FortiClient: Unified Endpoint Agent

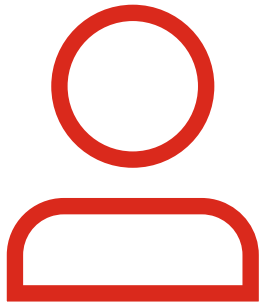
Endpoint Visibility, Secure Access, Endpoint Protection

A Unified Agent for the Fortinet Security Fabric

Jan 6, 2025

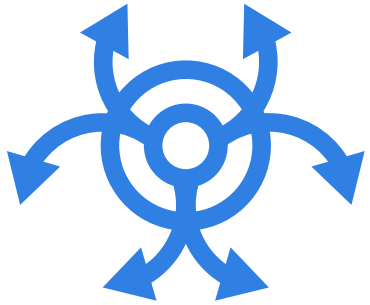
Customer Challenges

Hybrid Work



- Increased attack surface
- Endpoint posture

Advanced Threats



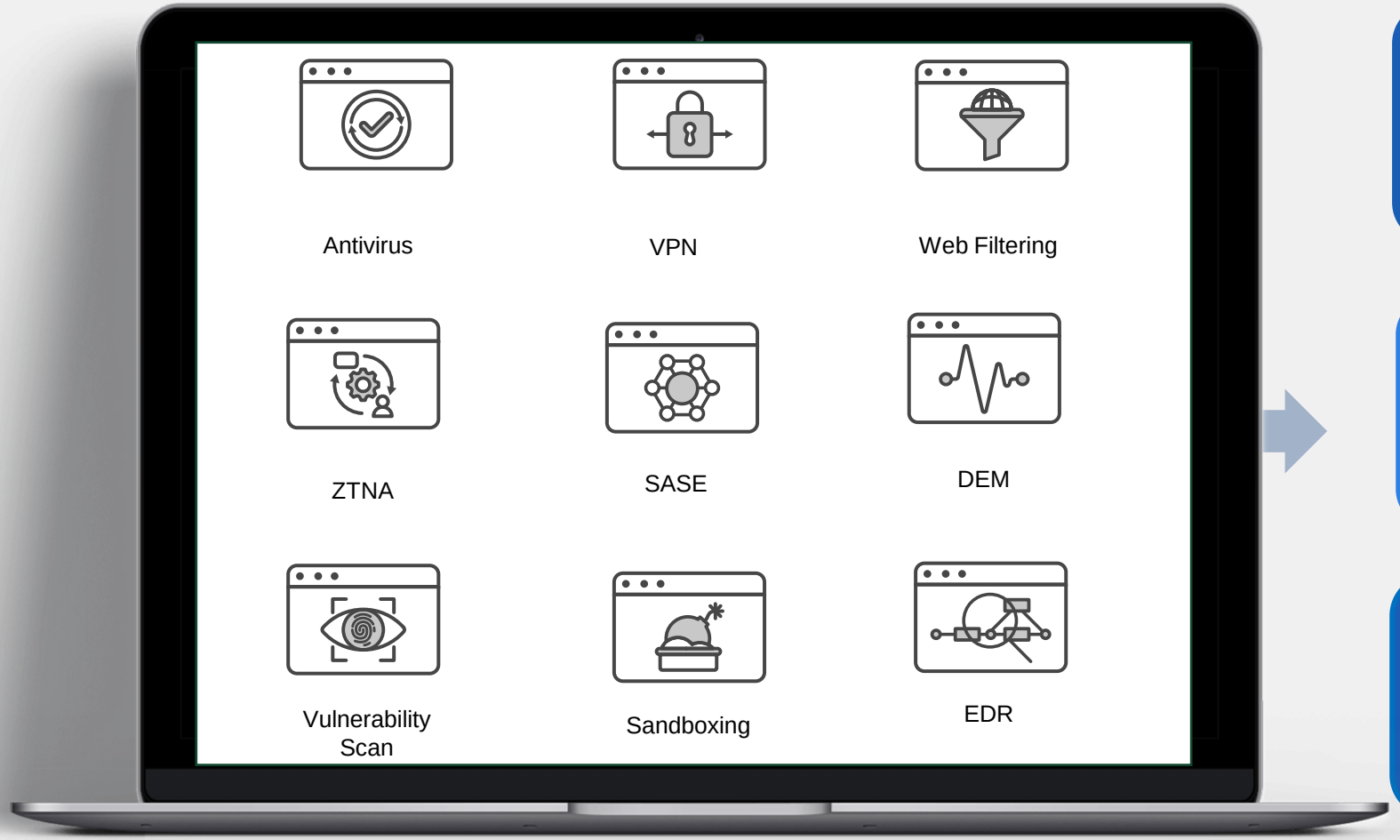
- Advanced threat actors
- Faster breakouts

Operational Complexity

- Disjointed products and siloed data
- Skills shortage

Problem with Endpoint Agent Sprawl

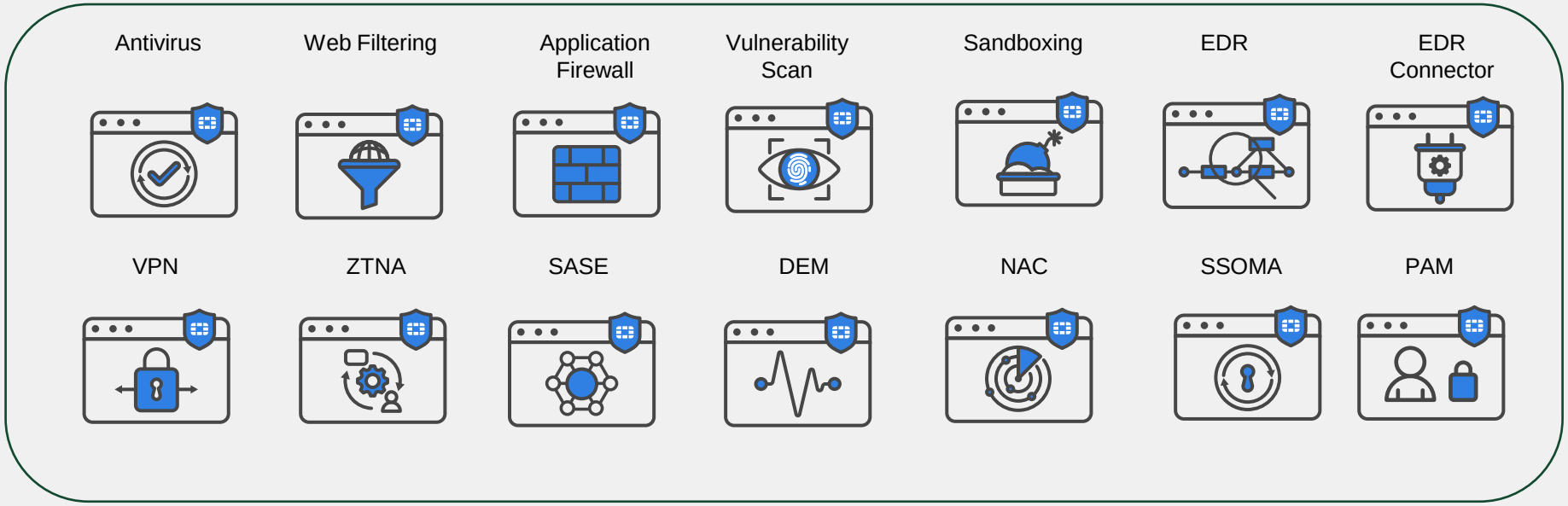
Drives Complexity, Cost and Gaps in Security



1. **Complex Operations**
2. **Lack of Integration and Security Gaps**
3. **Higher Cost**

