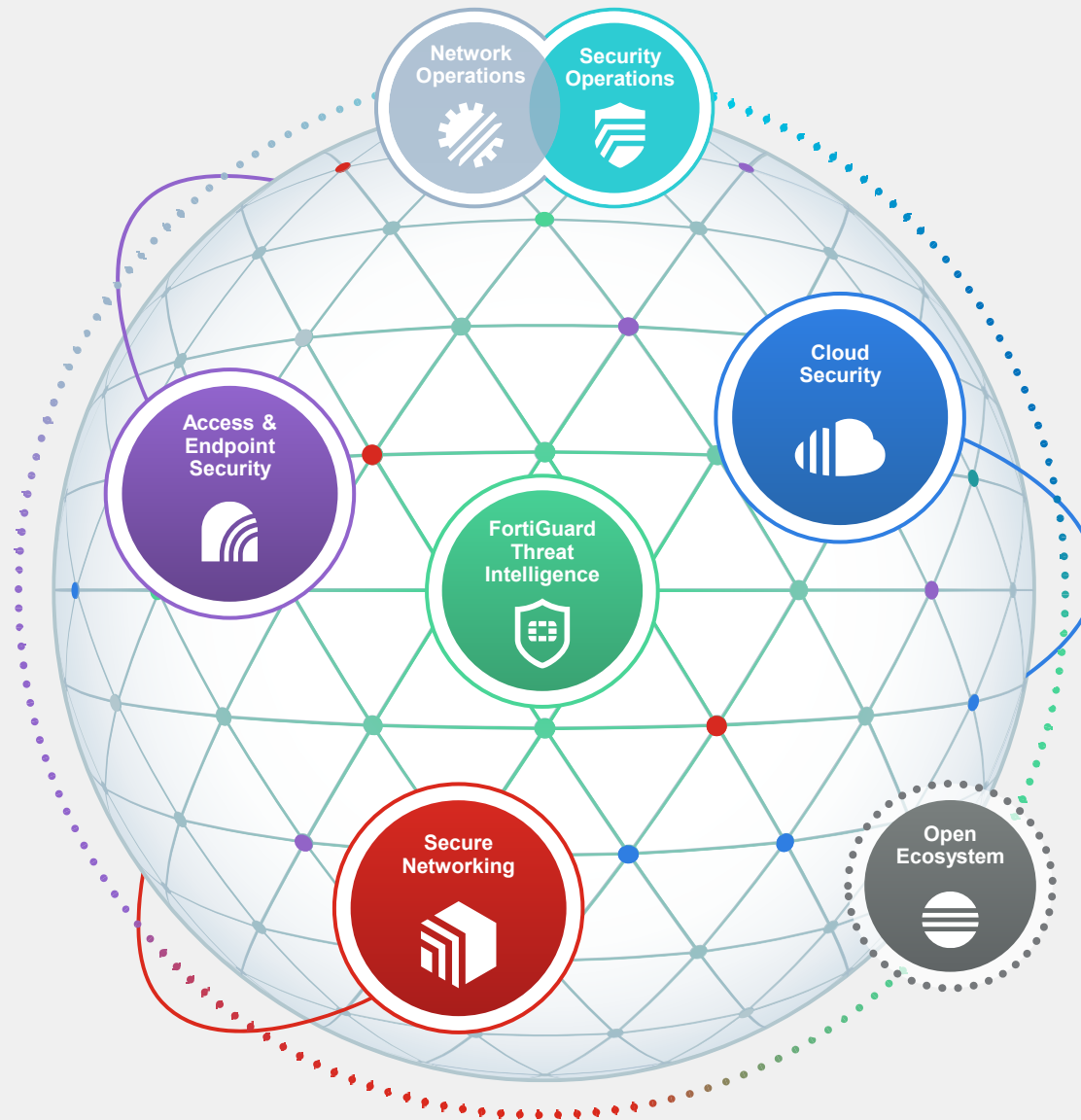
visibility and protection of the entire digital attack surface to better manage risk

Integrated

solution that reduces management complexity and shares threat intelligence

Automated

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



Appliance



Virtual



Hosted



Cloud



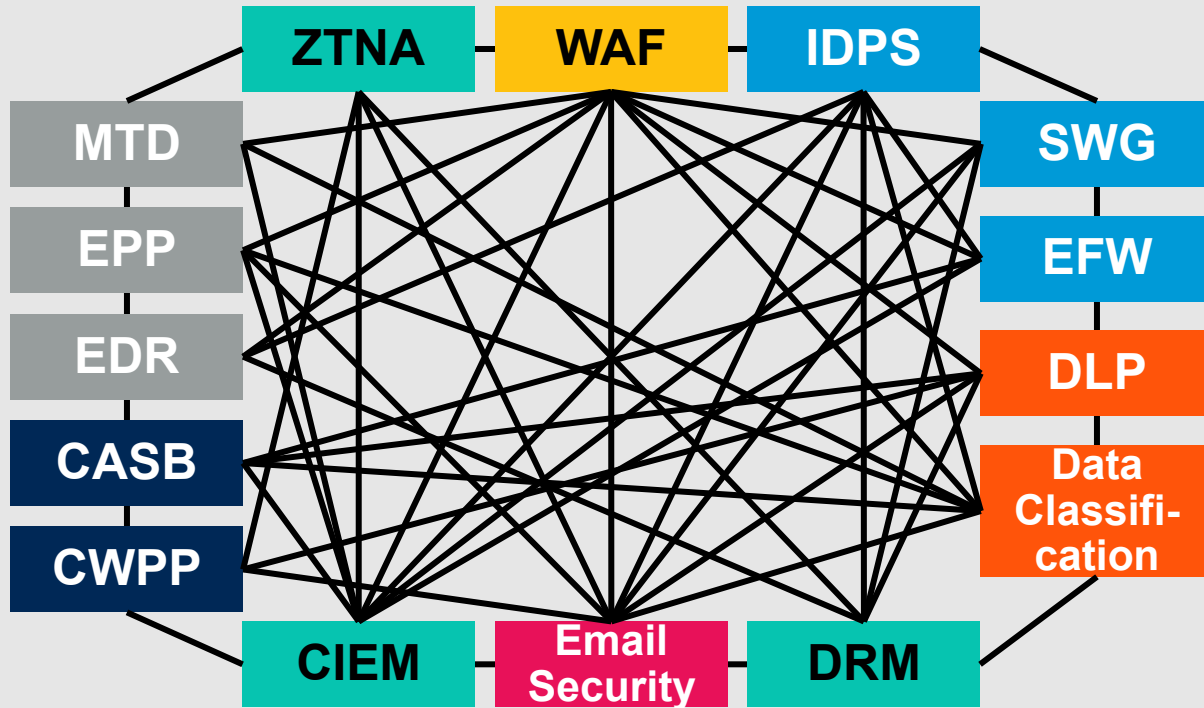
Agent



Container

Fortinet Security Fabric as CyberSecurity Mesh

Gartner



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



FortiSolator
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 gateway 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



