



FORTINET[®]

ZTNA-Integration von zero Trust-Strategien

Forti Client





Need for Security Platform



Through 2021,
99% of vulnerabilities exploited will continue to be ones known by security and IT professionals for at least one year.

Need for Cyber Hygiene



Global Workplace Analytics

25-30% of the workforce will be working-from-home multiple days a week by the end of 2021

Work From Anywhere



68% IT security professionals say their company experienced one or more endpoint attacks

Endpoint Protection Needed

Sources:

1. Gartner, Craig Lawson
2. Global Workplace Analytics
3. The Third Annual Study on the State of Endpoint Security Risk, Ponemon Institute, 2020



Fortinet Security Fabric

Broad

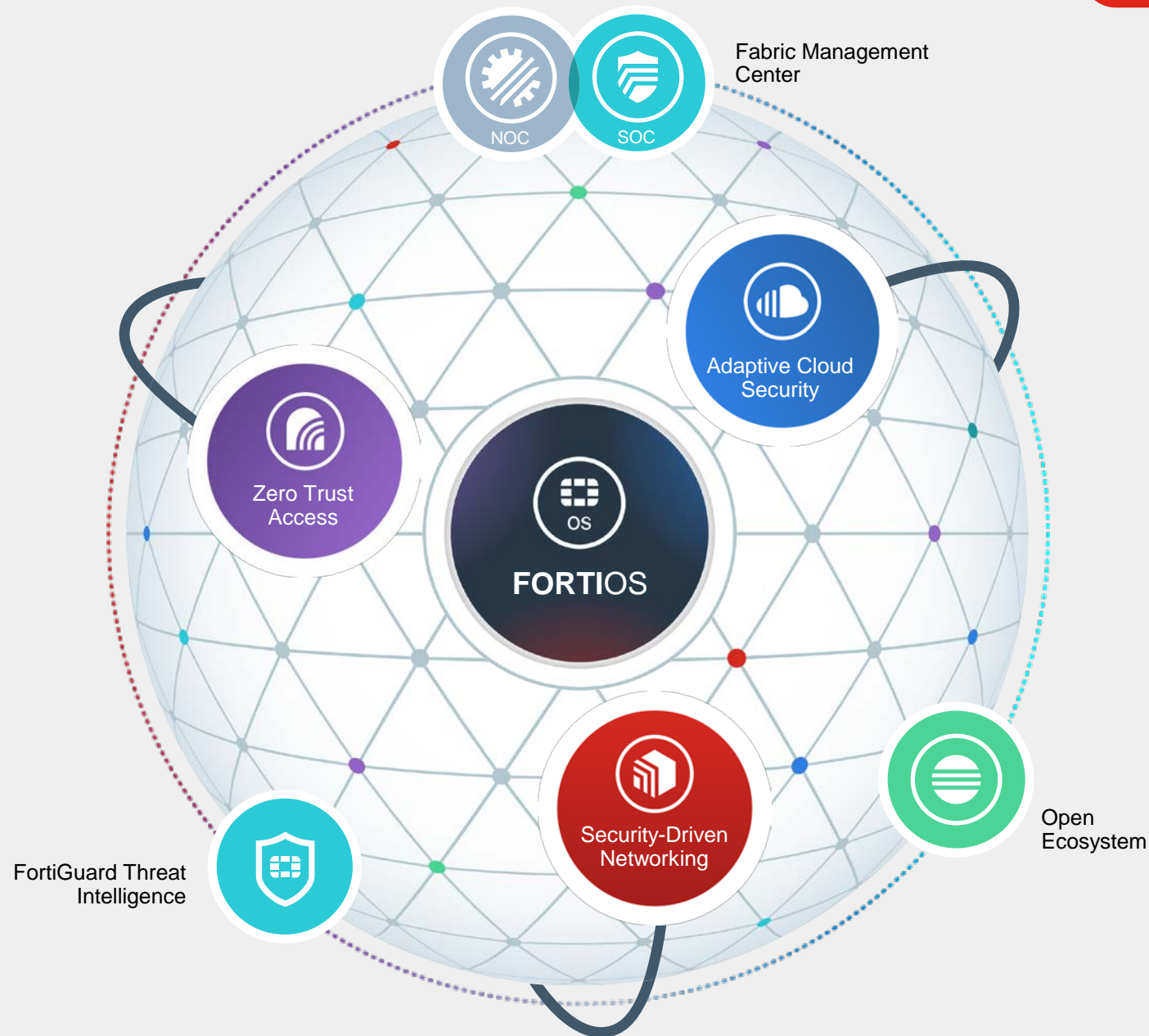
visibility and protection of the entire digital attack surface to better manage risk

Integrated

solution that reduces management complexity and shares threat intelligence

Automated

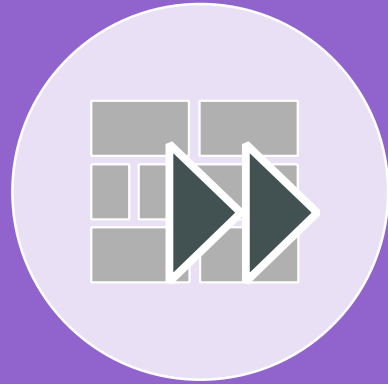
self-healing networks with AI-driven security for fast and efficient operations



FortiClient Integrated Threat Detections



**THREAT
INTELLIGENCE**



**NEXT GEN
FIREWALL**



**FILE
DETONATION/
SANDBOXING**



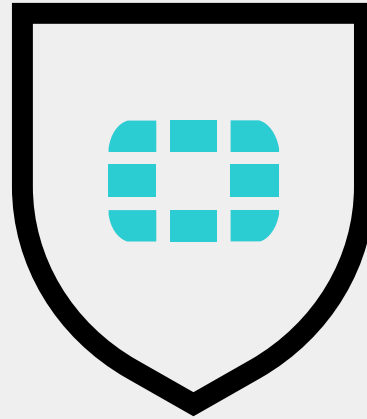
**FORTIGUARD
LABS**



**ANALYTICS &
UEBA**



FortiGuard



FortiGuard Labs Research

Fortinet's elite threat intelligence and research organization

Global Leadership & Collaboration

- Co-founded the Cyber Threat Alliance (CTA)
- Co-founded the World Economic Forum's Center for Cybersecurity

Threat Research with Actionable Insights

- Zero Day Research
- Adversary Playbooks

ML/AI Development and Training

- Leveraging AI/ML to provide timely and consistently top-rated protections

FortiGuard Security Services

Subscription Services providing automated updates to the Security Fabric



Content Security



Web Security



User Security



Device Security



SOC/NOC Tools

FortiGuard Labs Consulting

Before the Attack

- Penetration Testing
- Focused Threat Analysis
- Anti-Phishing Service
- Security Architecture Evaluation