15+ Years of Innovations – Unified Agent to Simplify Operations

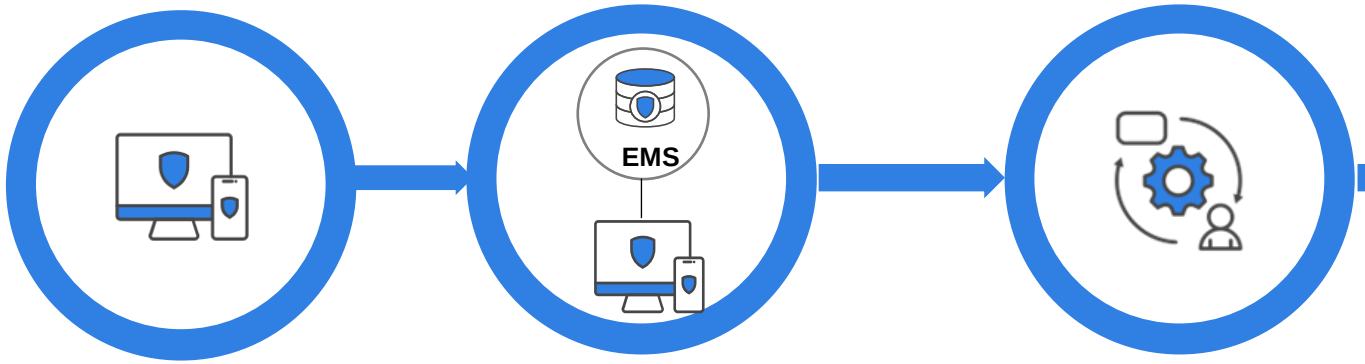
FortiClient



FortiClient Unified Agent Evolution

Continuous Innovation, Wide adoption with over 20M endpoints deployed

Evolution of Secure Access



FortiClient VPN

- Traditional VPN
- Free FortiClient

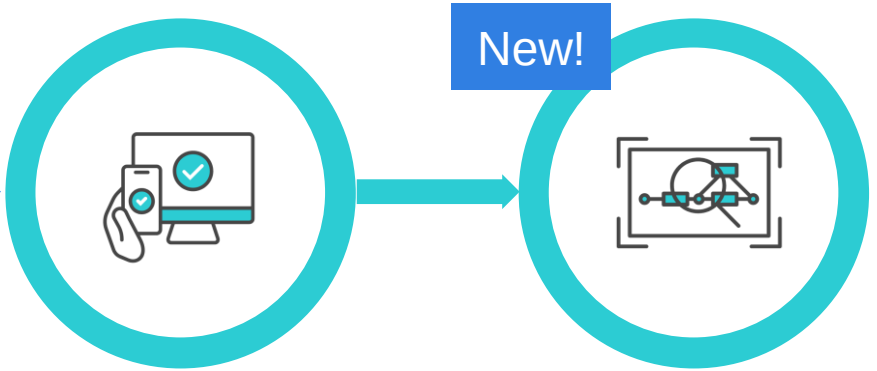
Endpoint Management (SaaS / On-prem)

- Centralized Endpoint Management
- Endpoint Telemetry and Visibility

Universal ZTNA (with IT Hygiene)

- Continuous Posture Validation
- Vulnerability Scanning and Patching Policy
- Web Filtering

Integrated Endpoint Security



Endpoint Protection (EPP)

- AI Powered Anti-Virus
- Application firewall
- Ransomware protection

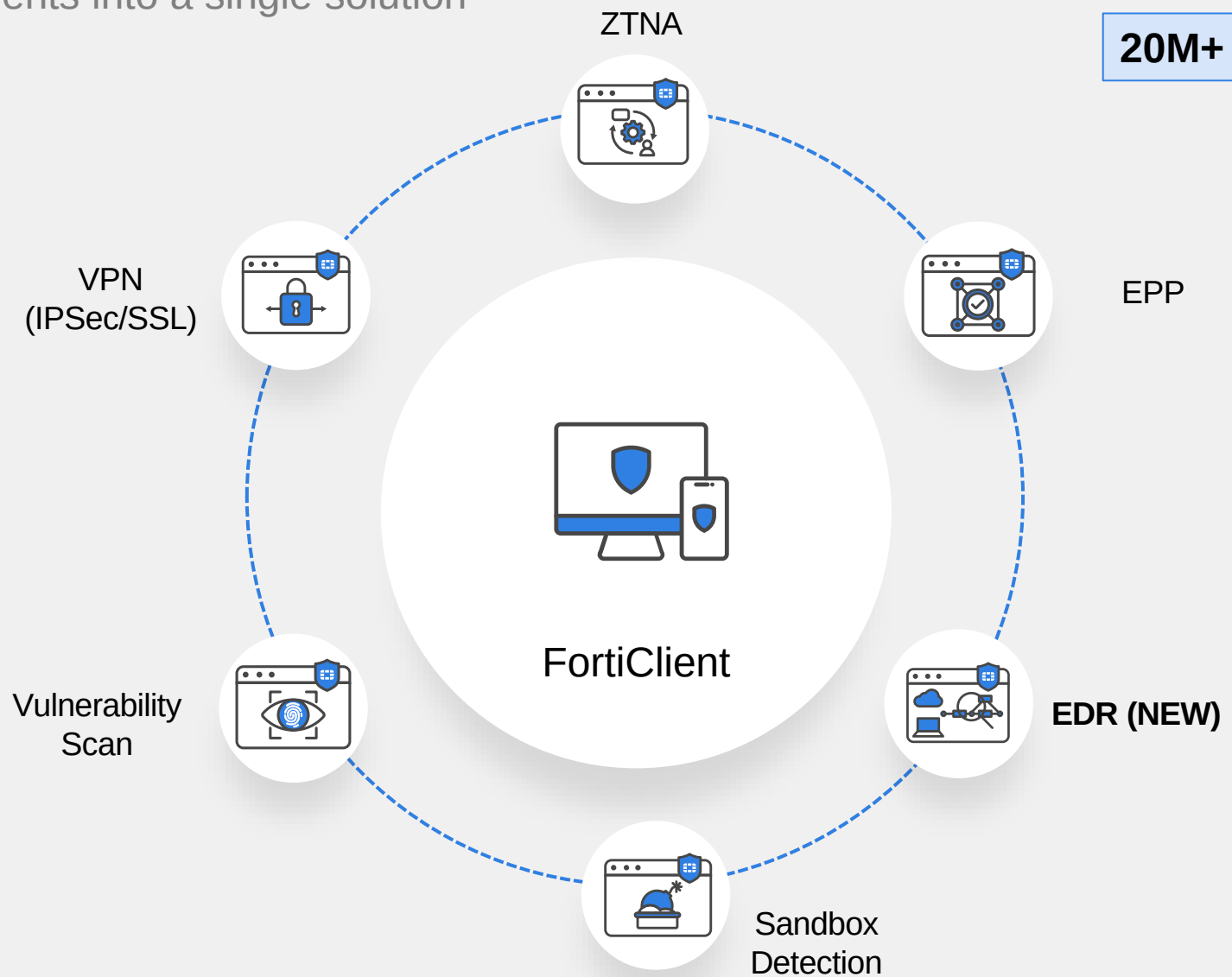
Endpoint Detection and Response (EDR)