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



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



FortiGuard Threat Intelligence

Powered by FortiGuard Labs



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

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

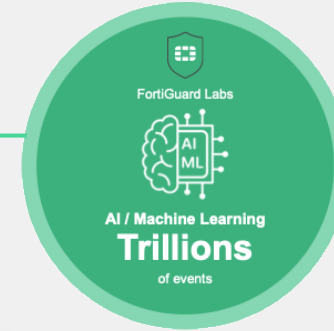


Fortinet's Network Firewall Solution

SecOps



FortiGuard



OS, Management & Analytics



FortiOS



FortiAnalyzer

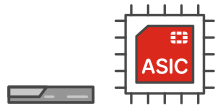


FortiAI



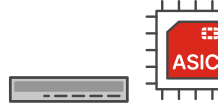
FortiManager

Branch



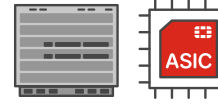
FortiGate
40-90 Series

Campus



FortiGate
100-900 Series

Data Center



FortiGate
1000-7000 Series

VM / Cloud / FWaaS



FortiGate VM



FortiCNF



FGaaS

Secure LAN Edge



FortiExtender



FortiAP



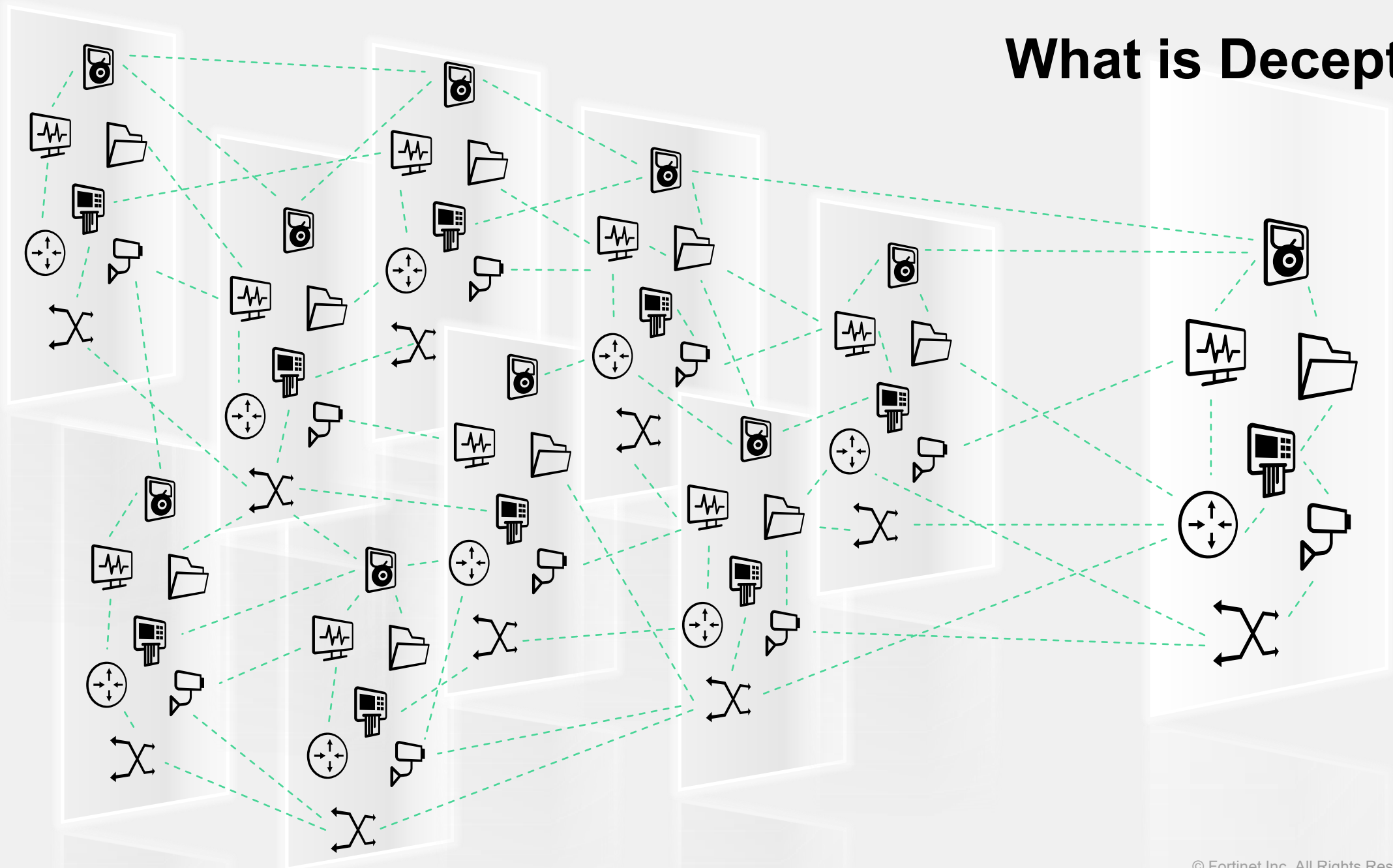
FortiSwitch



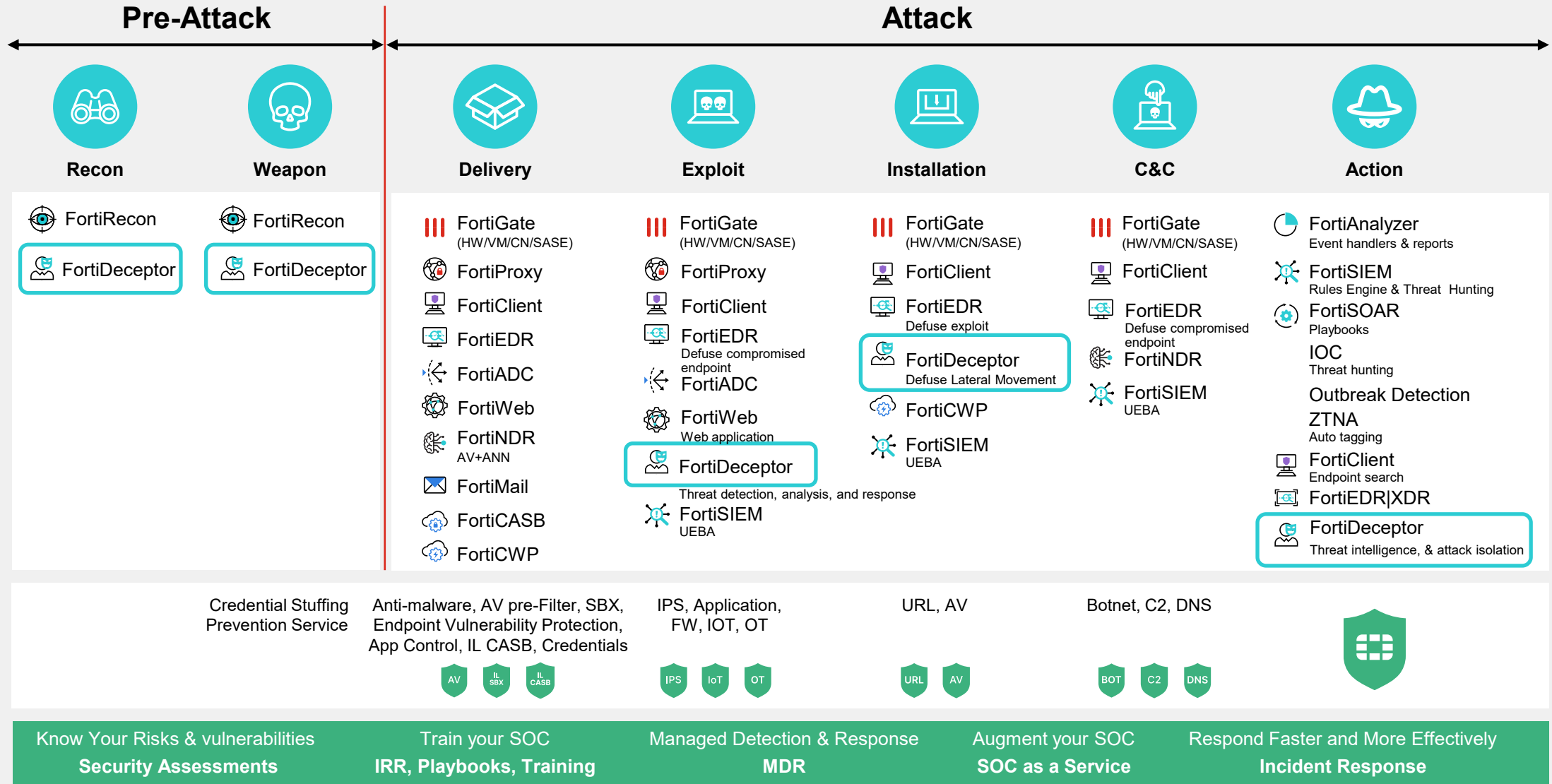
FortiNAC



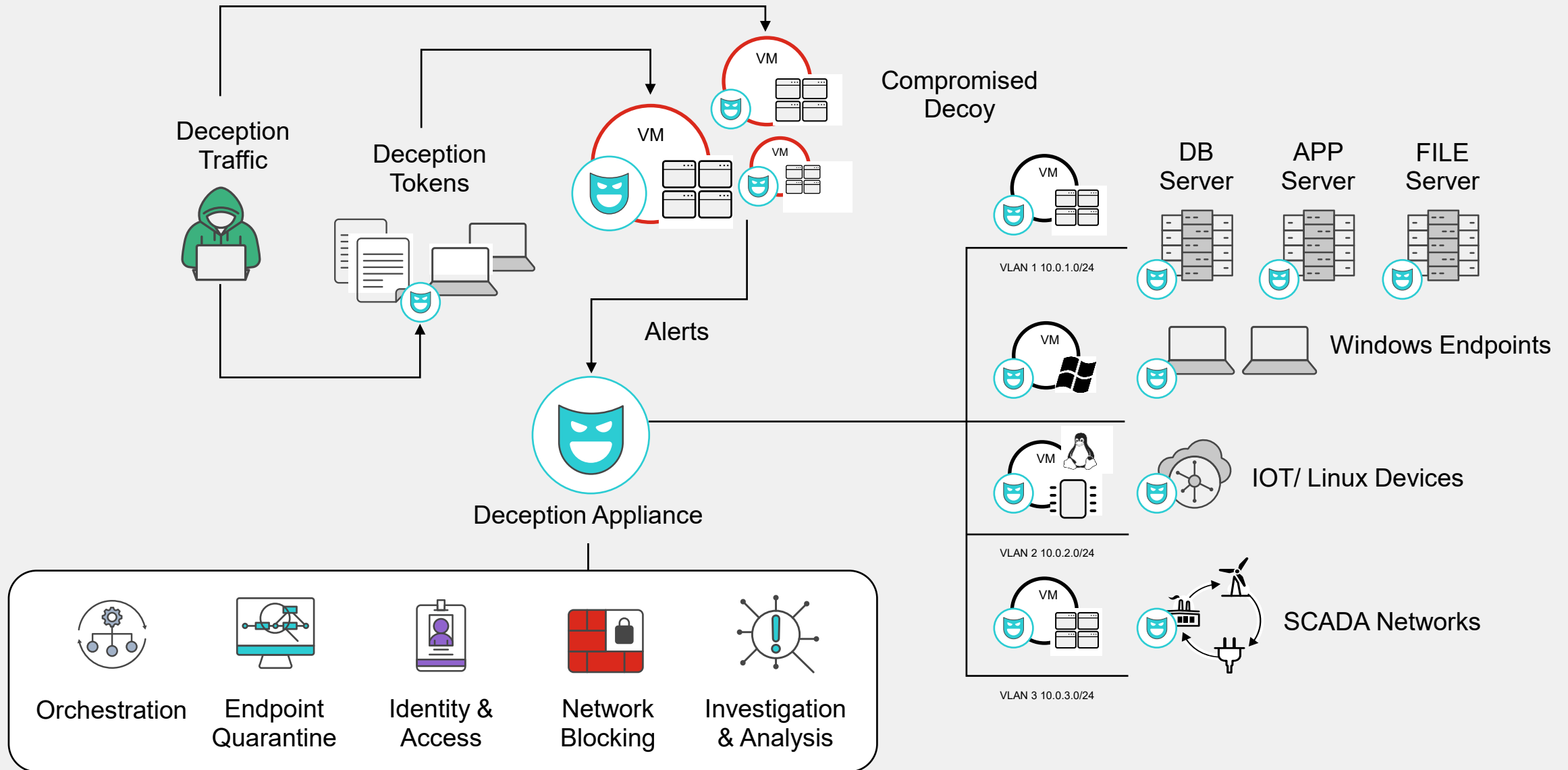
What is Deception?



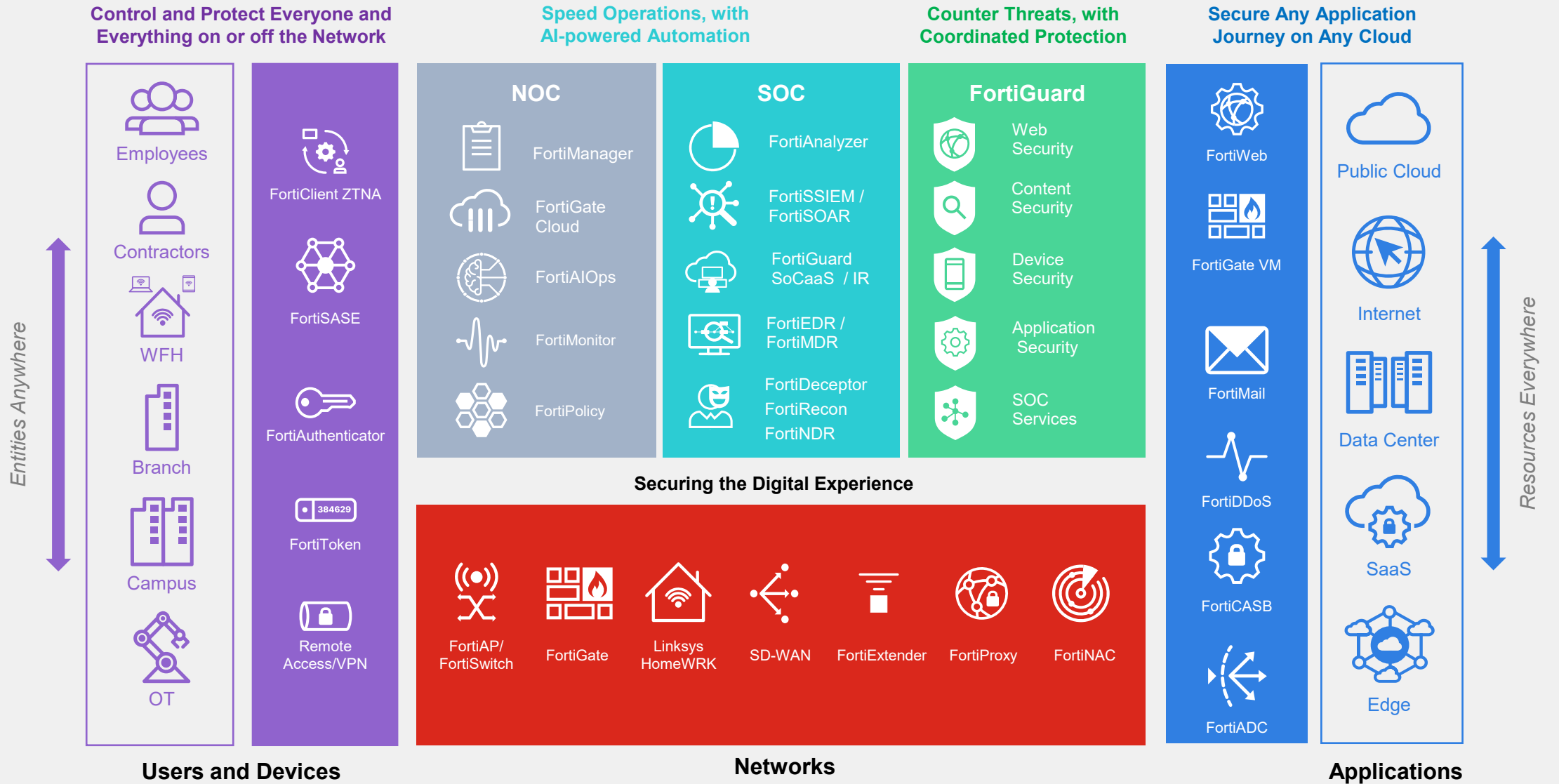
How to Break the Attack Sequence — FortiDeceptor Support