During the Attack

Real-time security protection updates

After the Attack

Incident Response

Security Mastery

Cybersecurity workshops



FortiGuard Security Services by Numbers

462K

Malicious Website Accesses
Blocked Per minute

15M

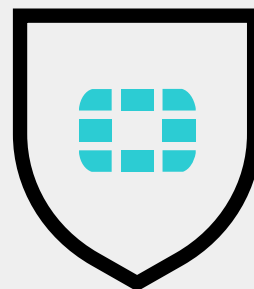
Botnet C&C Attempts Thwarted
Per minute

906

Zero Day
Threats Discovered

136K

Phishing Blocked
Per Minute



904K

Malware Programs Neutralized
Per Minute

609K

Threat Research Globally
Per Week

1.2 PB

Of Threat Samples

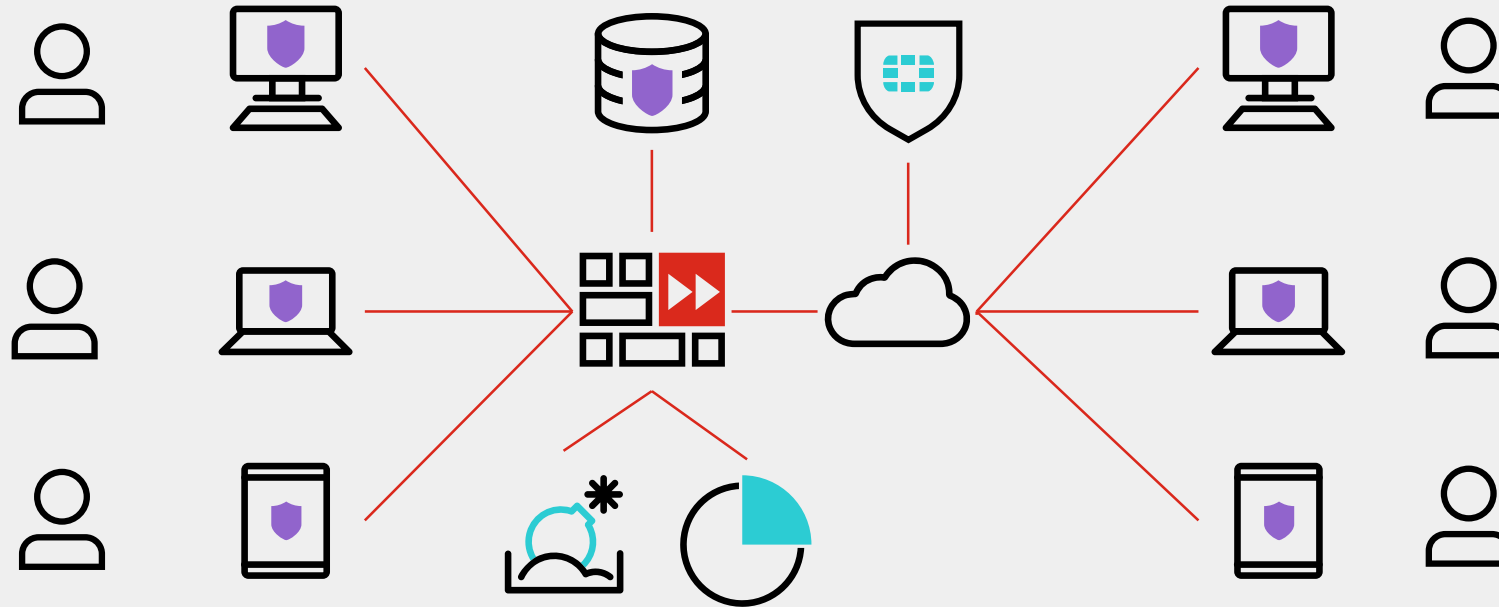
Near Zero

False positives
per month



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)
Secure Access Services Edge (SASE)
Single Sign On (SSO)
VPN (IPSec & SSL)

Endpoint Protection

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



FortiClient Components

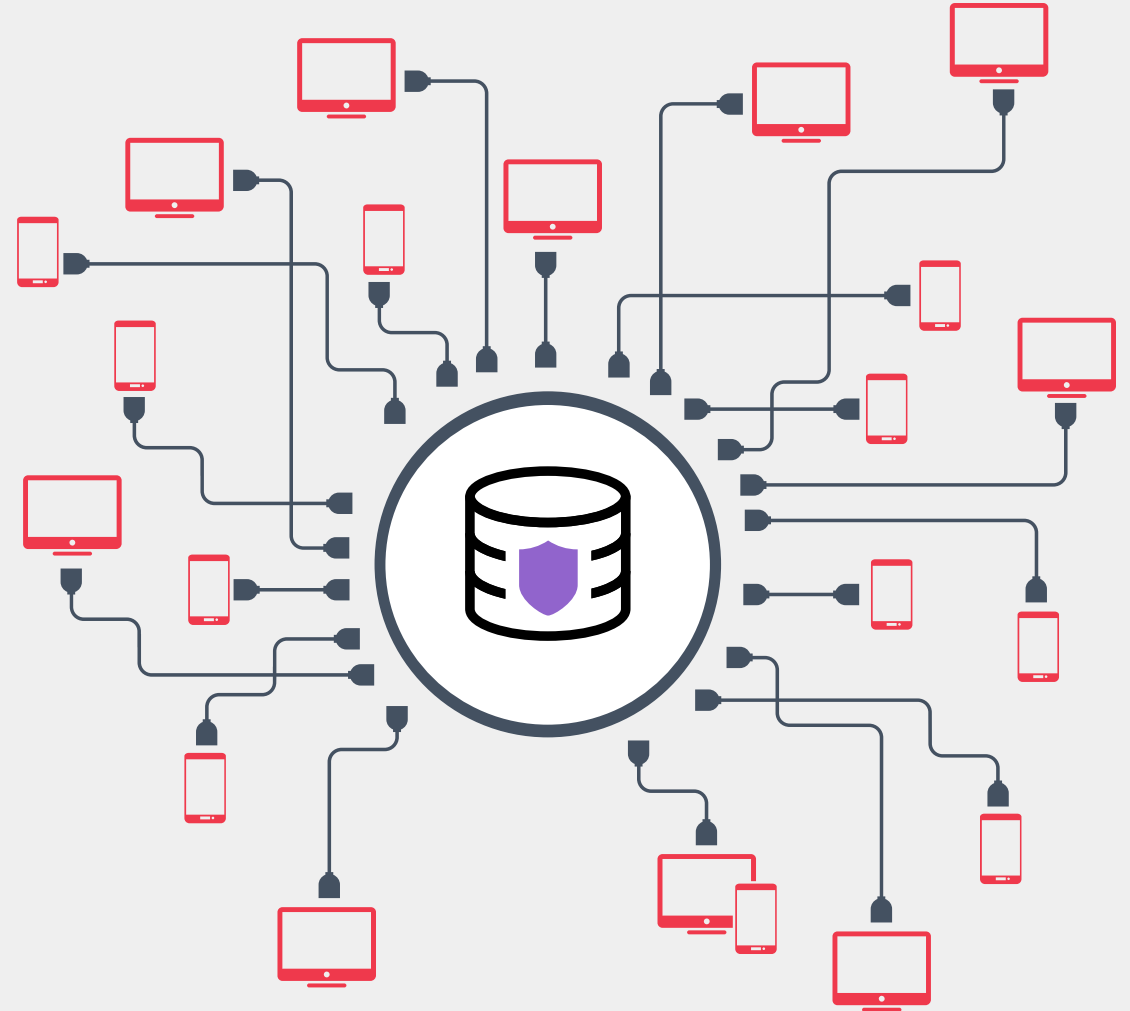


	VPN/ZTNA	EPP/APT
IT Hygiene/Fabric Agent		
Telemetry, Central Logging & Reporting	✓	✓
FortiGuard Web Filtering	✓	✓
Vulnerability & Remediation	✓	✓
USB Device Control	✓	✓
Secure Remote Access		
ZTNA Agent	✓	✓
SSL VPN	✓	✓
IPSec VPN	✓	✓
Protection		
FortiSandbox Integration (on-prem & cloud)	✓	✓
FortiClient Cloud Sandbox		✓
FortiGuard AI-powered NGAV		✓
Automated Quarantine		✓
Ransomware Protection		✓

Centralized Management

Enterprise Management System (EMS) or FortiClient Cloud

- Configure, deploy and manage FortiClient
 - Integrate with LDAP and other enterprise systems
- Real-time endpoint monitoring
- Threat summary, alert and notification
- Remote actions
 - Anti-malware scanning
 - Vulnerability scanning
 - Endpoint quarantine
- Software Inventory
- File quarantine management
- Highly scalable