- Behavior-based Protection
- Extended automated responses
- Threat hunting

FortiClient: The Industry's Only Unified Endpoint Agent

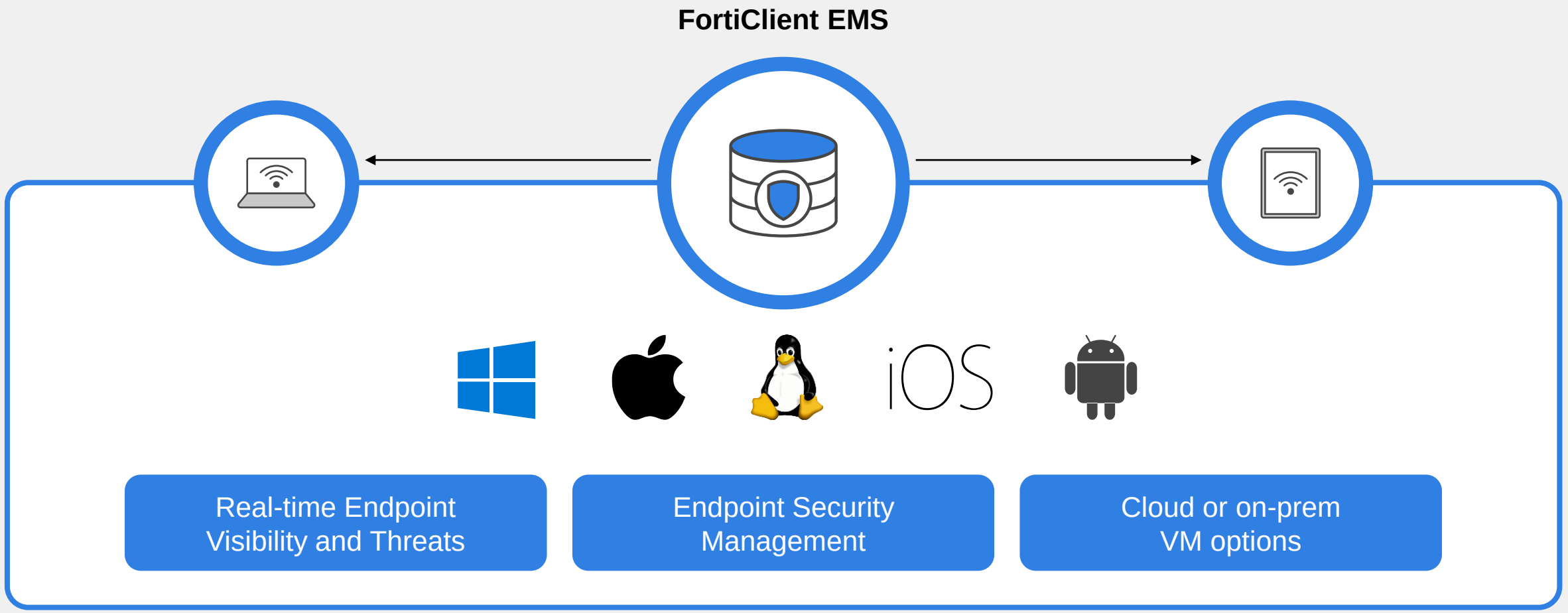
Condense multiple agents into a single solution

20M+ Endpoints Deployed



Centralized Endpoint Management

FortiClient Endpoint Management Server (EMS)



FortiClient Use Cases

Endpoint Hygiene

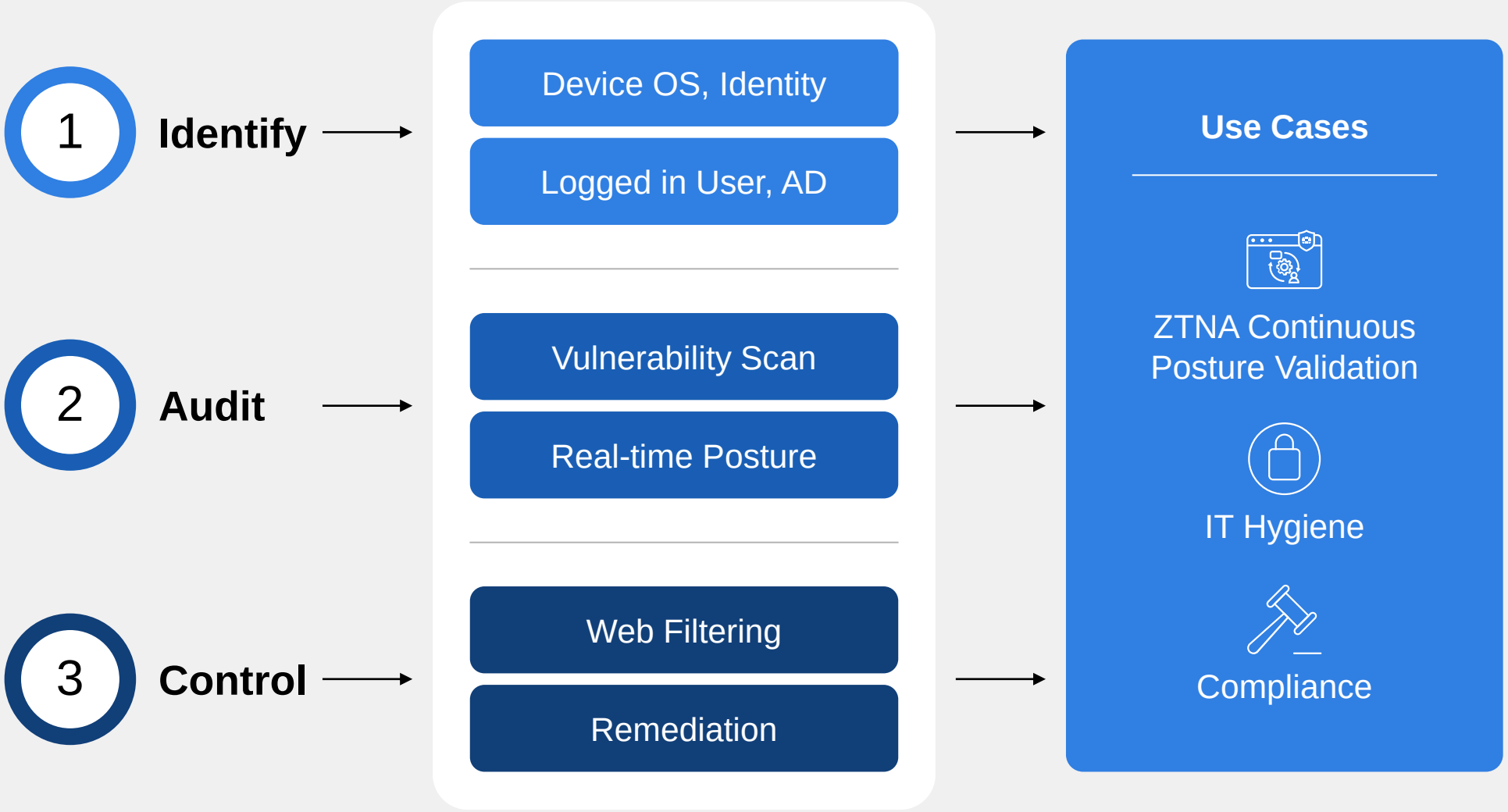
Secure Access

Endpoint Protection (EPP)