How Deception Works

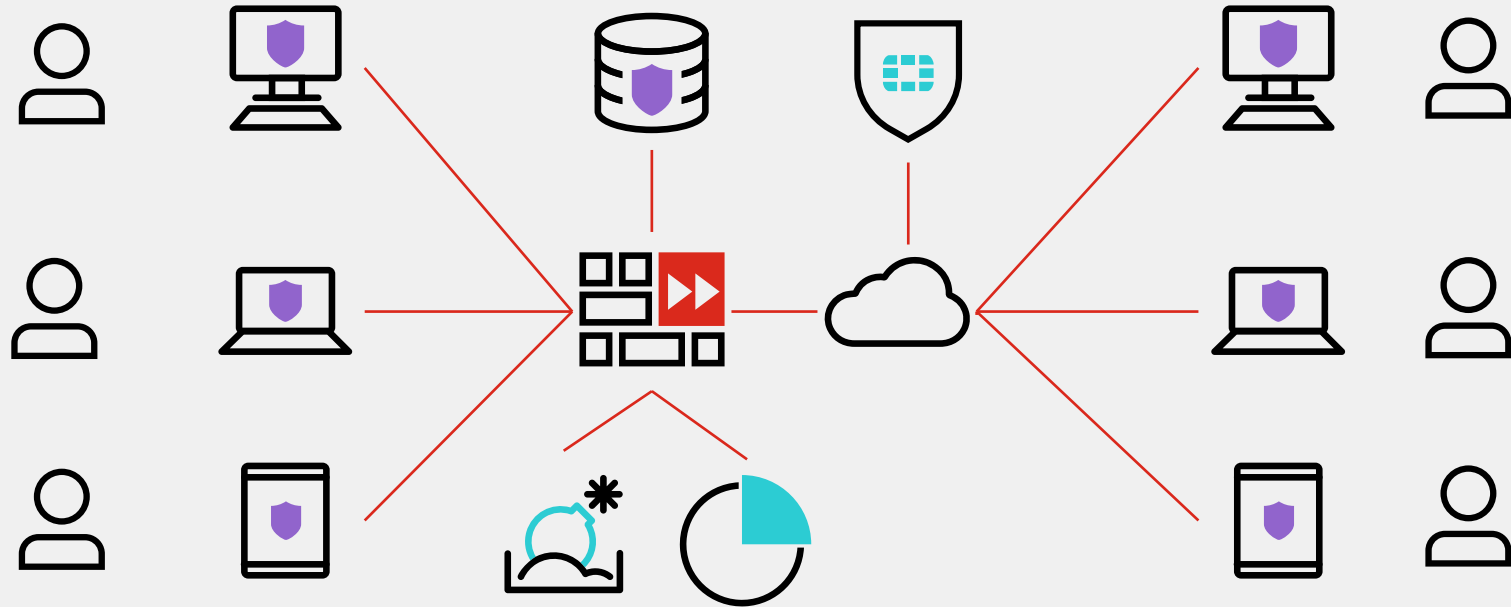


Fortinet Security Fabric Expansion



Zero Trust Access—Device Visibility & Control

FortiClient for Fabric Agent, Remote Access, and Endpoint Protection



Hygiene Control

- Vulnerability scanning
- FortiGuard Web Filtering
- Patching Policy
- Dynamic grouping

Secure Remote Access

- Zero Trust Network Access (ZTNA)
- VPN (IPSec & SSL)
- Single Sign On (SSO)

Endpoint Protection

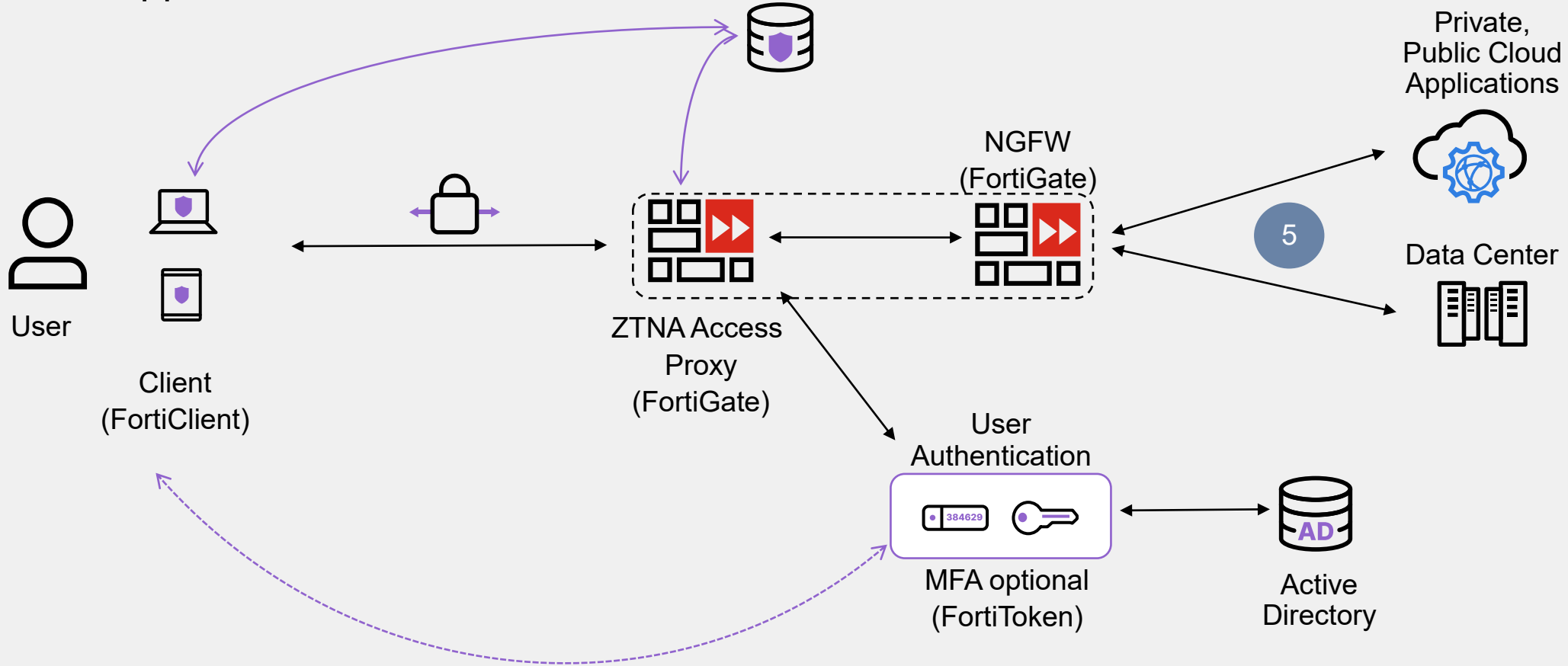
- FortiGuard ML-based AV
- Sandbox integration
- Anti-exploit
- Automated containment