FortiClient Components

	VPN/ZTNA	EPP/APT
IT Hygiene/Fabric Agent		
Telemetry, Central Logging & Reporting	✓	✓
FortiGuard Web Filtering	✓	✓
Vulnerability & Remediation	✓	✓
USB Device Control	✓	✓
Secure Remote Access		
ZTNA Agent	✓	✓
SSL VPN	✓	✓
IPSec VPN	✓	✓
Protection		
FortiSandbox Integration (on-prem & cloud)	✓	✓
FortiClient Cloud Sandbox		✓
FortiGuard AI-powered NGAV		✓
Automated Quarantine		✓
Ransomware Protection		✓

Fabric Agent Use Case

- Risk-based visibility
 - Identify unpatched vulnerabilities with patching options
 - Software inventory for visibility on installed application and versions
- Integrated and automated
 - Integrated with the Security Fabric
 - Automated response to contain incidents
- Compatibility with 3rd party vendors



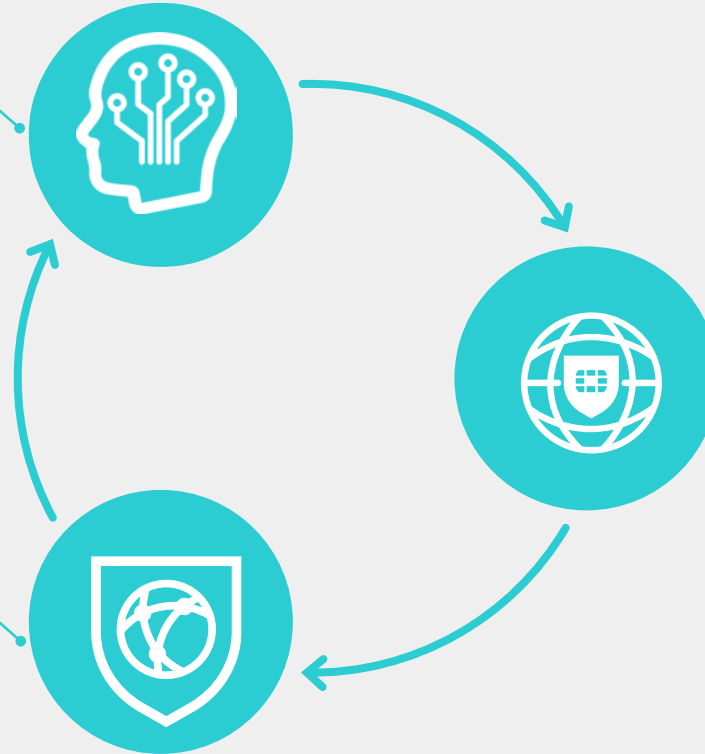
FortiGuard Web Filtering

AI-Analysis at Scale

- Supervised & unsupervised learning models
- Trained on large & diverse dataset from FortiGuard Labs

Defense in Depth

- Full spectrum of web protection against unknown & known threats
- Multiple layers of defense with near-zero false-negatives



Consistent Web Posture

- Across network, endpoints, and cloud
- Flexible Proxy Deployment (Explicit, Transparent, inline)



Critical Vulnerabilities Patch AllFilter

Vulnerability Name	FortiGuard ID	CVE ID	Category	Affected Endpoints	Patch Type
Cumulative Security Update for Internet Explorer	1492	CVE-2016-0178	OS	3	Patch
Firefox SVG Animation Remote Code Execution	31801	CVE-2016-9079	Browser	3	Patch
Sandbox restrictions not applied to nested frame elements	26051	CVE-2016-3223	AntiVirus	2	Patch
Security update available for Adobe Reader APSB17-01	38632	CVE-2017-2939	OS	2	Scheduled
Security Update for Group Policy					Scheduled
Security Update for Microsoft Graphics Component					Scheduled
Security Update for Microsoft RPC					Scheduled
Security Update for Microsoft Windows to Address Remote Code Execution					Scheduled
Security Update for Microsoft XML Core Services					Scheduled
Security Update for Netlogon					Scheduled
Security Update for Windows Print Spooler Components					Scheduled
Security Update for Windows Shell					Scheduled
Security Updates Available for Adobe Acrobat and Reader APSB16-09					Scheduled
Security Update for Adobe Flash Player					Scheduled
Security Vulnerability CVE-2016-5183 for Google Chrome					Scheduled
Security Vulnerability CVE-2016-5182 for Google Chrome					Scheduled
UI selection timeout missing on download prompts	26255	CVE-2016-0146	AntiVirus	1	Scheduled
Use after free mutating DOM during SetBody	22566	CVE-2016-0139	AntiVirus	1	Scheduled
WebGL content injection from one domain to rendering in another	27578	CVE-2016-0274	AntiVirus	1	Scheduled