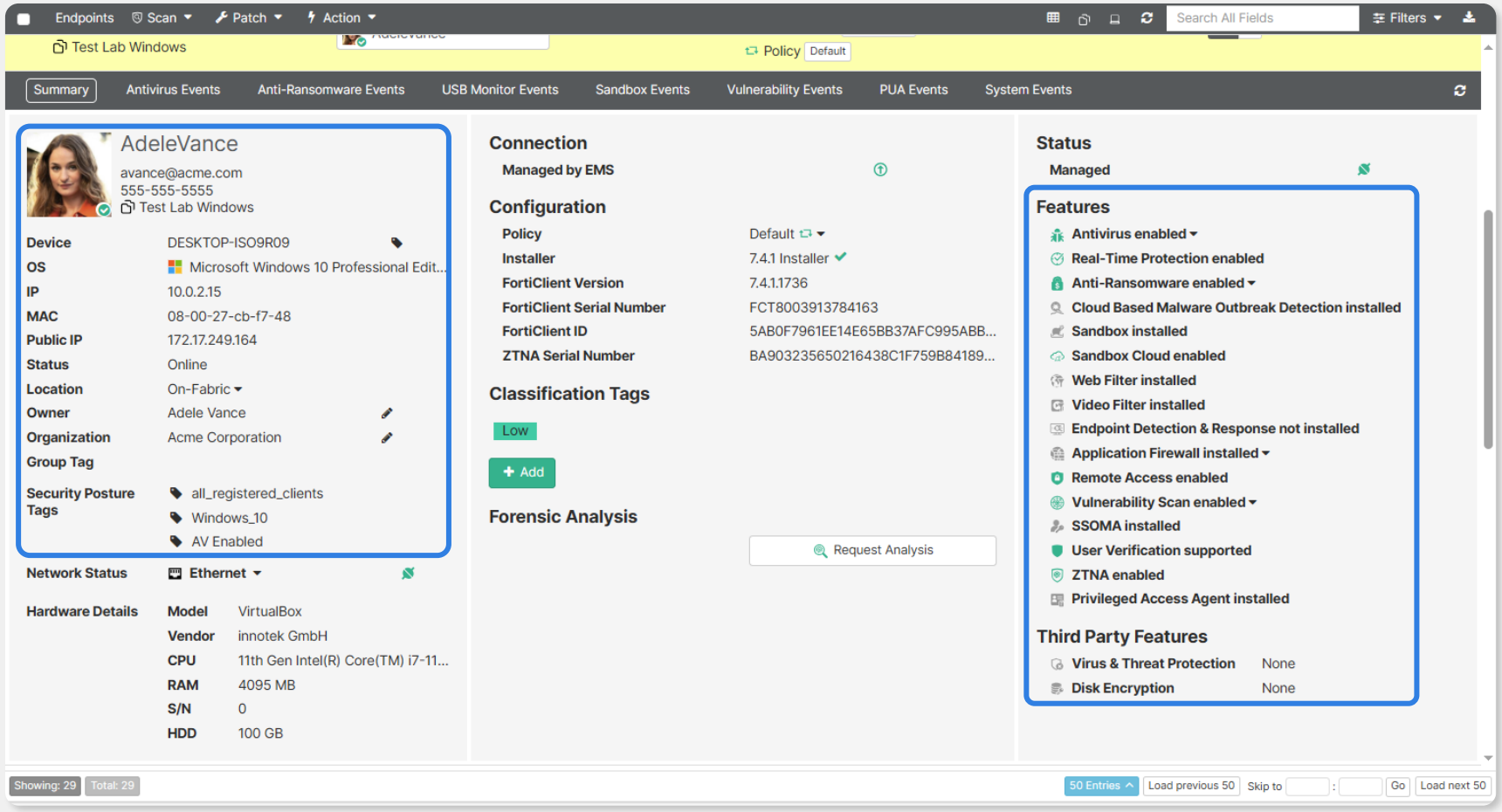
Endpoint Visibility and Control

Endpoint Telemetry, Vulnerability Scanning, Web Filtering

Endpoint Visibility and Control



Endpoint Visibility and Control



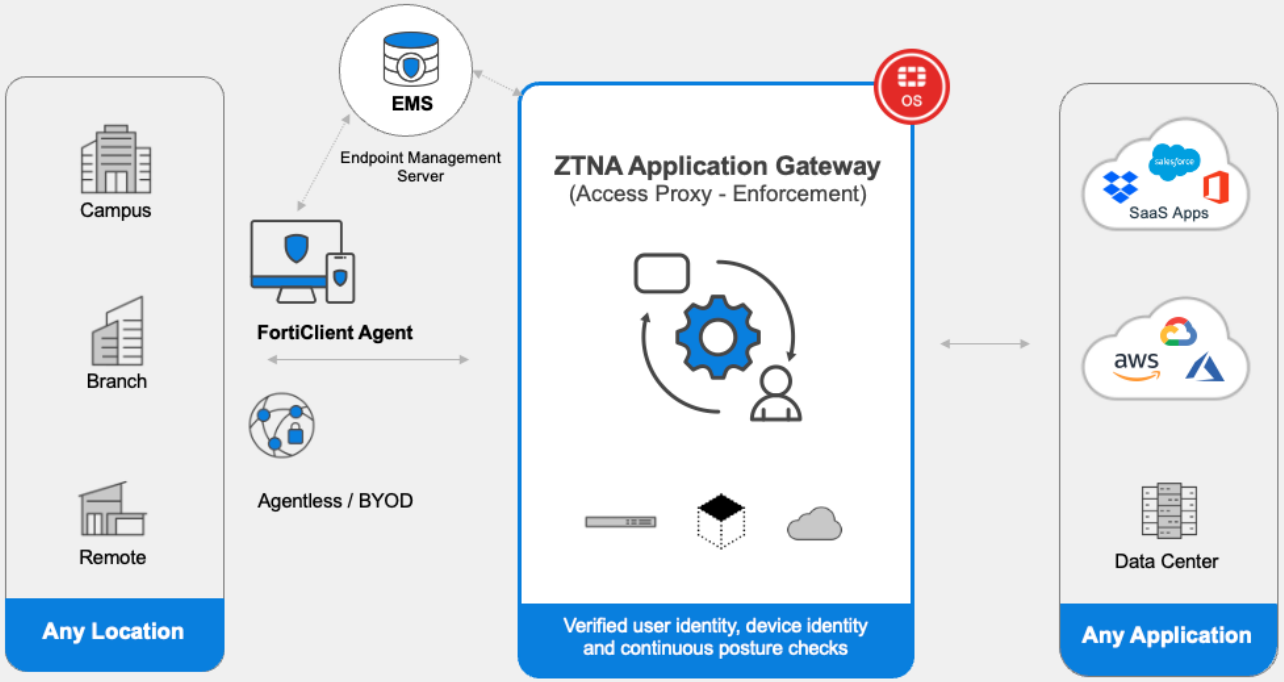
- Device Information
  OS, IP, MAC
- FortiClient Status
- Logged-in User
- Posture Tags
- Online / Offline
- Security Features Enabled
- Endpoint events and logs