Zero Trust Network Access (ZTNA) Technology



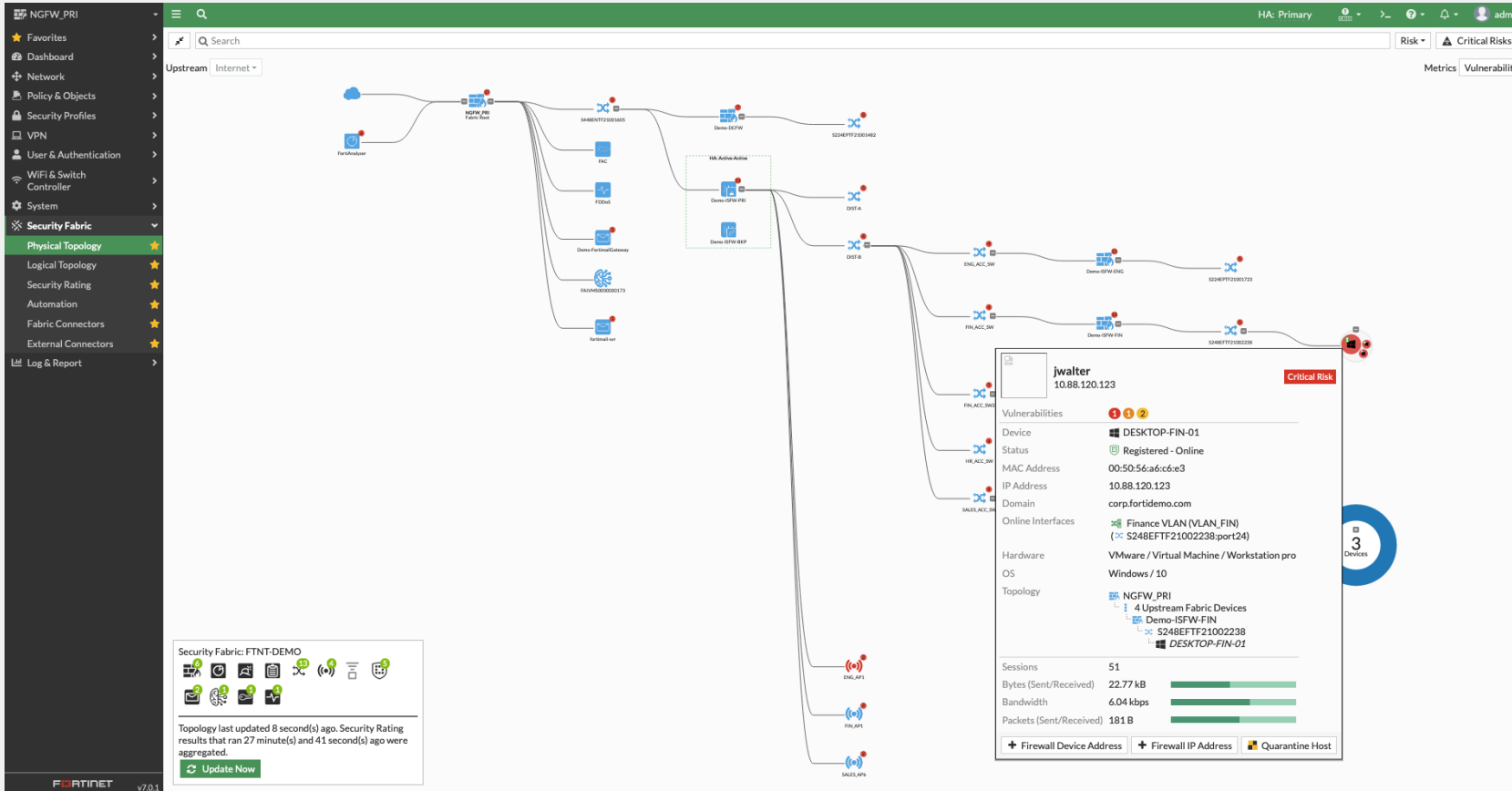
Granular Application Access



- 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

NGFW_PRI HA: Primary admin

Stitch Trigger Action

+ Create New View Delete Clone Search

Name	Status	Trigger	Actions	FortiGate(s)	Trigger Count	Last Triggered
Compromised Host 3						
AutoQ	Disabled	AutoQ	<ul style="list-style-type: none"> AutoQ_quarantine AutoQ_quarantine-forticlient AutoQ_ban-ip 	All FortiGates	0	
Compromised Host Quarantine	Disabled	Compromised Host Quarantine	<ul style="list-style-type: none"> Compromised Host Quarantine_quarantine Compromised Host Quarantine_quarantine-forticlient 	All FortiGates	0	
FortiClient	Enabled	FortiClient	<ul style="list-style-type: none"> FortiClient_quarantine-forticlient FortiClient_ban-ip 	All FortiGates	0	
FortiAnalyzer Event Handler 1						
FAZ-Automation-Trigger	Disabled	FAZ-Automation-Trigger	FAZ-Automation-Trigger_ios-notification	All FortiGates	0	
FortiOS Event Log 2						
FortiAnalyzer Connection Down	Enabled	FortiAnalyzer Connection Down	FortiAnalyzer Connection Down_ios-notification	All FortiGates	1,973	14 seconds ago
Network Down	Disabled	Network Down	Network Down_email	All FortiGates	0	
HA Failover 1						
HA Failover	Disabled	HA Failover	HA Failover_email	All FortiGates	0	
Incoming Webhook 1						
Incoming Webhook Quarantine	Disabled	Incoming Webhook Call	<ul style="list-style-type: none"> Compromised Host Quarantine_quarantine Compromised Host Quarantine_quarantine-forticlient 	All FortiGates	0	
License Expiry 1						
License Expired Notification	Enabled	License Expired Notification	License Expired Notification_ios-notification	All FortiGates	0	
Reboot 1						
Reboot	Disabled	Reboot	Reboot_email	All FortiGates	0	
Security Rating Summary 1						
Security Rating Notification	Enabled	Security Rating Notification	Security Rating Notification_ios-notification	All FortiGates	5	40 minutes ago

11 Updated: 17:04:11



Detailed event logging

FortiWiFi 92D FWF92D3G14001174 Interim build0732 admin

Dashboard Security Fabric FortiView Network System Policy & Objects Security Profiles VPN User & Device WiFi & Switch Controller **Log & Report** Forward Traffic Local Traffic Sniffer Traffic System Events Router Events VPN Events User Events Endpoint Events HA Events WAN Opt. & Cache Events WiFi Events AntiVirus Web Filter DNS Query Application Control Anomaly Learning Report Local Reports Log Settings