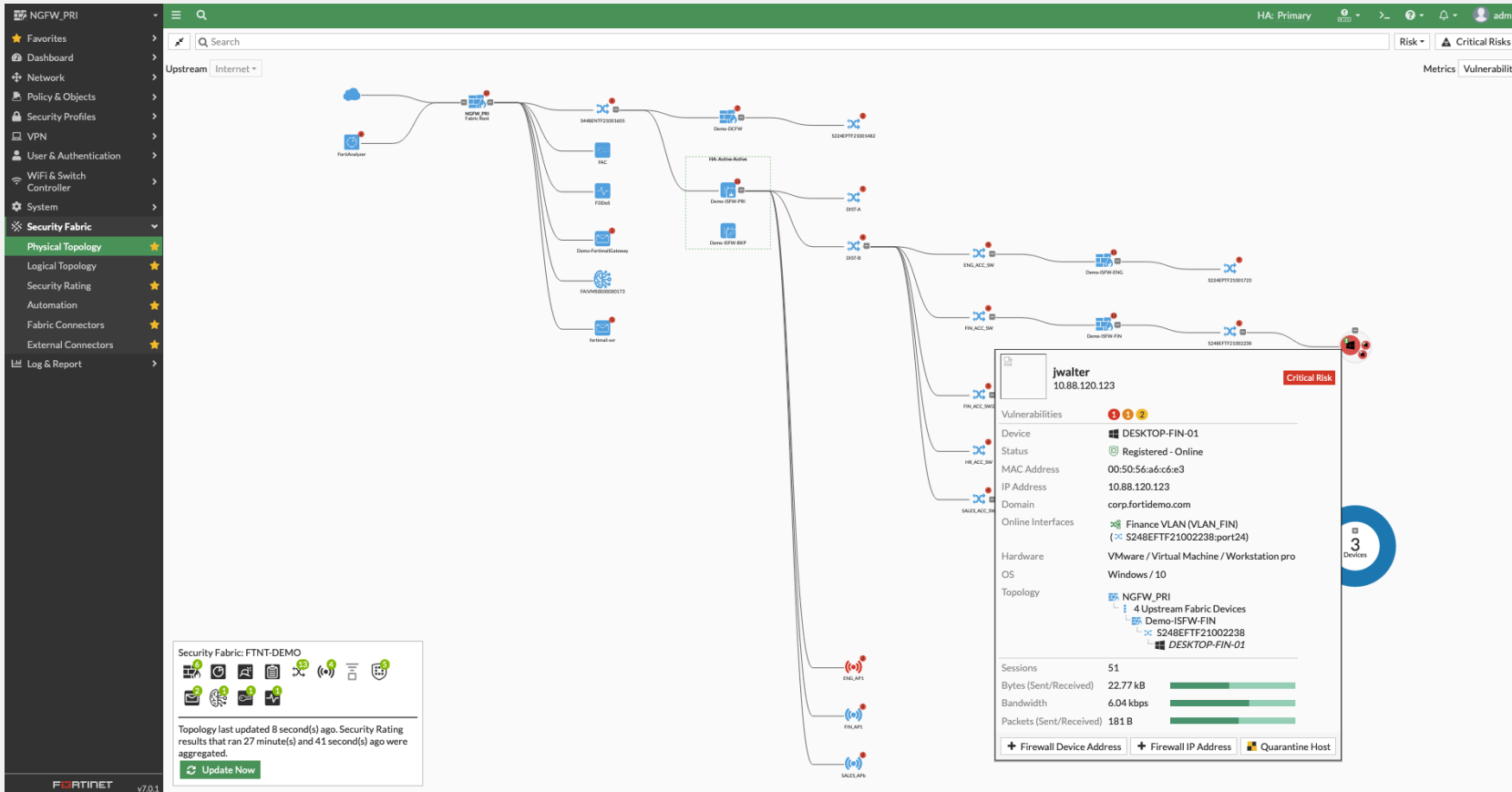
Affected Endpoints

Hostname	User	Last Seen	Scan Time
AHarris-PC	Andrew	2017-02-05 12:32:21	2017-02-05 12:32:21
km-ftnt-PC	admin	2017-02-04 18:25:45	2017-02-04 18:25:45
TiaraQuan-PC	Administrator	2017-02-04 09:15:22	2017-02-04 09:15:22

OK

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



Security Rating

NGFW_PRI
HA: Primary
admin

- ★ Favorites
- Physical Topology
- Logical Topology
- Fabric Connectors
- External Connectors
- Automation
- Security Rating
- FortiLink Interface
- Dashboard
- Network
- Policy & Objects
- Security Profiles
- VPN
- User & Authentication
- WiFi & Switch Controller
- System
- Security Fabric
- Log & Report

Security Posture Identify configuration weaknesses and best practice violations in your deployment.

Security Control Results

Report Details

Score: -297.03

Last Ran: 32 minute(s) and 36 second(s) ago

Endpoints: 165

Trends

High: -82.94

Low: -367.42

Change: -171.24%

Grades

- D Fabric Security Hardening
- A Audit Logging & Monitoring
- A Threat & Vulnerability Management
- A Network Design & Policies
- A Endpoint Management
- A Firmware & Subscriptions

Search

FSBP PCI Export All

Security Control	Device	Score	Result	Compliance	
Unlicensed 112					
Passed 51					
Failed 132					
<p>Default Port HTTPS</p> <p>HTTPS should not use the default port.</p>	8 Devices	-180	Failed	FSBP SH01.8	
<p>Endpoint Registration</p> <p>Interfaces which are classified as "LAN" and are used by a policy should have Security Fabric Connection enabled.</p>	6 Devices EZ	-120	Failed	FSBP EM01.1	
<p>Default Port SSH</p> <p>SSH should not use the default port.</p>	6 Devices	-120	Failed	FSBP SH01.10	
<p>Administrative Access</p> <p>Interfaces which are classified as "WAN" should have administrative access disabled.</p>	6 Devices EZ	-120	Failed	FSBP SH01.9	
<p>USB Auto Configuration</p> <p>Automatic USB firmware and configuration provisioning features should be disabled during normal operation.</p>	6 Devices EZ	-120	Failed	FSBP SH15.1	
<p>Valid HTTPS Certificate - Administrative GUI</p> <p>The administrative GUI should be using a valid and secure certificate.</p>	6 Devices	-120	Failed	FSBP SH03.1	
<p>FortiClient Vulnerabilities</p> <p>All registered FortiClient devices should have no critical vulnerabilities.</p>	6 Devices	-50	Unmet Dependencies	FSBP EM01.2	
<p>Unsecure Protocol - Telnet</p> <p>Interfaces which are classified as "WAN" and are used by a policy should not allow Telnet administrative access.</p>	9 Devices	-90	Failed	FSBP SH01.1	

0% 316

FortiClient Vulnerabilities

All registered FortiClient devices should have no critical vulnerabilities.

Category

Endpoint Management (EM)

Recommendations

- NGFW_PRI -50
- This Security Control could not run as the device or its parent did not meet the following dependencies:
- Endpoint Registration
- 0
- 0
- Demo-ISFW-SALES 0
- 0
- 0

Total Score: -50

Compliance Information

- FSBP EM01.2
- PCI 1.4
- PCI 5.1
- PCI 5.1.1
- PCI 6.2

Automation

NGFW_PRI HA: Primary admin

Stitch Trigger Action

+ Create New View Delete Clone Search

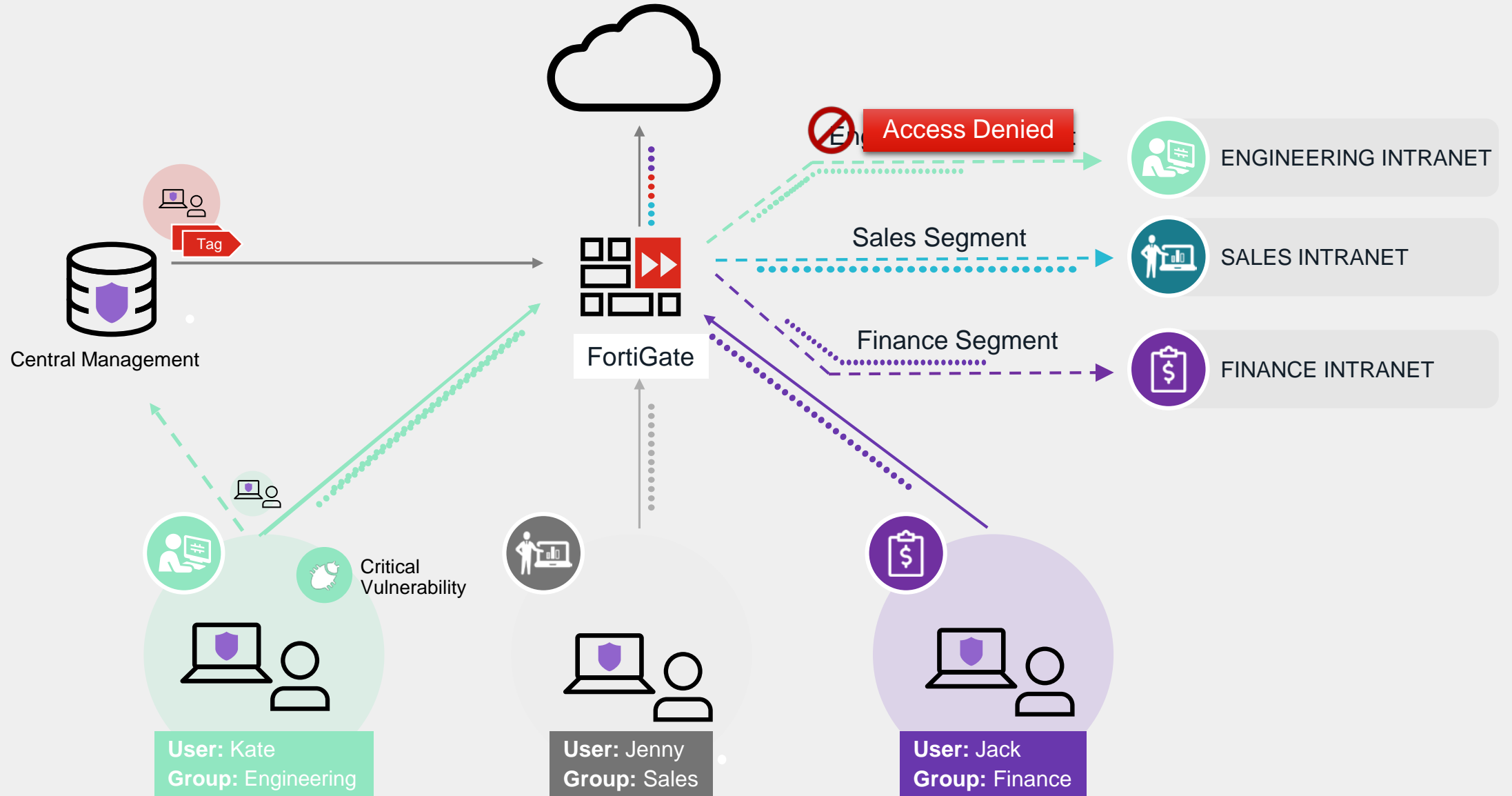
Name	Status	Trigger	Actions	FortiGate(s)	Trigger Count	Last Triggered
Compromised Host 3						
AutoQ	Disabled	AutoQ	AutoQ_quarantine AutoQ_quarantine-forticlient AutoQ_ban-ip	All FortiGates	0	
Compromised Host Quarantine	Disabled	Compromised Host Quarantine	Compromised Host Quarantine_quarantine Compromised Host Quarantine_quarantine-forticlient	All FortiGates	0	
FortiClient	Enabled	FortiClient	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	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