Secure Access

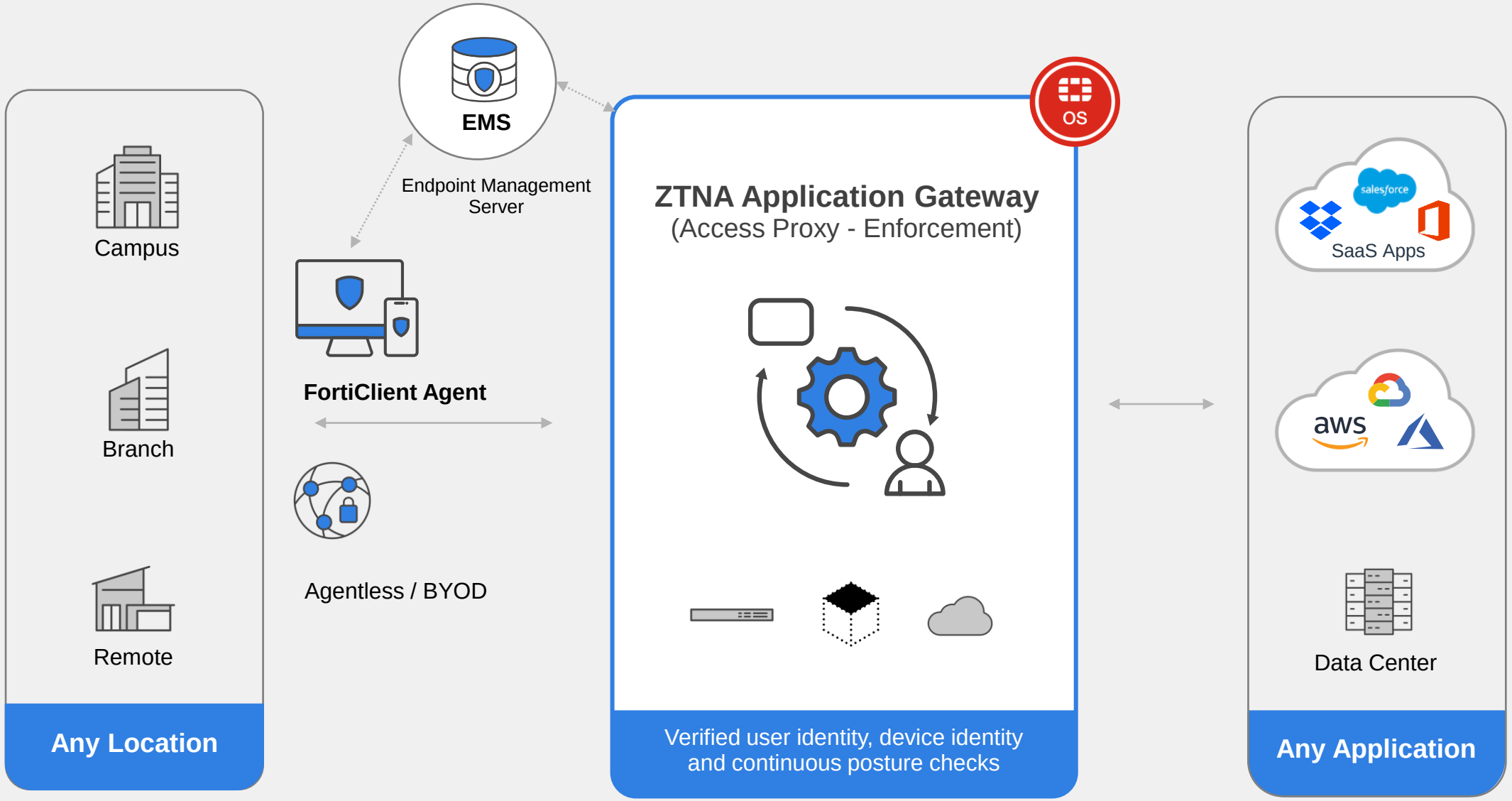
Universal ZTNA, VPN

Zero-Trust Access

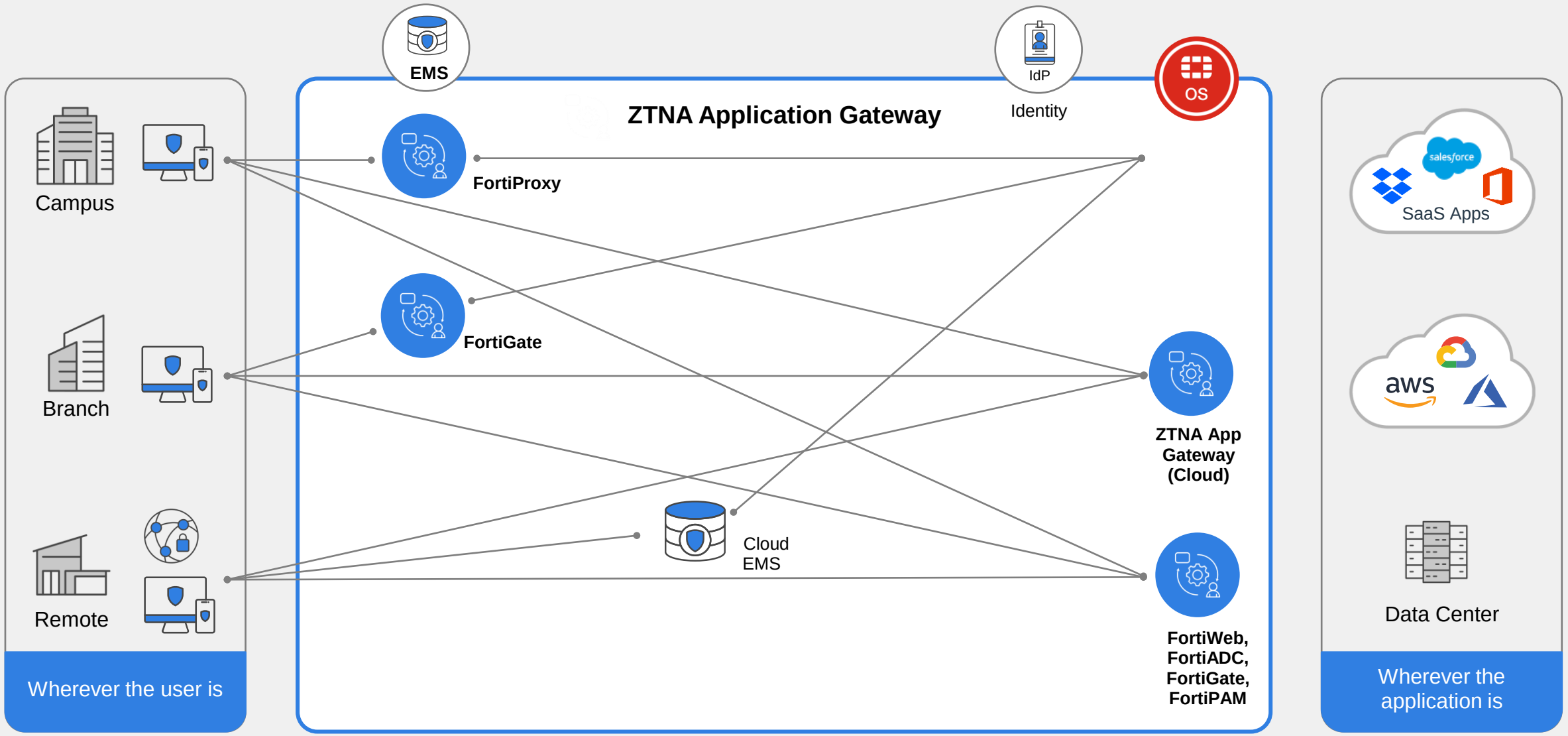
- **Key Benefits**
  - Improve security posture
  - Reduce attack surface
- **Universal ZTNA**
  - Access from on-prem and cloud
  - Verify user, device identity
  - Continuous posture assessment
- **Integrated Endpoint Security**
  - Vulnerability Scan
  - Web Filtering & SaaS Control