#	Date/Time	Level	Action	Message	SSID	Log Details
51	Minute ago	client-association-failure	client-association-failure	Client 00:09:0f:01:02:03 association failed	log-test-s	
52	Minute ago	PSK-max-sta-count	PSK-max-sta-count	STA count reached the max limit of the PSK for client 00:09:0f:01:02:03.	log-test-s	
53	Minute ago	group-key-handshake-2nd-msg	group-key-handshake-2nd-msg	AP receives 2/2 message of group key handshake from client 00:09:0f:01:02:03.	log-test-s	
54	Minute ago	group-key-handshake-1st-msg	group-key-handshake-1st-msg	AP sends 1/2 message of group key handshake to client 00:09:0f:01:02:03.	log-test-s	
55	Minute ago	4-way-handshake-4th-msg	4-way-handshake-4th-msg	AP receives 4/4 message of 4-way handshake from client 00:09:0f:01:02:03.	log-test-s	
56	Minute ago	4-way-handshake-3rd-msg	4-way-handshake-3rd-msg	AP sends 3/4 message of 4-way handshake to client 00:09:0f:01:02:03.	log-test-s	
57	Minute ago	4-way-handshake-2nd-msg	4-way-handshake-2nd-msg	AP receives 2/4 message of 4-way handshake from client 00:09:0f:01:02:03.	log-test-s	
58	Minute ago	4-way-handshake-1st-msg	4-way-handshake-1st-msg	AP sends 1/4 message of 4-way handshake to client 00:09:0f:01:02:03.	log-test-s	
59	Minute ago	4-way-handshake-invalid-4th-msg	4-way-handshake-invalid-4th-msg	4-way handshake didn't complete, invalid MIC in 4/4 message of 4-way handshake from client 00:09:0f:01:02:03.	log-test-s	
60	Minute ago	4-way-handshake-invalid-2nd-msg	4-way-handshake-invalid-2nd-msg	Probably wrong password entered, invalid MIC in 2/4 message of 4-way handshake from client 00:09:0f:01:02:03.	log-test-s	<p>General</p> <p>Date 2018/08/31 Time 17:35:03 Virtual Domain root Log Description Wireless client 4 way handshake failed with invalid 2/4 message</p> <p>Source</p> <p>IP 192.168.0.9 MAC 00:09:0f:01:02:03 Interface log-test-vap SSID log-test-ssid User N/A Group N/A</p> <p>Action</p> <p>Action 4-way-handshake-invalid-2nd-msg Reason Reserved 0</p> <p>Security</p> <p>Level Security Mode Open Encryption N/A</p> <p>Event</p> <p>Physical AP N/A Channel 153 Band Unknown Radio ID 1 Message Probably wrong password entered, invalid MIC in 2/4 message of 4-way handshake from client 00:09:0f:01:02:03.</p> <p>Other</p> <p>roll 65018 Log event original timestamp 1535762104 Multiple Pre-shared Key N/A Log ID 43642 Sub Type wireless Serial Number FAP22B0123456789</p>
61	Minute ago	OKC-inter-AP-match	OKC-inter-AP-match	Client 00:09:0f:01:02:03 OKC match for inter-AP PMKID.	log-test-s	
62	Minute ago	OKC-inter-AC-match	OKC-inter-AC-match	Client 00:09:0f:01:02:03 OKC match for inter-controller PMKID.	log-test-s	
63	Minute ago	OKC-local-match	OKC-local-match	Client 00:09:0f:01:02:03 OKC match for local PMKID.	log-test-s	
64	Minute ago	OKC-no-match	OKC-no-match	Client 00:09:0f:01:02:03 no OKC match for PMKID.	log-test-s	
65	Minute ago	RADIUS-MAC-auth-no-resp	RADIUS-MAC-auth-no-resp	Client 00:09:0f:01:02:03 RADIUS MAC authentication server not responding.	log-test-s	
66	Minute ago	RADIUS-MAC-auth-success	RADIUS-MAC-auth-success	Client 00:09:0f:01:02:03 RADIUS MAC authentication success.	log-test-s	
67	Minute ago	RADIUS-MAC-auth-failure	RADIUS-MAC-auth-failure	Client 00:09:0f:01:02:03 RADIUS MAC authentication failure.	log-test-s	
68	Minute ago	RADIUS-auth-no-resp	RADIUS-auth-no-resp	Client 00:09:0f:01:02:03 RADIUS authentication server not responding.	log-test-s	
69	Minute ago	RADIUS-auth-success	RADIUS-auth-success	Client 00:09:0f:01:02:03 RADIUS authentication success.	log-test-s	
70	Minute ago	RADIUS-auth-failure	RADIUS-auth-failure	Client 00:09:0f:01:02:03 RADIUS authentication failure.	log-test-s	
71	Minute ago	CMCC-MAC-auth-success	CMCC-MAC-auth-success	Client 00:09:0f:01:02:03 CMCC MAC auth success.	log-test-s	
72	Minute ago	CMCC-sign-on-timeout	CMCC-sign-on-timeout	Client 00:09:0f:01:02:03 CMCC login timeout.	log-test-s	
73	Minute ago	CMCC-sign-on-failure	CMCC-sign-on-failure	Client 00:09:0f:01:02:03 CMCC login failure.	log-test-s	
74	Minute ago	CMCC-sign-on-success	CMCC-sign-on-success	Client 00:09:0f:01:02:03 CMCC login success.	log-test-s	
75	Minute ago	disclaimer-decline	disclaimer-decline	Client 00:09:0f:01:02:03 disclaimer decline.	log-test-s	
76	Minute ago	disclaimer-check	disclaimer-check	Client 00:09:0f:01:02:03 disclaimer check.	log-test-s	
77	Minute ago	email-collect-failure	email-collect-failure	Client 00:09:0f:01:02:03 email invalid.	log-test-s	
78	Minute ago	email-collect-failure	email-collect-failure	Client 00:09:0f:01:02:03 email collect failure.	log-test-s	
79	Minute ago	email-collect-success	email-collect-success	Client 00:09:0f:01:02:03 email collect success.	log-test-s	
80	Minute ago	email-collect-request	email-collect-request	Client 00:09:0f:01:02:03 email collect request.	log-test-s	
81	Minute ago	user-sign-on-failure	user-sign-on-failure	Client 00:09:0f:01:02:03 user login failure.	log-test-s	
82	Minute ago	user-sign-on-success	user-sign-on-success	Client 00:09:0f:01:02:03 user login success.	log-test-s	