Fortinet v7.0.1 11 Updated: 17:04:11



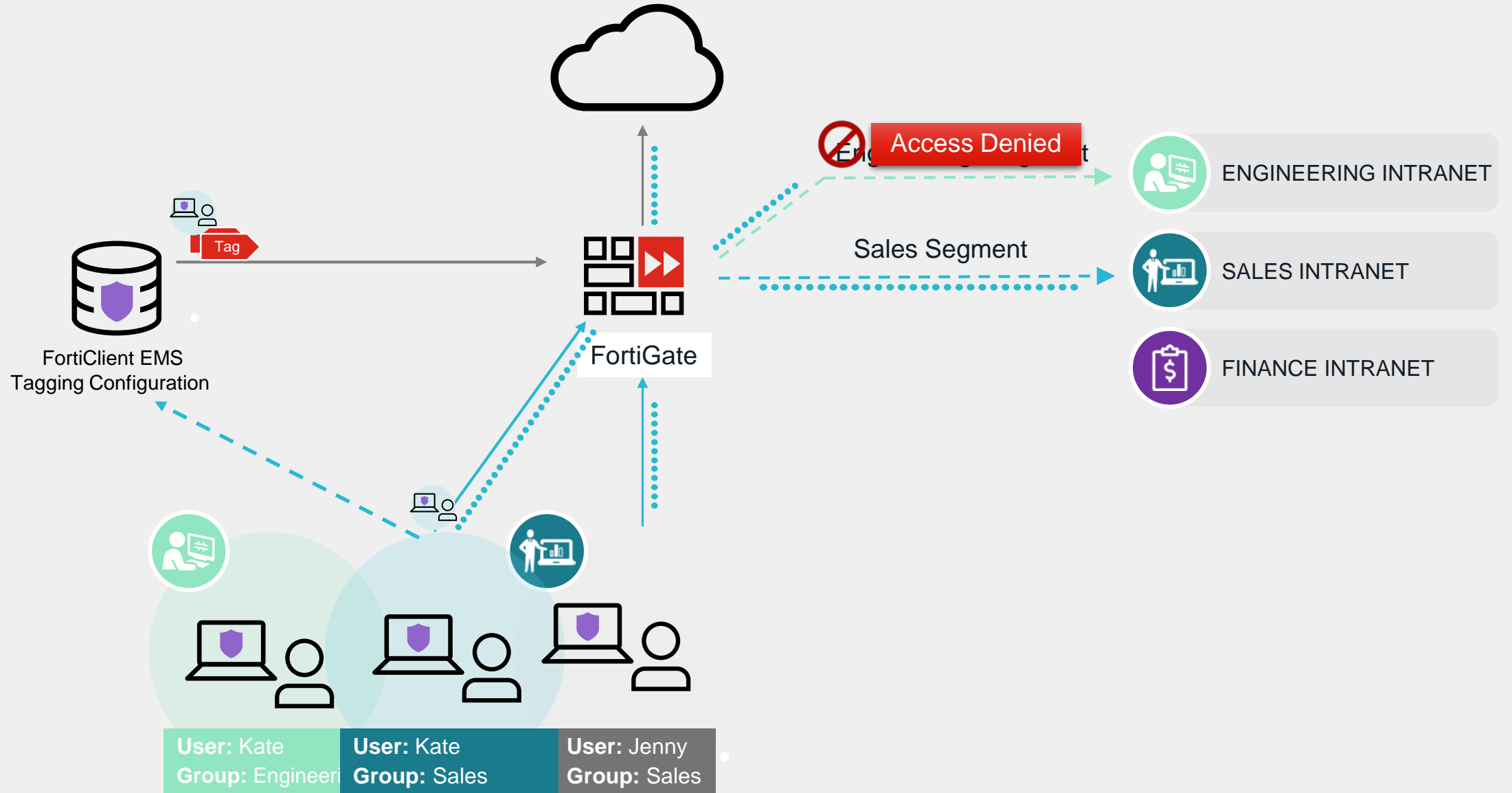
Zero-Trust Access Control

Use Case: Block Access for Security Risk Endpoints



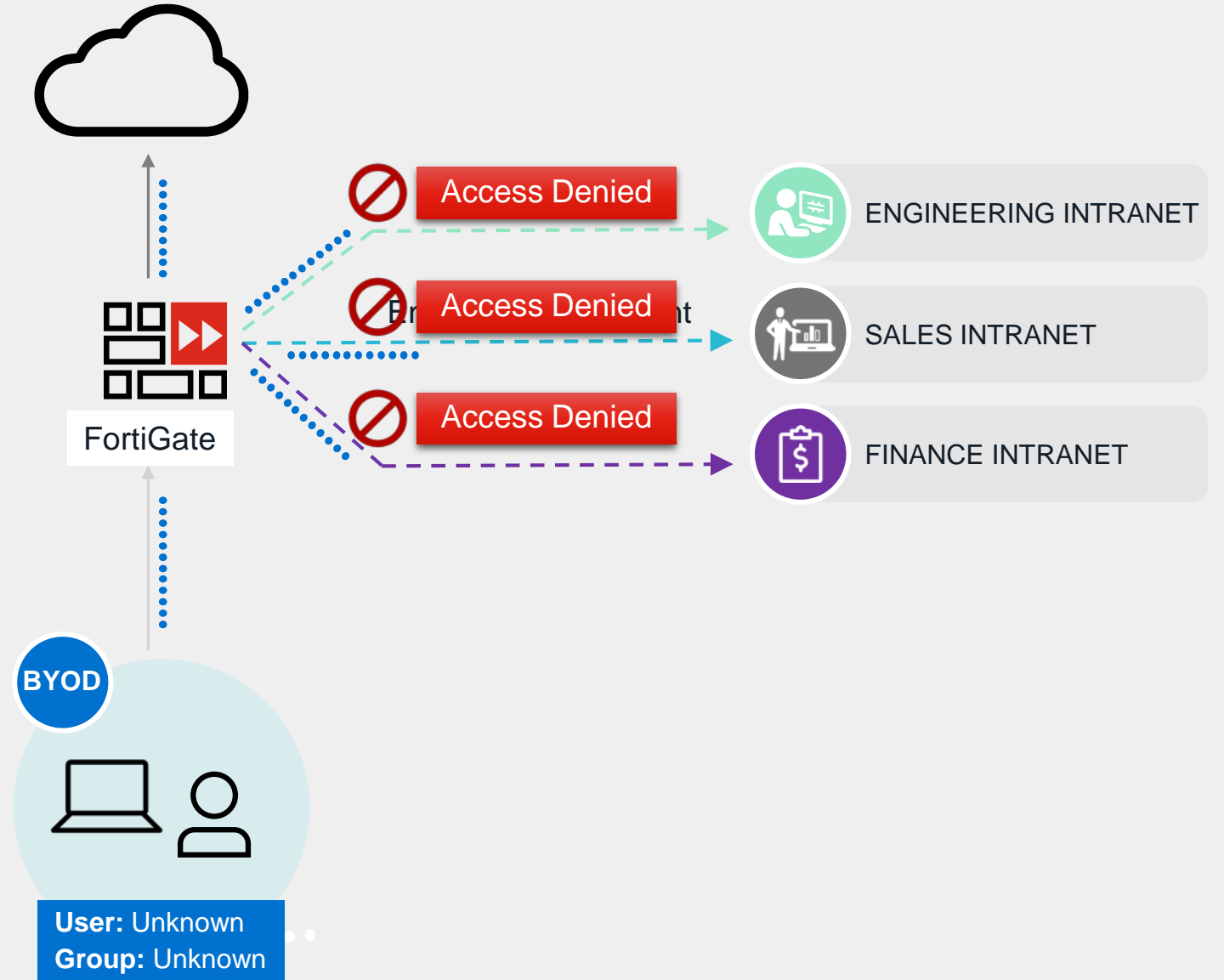
Zero-Trust Access Control

Use Case: Access Based on AD Groups



Zero-Trust Access Control

Use Case: Restricted Access for Unknown Endpoints

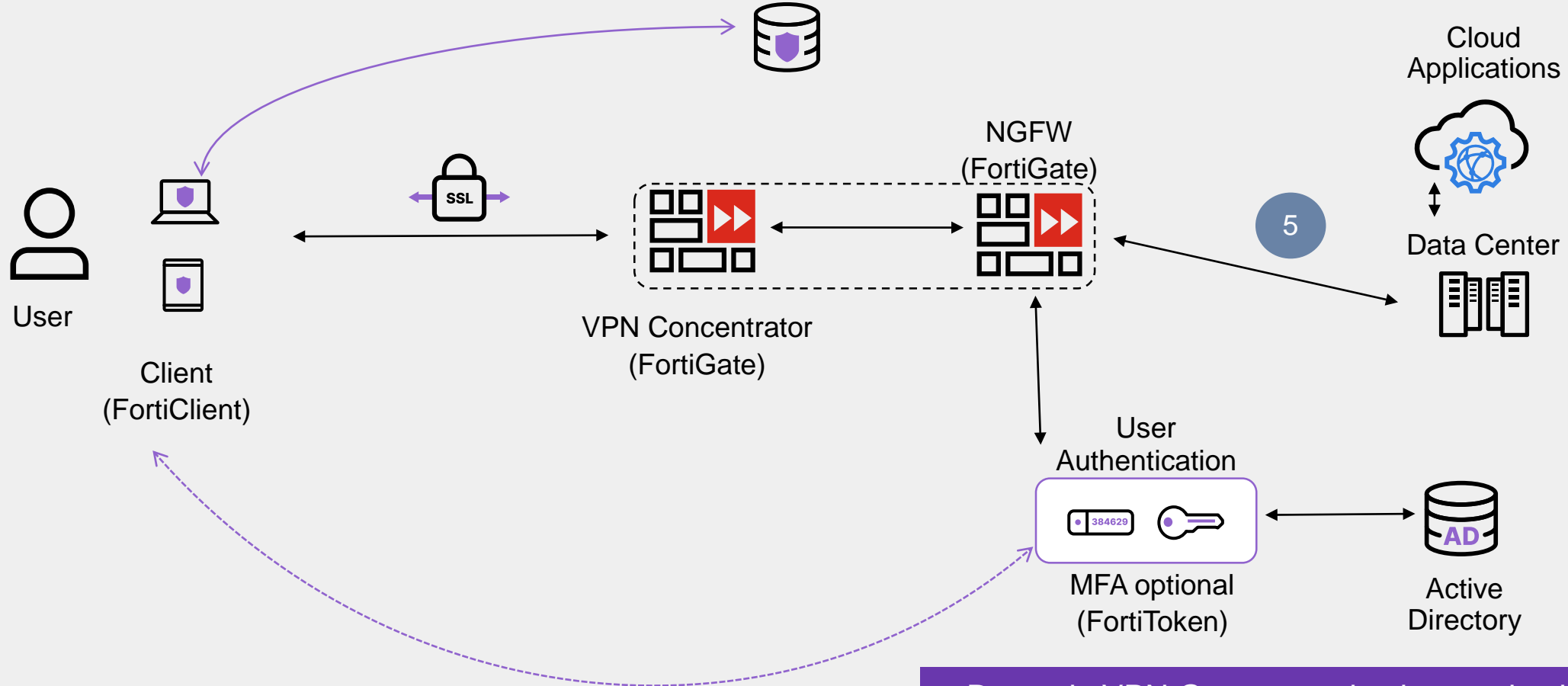


FortiClient Components

	VPN/ZTNA	EPP/APT
IT Hygiene/Fabric Agent		
Telemetry, Central Logging & Reporting	✓	✓
FortiGuard Web Filtering	✓	✓