Fortinet Universal ZTNA Solution

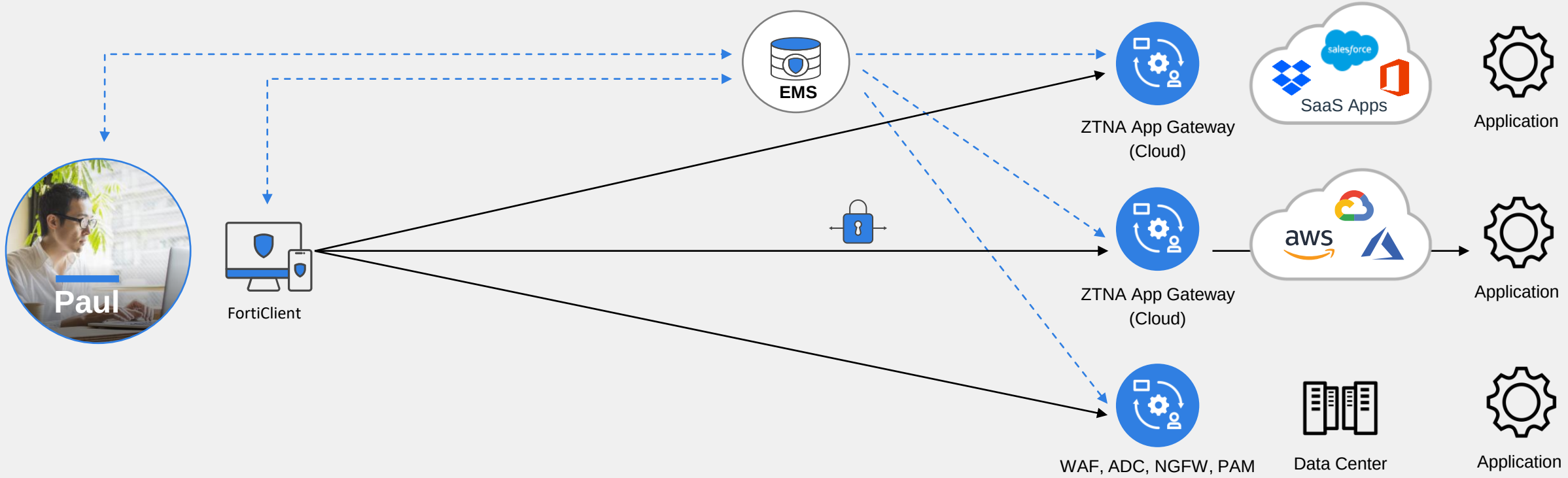


Fortinet Universal ZTNA Solution



Universal ZTNA Use Case: Remote Employee Access

Private application and SaaS



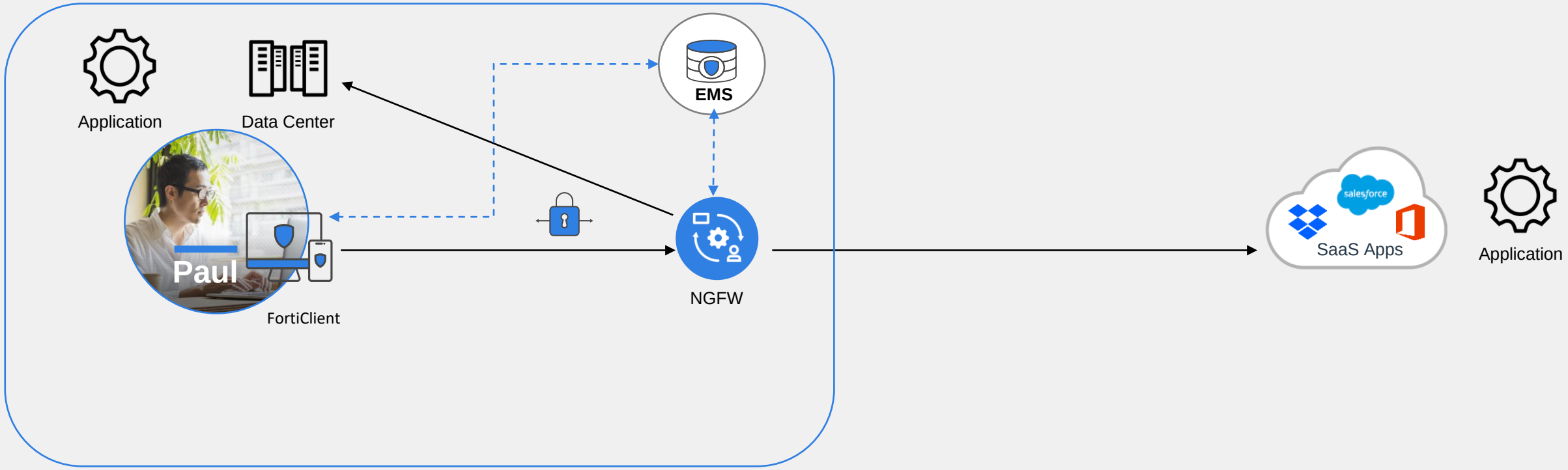
1. Validate Device
2. Verify User
3. Device Posture
4. Application Access Only
5. Encrypted Access

Benefits

- Low-latency for best user experience
- Continuous Verification
- Leverages Existing Infrastructure
- Traffic Security Inspection

Universal ZTNA Use Case: On-Prem Employee Access

On-prem data center/on-prem application and SaaS



1. Validate Device
2. Verify User
3. Device Posture
4. Application Access Only
5. Encrypted Access

Benefits

- Low-latency for best user experience
- Local Enforcement avoid cloud hairpinning
- Leverages Existing Infrastructure
- Full ZTNA controls
- Continuous Verification

Fortinet ZTNA

What's it made of? Existing Fortinet security fabric products that many customers already have

Core Elements

ZTNA Application Gateway

FortiOS

FortiOS performs access checks, maintains user group/application access table, proxies application (FOS 7.0+)

ZTNA Agent and Policy Orchestration

FortiClient/Central Management

FortiClient Central Management configures the ZTNA agent; FortiClient for ZTNA agent (FortiClient 7.0+)

Optional

Identity Solution

FortiAuthenticator

FortiToken

FortiTrust Identity

any 3rd party ID providers supported by the Security Fabric

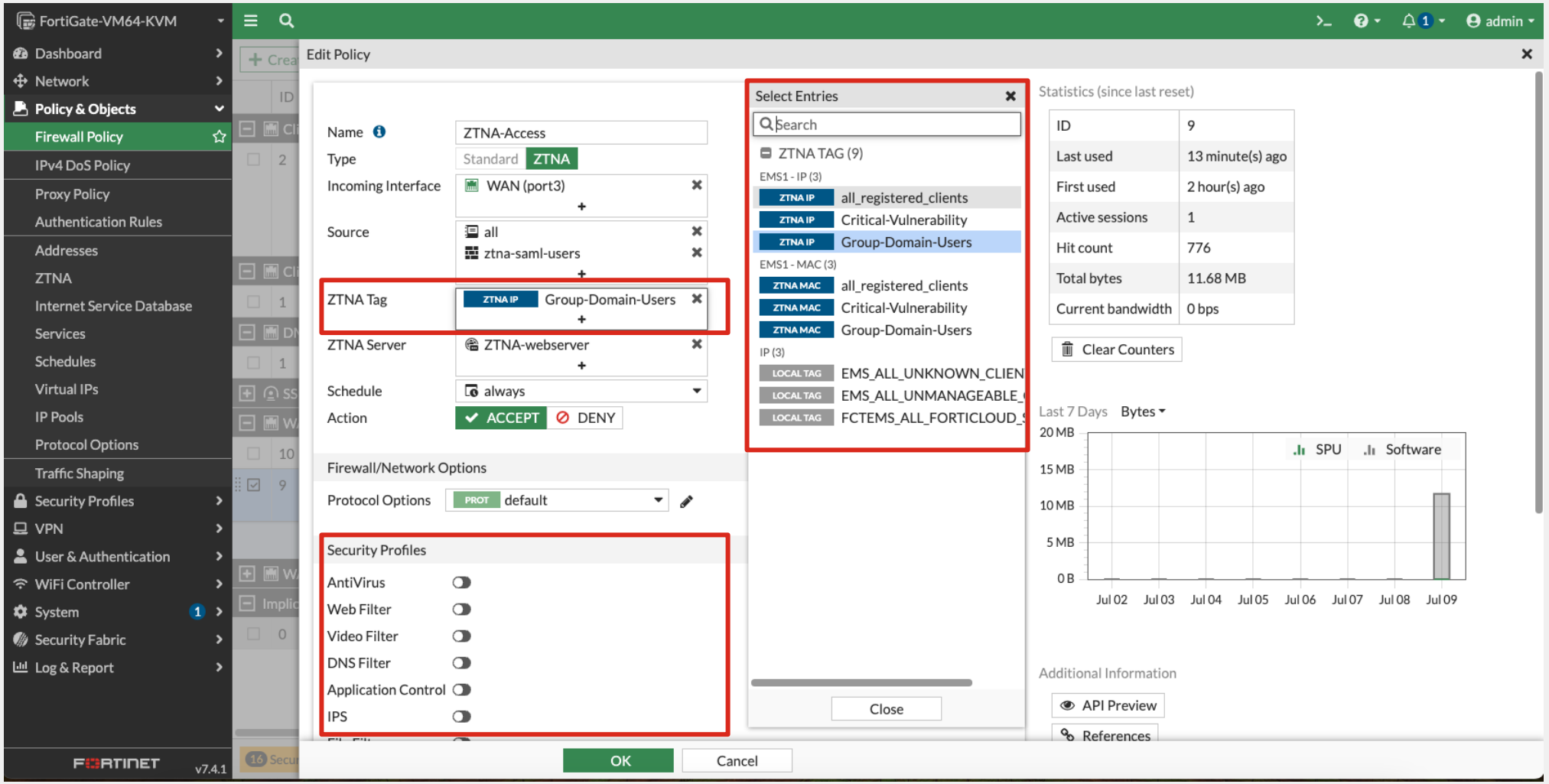
Secure VPN Connectivity with Endpoint Posture Validation