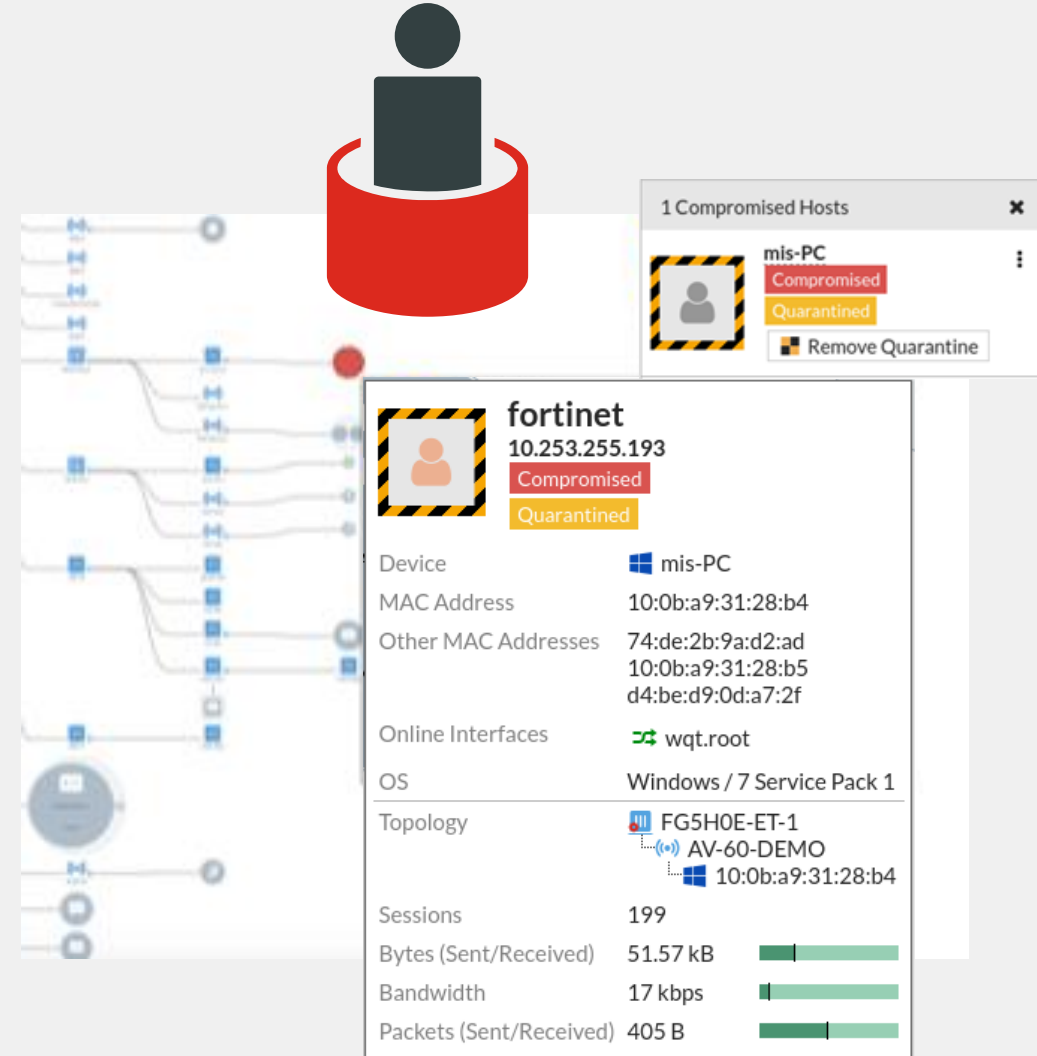
<< < 2 /1837 > >> [Total: 91823]



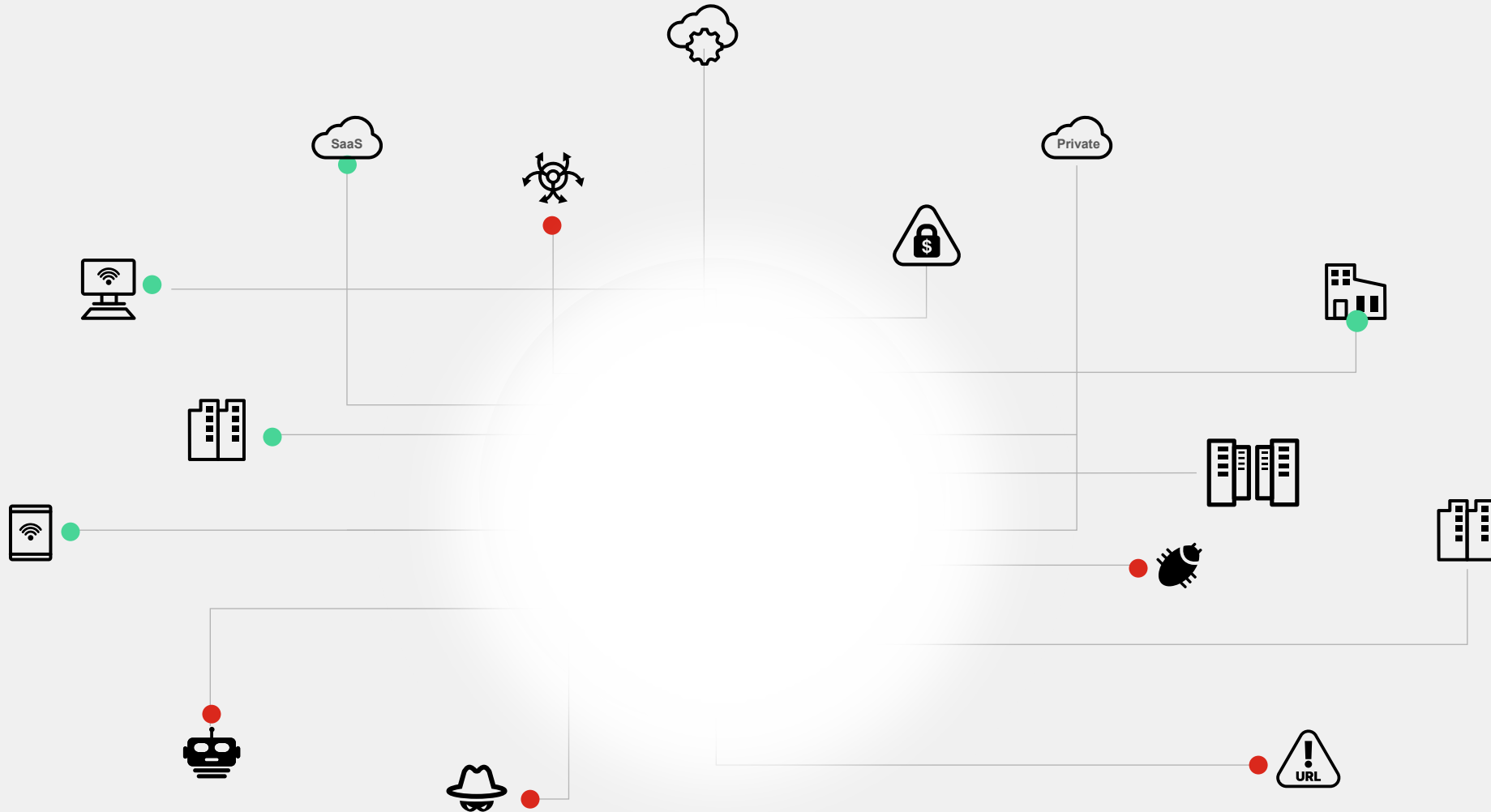
Automated response to compromised devices

TAKING RESPONSE TIME OUT OF THE EQUATION

- How it works
 - A device 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

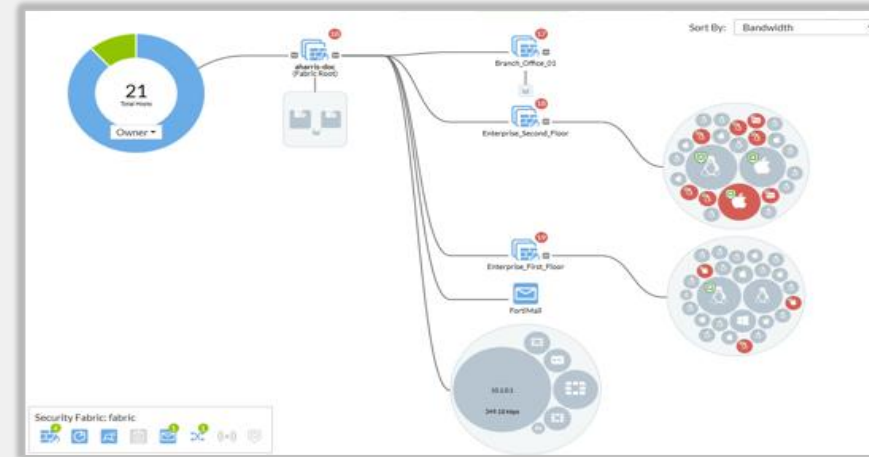
Real-time Network Insights

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



Forti View	Log View	Fabric View	SOC	Incidents & Events	Reports				
Traffic Logs		Event Logs		DNS Logs		Security Logs			
☰	✉	📄	🎯	• REC	☀️	🔒	☁️	📶	3rd Party Logs
⚙️	↔️	📄	📈	📄	↓	v4 v6	📊	🔑	



What is FortiAnalyzer?