Vulnerability & Remediation	✓	✓
USB Device Control	✓	✓
Secure Remote Access		
ZTNA Agent	✓	✓
SSL VPN	✓	✓
IPSec VPN	✓	✓
Protection		
FortiSandbox Integration (on-prem & cloud)	✓	✓
FortiClient Cloud Sandbox		✓
FortiGuard AI-powered NGAV		✓
Automated Quarantine		✓
Ransomware Protection		✓

Virtual Private Networking (VPN) Technology

Access to the Network



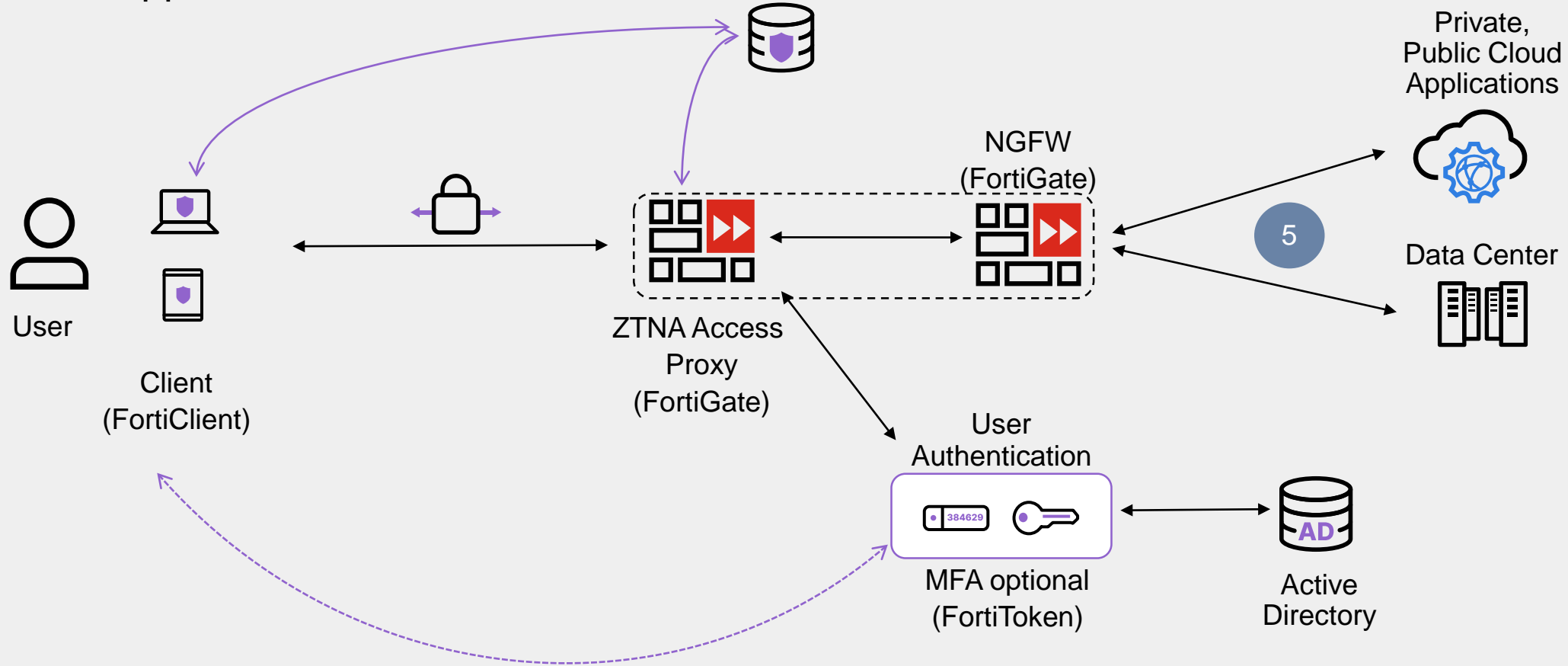
- Dynamic VPN Gateway selection, and split tunneling
- Additional layers of security with MFA
- Single-Sign-on agent supports FortiAuthenticator