Feature	Free VPN-only standalone FortiClient	Licensed FortiClient
Basic VPN connection	Yes	Yes
Managed remote access profiles	No	Yes
Compliance using ZTNA tags: • Allow or block VPN connections based on ZTNA security posture • Per-firewall policy security posture checks using ZTNA tags	No	Yes

- Zero-trust posture checks as part of IPSec VPN (IKE v2) connection setup
- Only verified endpoints with validated ZTNA posture tags can connect via VPN
- Continuous ZTNA endpoint posture tag validation for VPN using firewall policies

Flexible Transition from VPN to ZTNA (Firewall Policy)

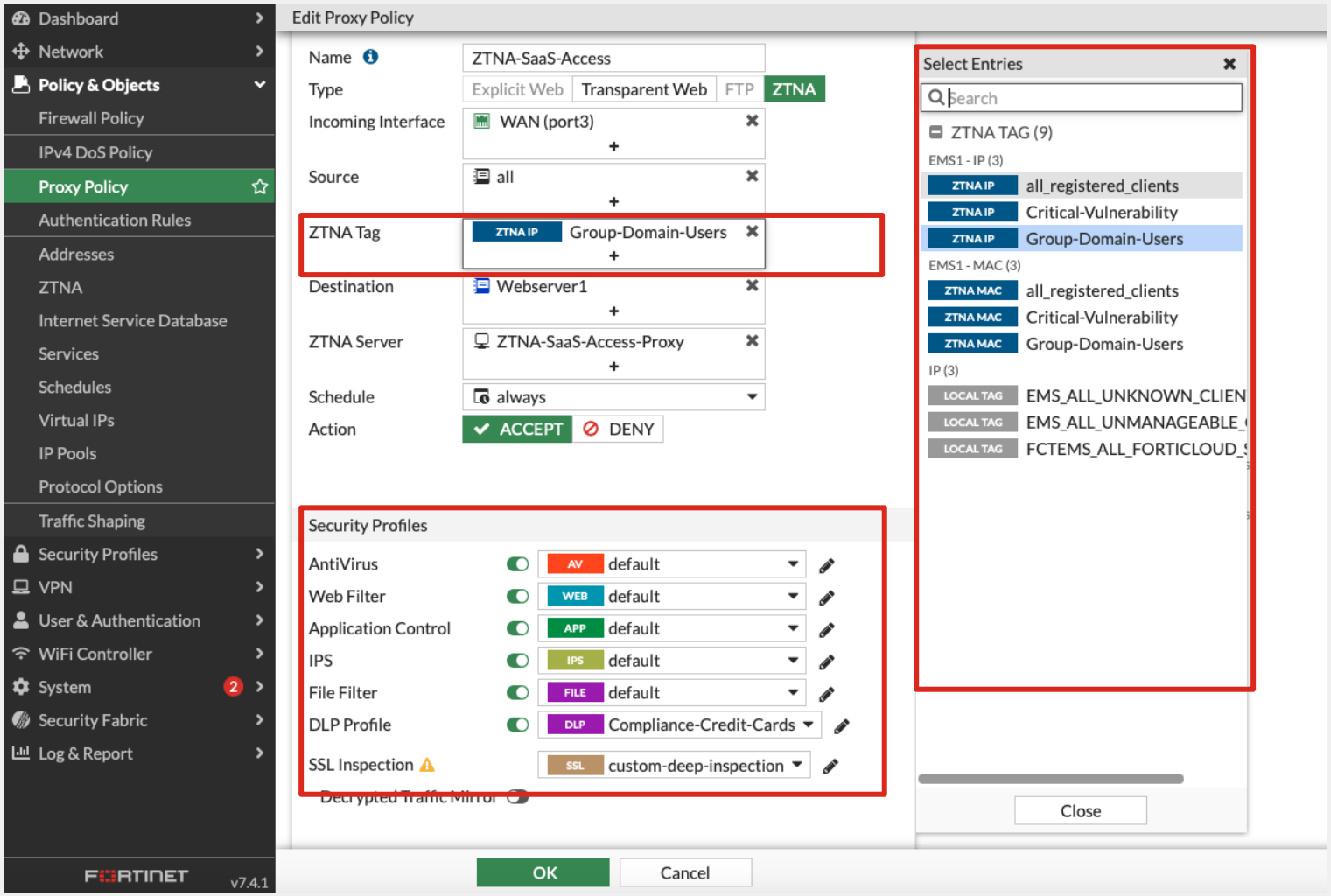
Define Firewall Policies based on Zero-Trust Posture Tags



- Specify one or more Zero-trust posture tags
- Supports comprehensive security inspection for VPN traffic

Flexible Transition from VPN to ZTNA (Proxy Policy)

Define Proxy ZTNA Policies based on Zero-Trust Tags



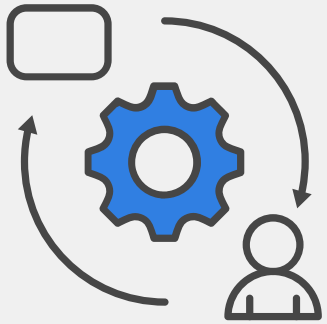
- Specify one or more Zero-trust posture tags
- Supports comprehensive security inspection for ZTNA traffic

Fortinet ZTNA Advantages

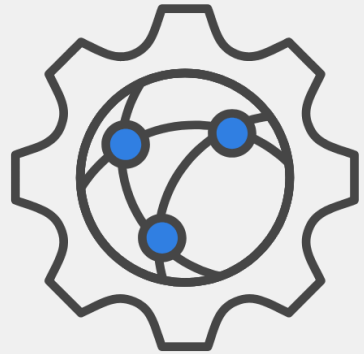
Convergence of capabilities, complete coverage, and cost

Universal ZTNA	Unified Agent	Lower TCO

- Complete location coverage based on FortiOS (on-prem and cloud)
- Full traffic inspection
- Near real-time posture verification



- Easy to transition from VPN to ZTNA
- Shift to ZTNA at customer's pace
- Unified agent with endpoint security



- Existing FortiClient VPN and FortiGate customers get ZTNA without additional license
- Simply a feature in FOS & FortiClient to turn on!