Security Fabric Log management, analytics and reporting

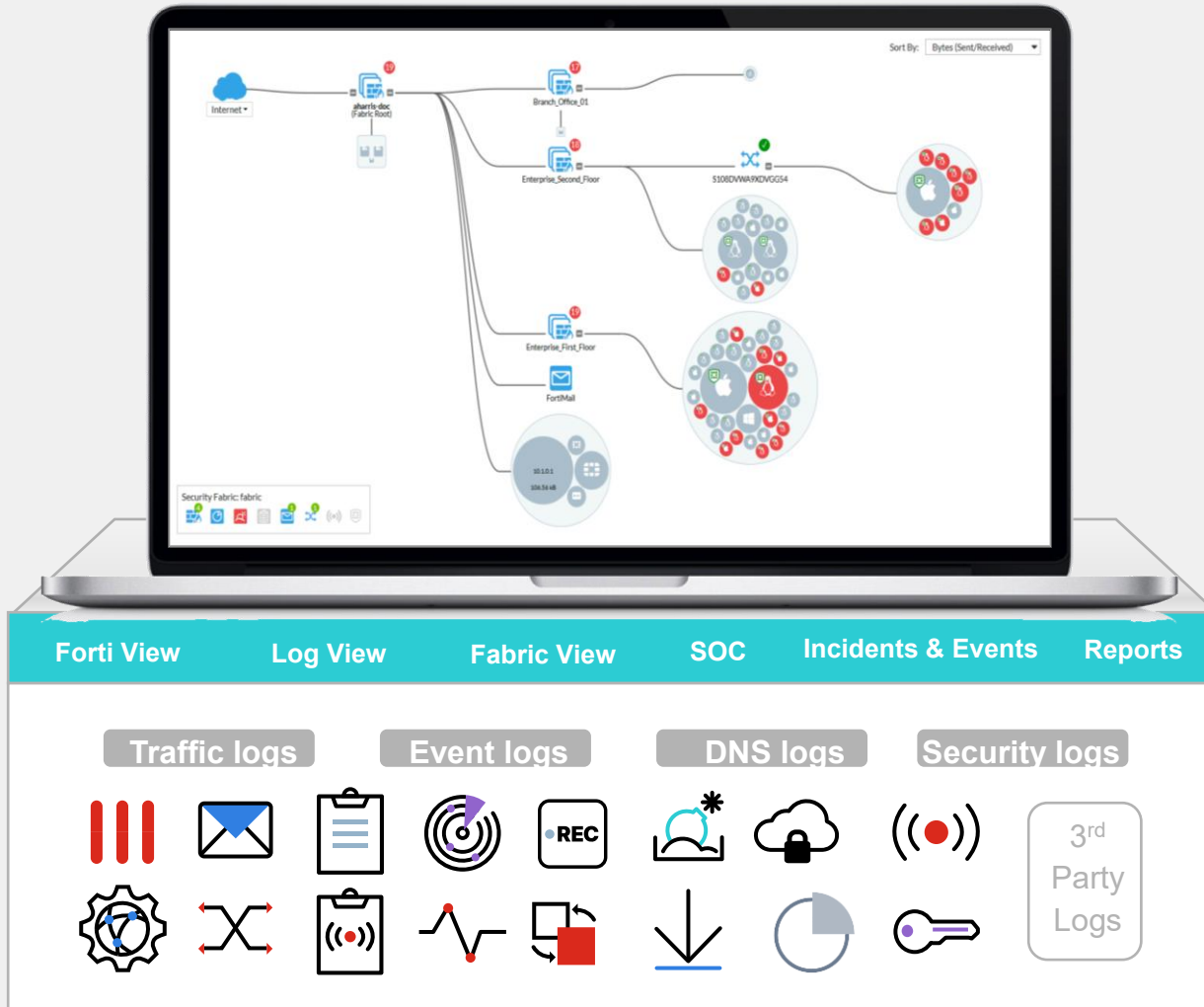


Solution: FortiAnalyzer

- ✓ 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

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

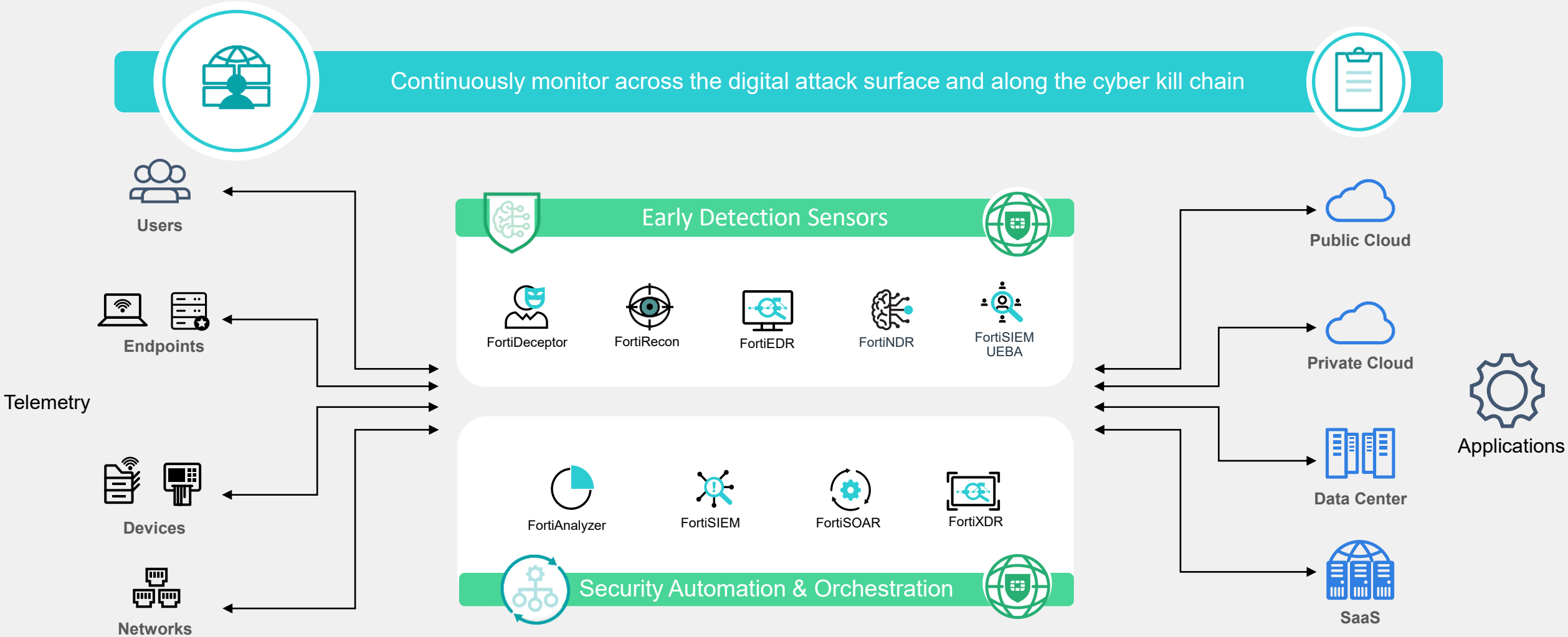


Improve Network Visibility, Risk Assessment & Eliminate Blind spots



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 to training over 1 million people by 2025

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 gateway 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



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®