Zero Trust Network Access (ZTNA) Technology



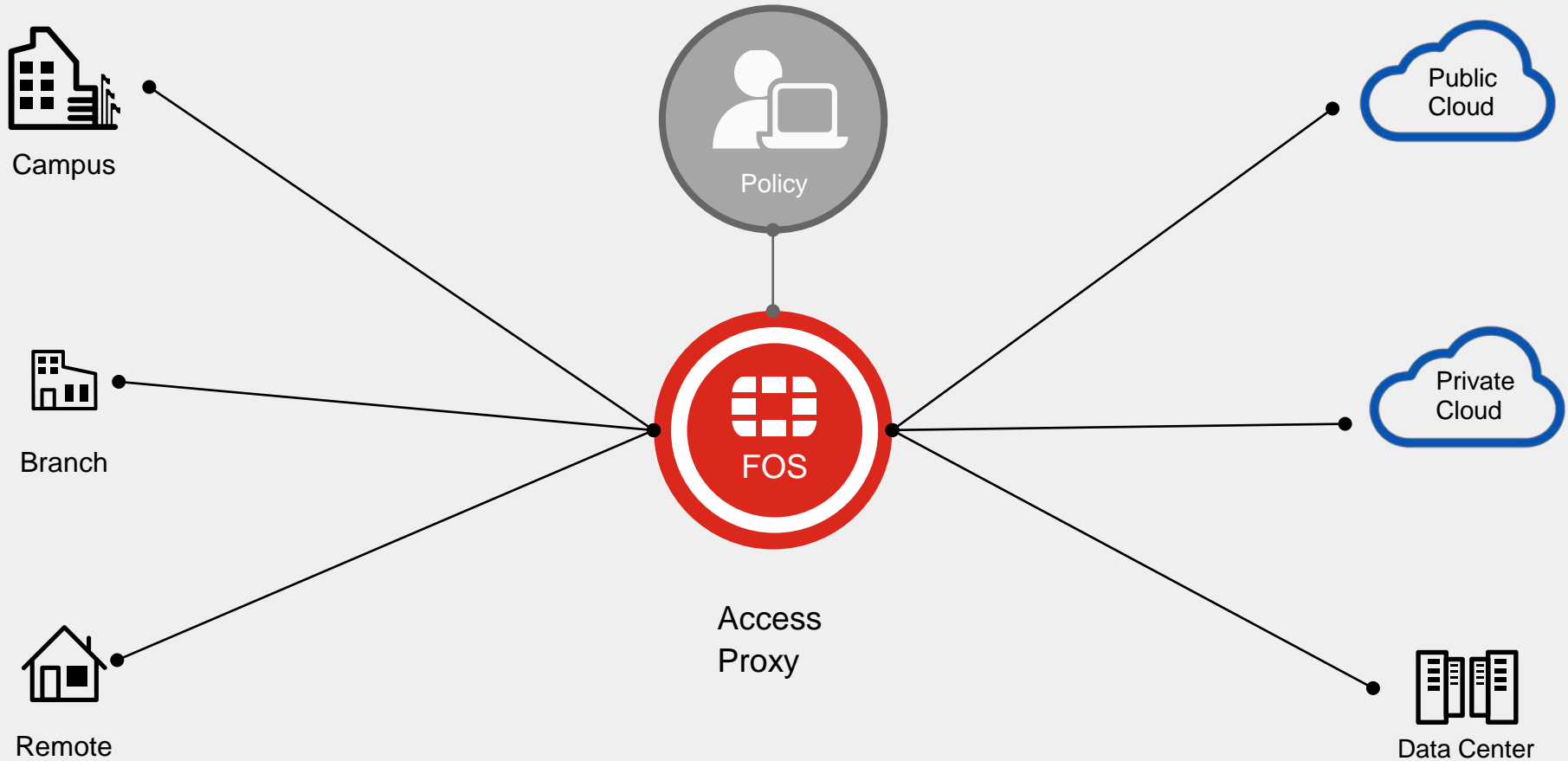
Granular Application Access



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



ZTNA Flexible Architecture



Wherever the user is

Verified user identity, device identity & posture check prior to access

Wherever the application is



Fortinet's ZTNA

What's it made of? Existing Fortinet Security Fabric Products

Core Elements



FortiGate



- FortiGate builds the secure tunnel, maintains user group/application access table (FOS 7.0)
- FortiClient Central Management configures the ZTNA agent in FortiClient for the secure connection back to the FortiGate (FortiClient 7.0)
 - FortiClient Central Management: Either FortiClient EMS or FortiClient Cloud
- Authentication Solution
 - FortiAuthenticator, FortiToken or any 3rd party supported by the Security Fabric



Fortinet ZTNA advantages

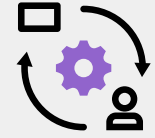
Complete coverage vs. other ZTNA solutions

- Leveraging existing investments in on-prem Firewalls
 - Most ZTNA solutions are SASE-only options with expensive charges for company-wide coverage
 - Leverage SD-WAN, SD-Branch capabilities
- Improved Security (“Secure ZTNA”)
 - Extend FortiGate protection to wherever you are
 - Traffic traversing Industry-leading FortiGate technology
- No Licenses Required
 - Simply a feature in FOS & FortiClient to turn on!