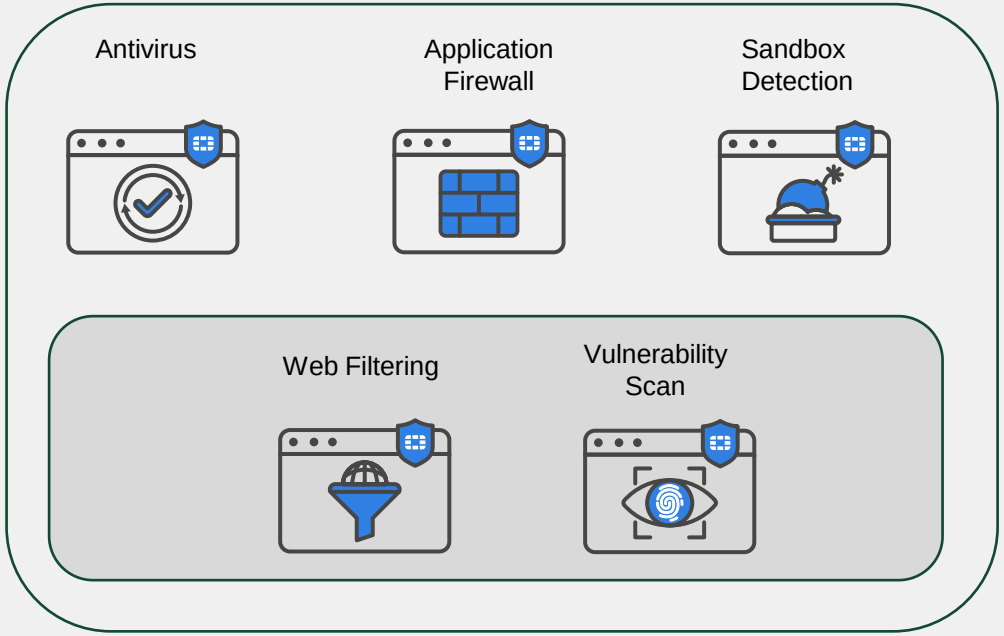
Endpoint Protection (EPP)

AI-powered Anti-Virus, Malware and Ransomware Protection

FortiClient EPP/ATP

- **Key Benefits**
  - Malware and Exploit Prevention
  - Ransomware Protection

- **Key Features**
  - AI-powered Anti-Virus
  - Application Firewall
  - Anti-exploit and Anti-ransomware
  - Sandbox detection
  - Removable media control



Detect and Block Malware and Advanced Threats

Anti-Virus and Malware Protection

- AV engine scans system files, executable files, root kits, drivers, removable media for malware
- Anti-malware engine uses Content Pattern Recognition Language (CPRL)
- Big data analysis, machine learning and AI in the Cloud
- Quarantine files that pose threat to endpoint

Anti-ransomware and Anti-exploit

- Anti-ransomware protects files and folders from unauthorized changes
- Restores files that the detected ransomware encrypted
- Anti-exploit protects endpoints from exploits that use zero-day or unpatched vulnerabilities

Sandbox Integration

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

FortiClient Customer Wins

FortiClient Customer Use Cases

Government Organization

- **Use case: Secure remote user access**
- **140,000** endpoint devices (tablets)
- Secure access from tablets with MFA
- Needed a remote access solution with centralized management and easy to use

Hotel Chain

- **Use case: Endpoint Hygiene and Control**
- **10,000** endpoints**, 13K** employees
- Endpoint posture & hygiene
- Centralized visibility and compliance
- Previously had issues with endpoint scans and PCI compliance

Construction Engineering

- **Use case: Universal ZTNA for on-prem and remote access**
- **13,000 endpoints**
- **Hybrid** application environment
- Local policy enforcement
- Had latency issues with previous cloud only ZTNA vendor solution

FortiClient Customer - Barnes Group

Aerospace manufacturer in US

Pains

- Need for ZT strategy organization wide for increased security
- Lack of control for business critical applications

Business outcomes

- Moved from free FortiClient to managed FortiClient was easy transition
- Transition from VPN to ZTNA is simple compared to alternatives
- Better security outcomes by providing granular application access
- Utilize existing FortiGate deployment

Manufacturing, US

https://www.onebarnes.com/

Competition

Symantec

Products

FortiClient

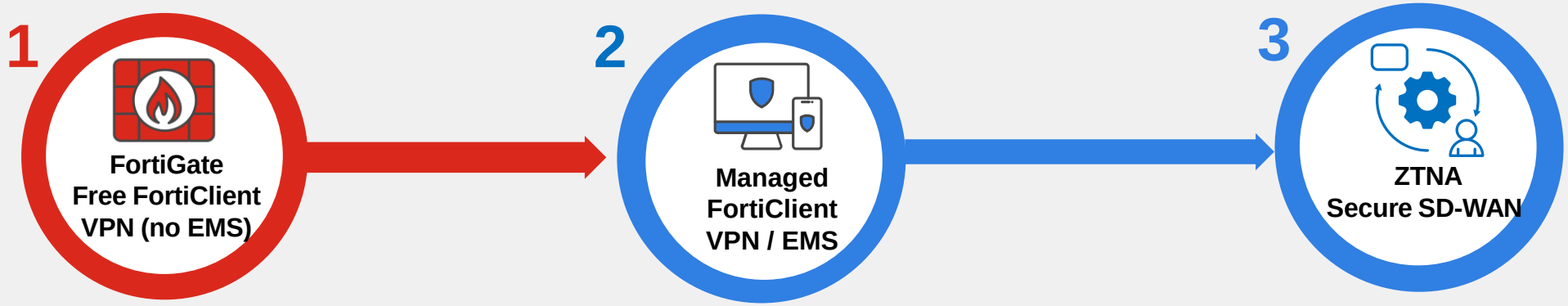
FortiGate

Use case

Secure remote access

AMER	1100 patents	41 Locations	2.5K ZTNA users **deal size**

FortiClient Customer Journey - Barnes Group



- Securing over 100+ Locations
- 150+ Firewalls with FortiGuard
- FortiManager
- FortiAnalyzer

- VPN with remote endpoint config without bringing on-prem
- Remote endpoint posture visibility
- Web filtering off-net internet access to secure endpoints

- ZTNA roll out for key applications (File server, ERP) to replace VPN
- Endpoint posture validation based on ZTNA tags (Patch status, Bit locker)
- Cost savings and simplified management with SD-WAN

FortiClient Services

Best Practices (BPS), Managed Services, Forensics Services

FortiClient Best Practices Service

Sharing Our Experience so Customers Get to Success Faster

- Phone-based advice on how to best configure FortiClient and FortiClient EMS
- Account-based, annual subscription
- Fortinet experts learn about the customers requirements and provide tailored recommendations
  - Sample code
  - Links to tools
  - Recommended technical documentation
  - Sample configurations
- Does not include logging into or configuring customer systems

FortiClient Managed Service

Offloading the Monitoring and Analysis of Endpoint

- Fortinet professionals actively assisting with deployment, configuration, management, and analysis of FortiClient deployments
- Cloud-provisioning of:
  - ZTNA and/or VPN
  - Endpoint Security
  - Vulnerability management
  - Posture Check tools
- Endpoint onboarding (putting FortiClient onto customer devices)
- Vulnerability monitoring & reporting (with recommendations)
- Requires FortiClient Cloud

FortiClient Forensic Service

Post-event review, analysis and reporting

- Helps customers respond and recover from incidents
- Fortinet professionals will collect info, analyze, and report
  - Accelerates response time to an event
  - Offloads customer teams
- For FortiClient Cloud & on-prem
- Annual subscription (not per-incident)
  - No restriction on number of incidents

FortiClient Delivers Visibility, Secure Access and Endpoint Protection

Endpoint Visibility and Control

- Endpoint Telemetry
- Vulnerability Scanning
- Web Filtering
- Patching Policy

Secure Access

- Universal ZTNA
- VPN
- Single sign on (SSO)

Endpoint Protection (EPP)

- AI-powered Anti-Virus
- Anti-exploit
- Ransomware Protection
- Automated quarantine


FORTINET