Evolution of VPN tunnels

Bringing Zero Trust principles to remote access



- Ongoing verification
 - Per session user identity checks
 - Per session device posture checks (OS version, A/V status, vulnerability assessment)
- More granular control
 - Access granted only to specific application
 - No more broad VPN access to the network
- Easier user experience
 - Auto-initiates secure tunnel when user accesses applications
 - Same experience on and off-net



FortiClient Components

	VPN/ZTNA	EPP/APT
IT Hygiene/Fabric Agent		
Telemetry, Central Logging & Reporting	✓	✓
FortiGuard Web Filtering	✓	✓
Vulnerability & Remediation	✓	✓
USB Device Control	✓	✓
Secure Remote Access		
ZTNA Agent	✓	✓
SSL VPN	✓	✓
IPSec VPN	✓	✓
Protection		
FortiSandbox Integration (on-prem & cloud)	✓	✓
FortiClient Cloud Sandbox		✓
FortiGuard AI-powered NGAV		✓
Automated Quarantine		✓
Ransomware Protection		✓

Detect and Block Malware and Advanced Threats



Sandbox Integration

- Detect advanced or custom malware
- Automatic file submission for analysis
- Threat intelligence sharing across enterprise



Anti-Malware

- Pattern-based (CPRL) antimalware engine
- Detect polymorphic malware
- Block known attack channels and malicious website
- Big data analysis, machine learning and AI in the Cloud



Anti-Exploits (exploit protection)

- Behavior-based detection
- Can detect Advanced malware and ransomware typically package an exploit
- Prevents attacks that leverage PowerShell or other scripts

Enhanced FortiSandbox Integration

The screenshot displays the FortiClient Enterprise Management Server interface. The main area shows a process tree starting with a red document icon labeled '6666xp.exe'. This process has spawned several child processes: 'AcroRd32.exe' (highlighted with a green gear icon), 'svchost.exe', and 'sdclt.exe' (with a red '2' badge). 'AcroRd32.exe' further spawned 'services.exe', 'svchost.exe', 'msiexec.exe', and 'taskhost.exe'. 'svchost.exe' spawned four instances of 'mscorsvw.exe' (with a red '4' badge). The left sidebar contains navigation options like Dashboard, Endpoints, Domains, Workgroups, and Quarantine Management. The bottom pane shows details for the selected file.

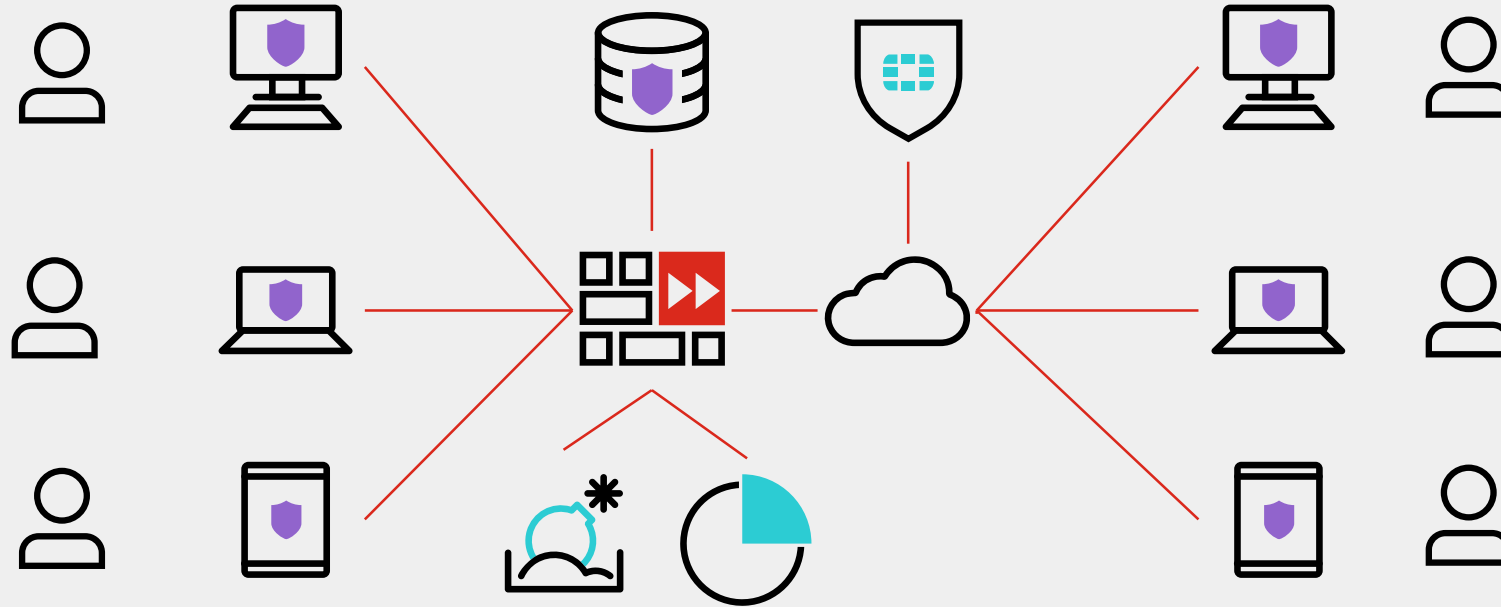
Details

Process Information	
PID	3844
File Path	%CURRENTPATH%\tloader.exe
File Type	pdf
CMD Line	c:\work\tloader.exe"c:\work\403530244237709471.pdf" 55000
MD5	494c08f7a144d3cc4cfa661ed1244039
Detail	Executable dropped dll/sys file(s) to system directory



Zero Trust Access—Device Visibility & Control

FortiClient for Fabric Agent, Remote Access, and Endpoint Protection



Fabric Agent & Hygiene Control

Vulnerability scanning
FortiGuard Web Filtering
Patching Policy
Dynamic grouping

Secure Remote Access

Zero Trust Network Access (ZTNA)
Secure Access Services Edge (SASE)
Single Sign On (SSO) & SAML support
VPN (IPSec & SSL)

Endpoint Protection

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



F**RTINET**®

Education



Protecting Students on the Internet



- Students must be protected from inappropriate content
- Internet browsing must be transparent—visible/logged/reported









Web Filtering

- 75+ URL categories
- More than 43 million rated websites, and 2 billion+ web pages
- Works with Google Safe Search
- Includes whitelisting and blacklisting of websites
- Monitor all web browser activity

The screenshot shows the FortiClient Enterprise Management Server interface. The left sidebar contains a navigation menu with categories like Dashboard, Endpoints, Google Domains, and Local Chromebook Profiles. The main content area is titled 'Web Filter' and is configured for the 'High School - District B' profile. It features several sections: 'General' with toggle switches for 'Log All URLs', 'Log User Initiated Traffic', 'Show Bubble Notification When HTTPS Site Is Blocked', and 'Enable Safe Search'; 'Site Categories' with a list of categories such as 'Adult/Mature Content', 'Abortion', 'Alcohol', etc., each with a red 'X' icon indicating it is blocked; and an 'Exclusion List' at the bottom with a text input field and a list of excluded URLs including 'https://yandex.com', '*yandex.*', and '*openvpn.net'.



Web Filtering Across all Popular OSs

	 WINDOWS	 MAC OS X	 ANDROID	 iOS	 ChromeBook	 Linux
SECURITY FABRIC COMPONENTS						
Endpoint Telemetry ¹	✓	✓	✓	✓	✓	✓
Compliance Enforcement ¹	✓	✓	✓	✓		✓
Endpoint Audit and Remediation with Vulnerability Scanning ¹	✓	✓				✓
Automated Endpoint Quarantine	✓	✓				
HOST SECURITY AND VPN COMPONENTS						
Antivirus	✓	✓				✓
Anti-Exploit	✓					
Sandbox Detection	✓					✓*
Web Filtering²	✓	✓	✓	✓	✓	
Application Firewall ¹	✓	✓				
IPSec VPN	✓	✓	✓	✓		
SSL VPN ³	✓	✓	✓	✓		✓



F**RTINET**®

Endpoint & Network Security Integration Check List

Visibility & Control	Threat Intelligence Sharing	Alert Resolution	Automation	Open Ecosystem
✓	Can you see all devices and identify them?			
✓	Can you monitor the device and associated risks? i.e. unpatched vulnerability? Outdated applications? Indicator of compromise?			
✓	Enforce control on a network level? Ensure security hygiene?			
✓	Threats intelligence aggregated to the vendor's "cloud" then push down?			
✓	Can threats intelligence discovered in one endpoint/location shared in real time instantaneous with the rest of the enterprise regardless of its location?			
✓	Alert resolution? Threat verification?			
✓	Can you set policy to automate response—contain threats automatically, quarantine compromised hosts?			
✓	How open is the integration?			



Endpoint Product Positioning

