FORTINET FEDERAL® With Innovative Solutions

CSMA - Including Zero Trust & Secure SD-WAN

Mark Wiggins – Director, DoD

Ben Brooks – Systems Engineer, DoD

Bob Heriford- CEO, Innovative Solutions

Fortinet Federal Value: DCSA Action Plan

- Fortinet Federal Inc, Fortinet Inc., and DCSA entered into a Security Control Agreement (SCA) in late October 2021.
- The SCA requires that Fortinet Federal, Inc. operate as an independent entity from Fortinet, Inc.
- Fortinet Federal Inc. (FFI) is operating as an independent entity from Fortinet Inc. FFI is controlled by a Government Security Committee (GSC) made up of:
    - Cindy Moran - Chairman of the Board
    - Honorable William “Mac” Thornberry - GSC Chair
    - Jim Loi - GSC Board Member

Fortinet Federal Value: DCSA Action Plan

- Fortinet Federal, Inc. and the GSC controls the list of products that it offers for sale to USG and DIB customers. It has the authority to accept or reject any product from Fortinet, Inc. based upon its assessment of supply chain security and quality of that product.
- Fortinet products sold by FFI require approval by the GSC for Security Gate Certification and conformity to the SCA-required supply chain processes.
- All products that are being sold through FFI are Trade Agreements Act (TAA) compliant. All products also will have necessary Department of Defense (DoD) certifications (or such certifications will be obtained when needed).
- Fortinet Inc. has adopted through board resolutions the security controls of NIST 800-161.

Fortinet Federal Value: DCSA Action Plan

- Fortinet Inc. has appointed a Federal Compliance Officer to oversee implementation agreed upon measures within Fortinet Inc.

- FFI will operate as the Exclusive Distributor of Fortinet products sold to US Government Customers. As the Master Distributor, FFI will provide the following logistical services to comply with the SCA:

  Distribution warehouse with access and visibility to US persons only.
  Masking of end customer information from any Fortinet employee.
  Final Security check pertinent to US Government Customers.

DCSA SCA Implementation Status

Fortinet Federal Inc

- Per the Electronic Control Plan (ECP) in conjunction with the SCA, FFI will operate its own, separate IT Network within Microsoft's GCC High Environment in the Gov Cloud. This separate network will run all FFI's business applications needed to run as an independent entity.

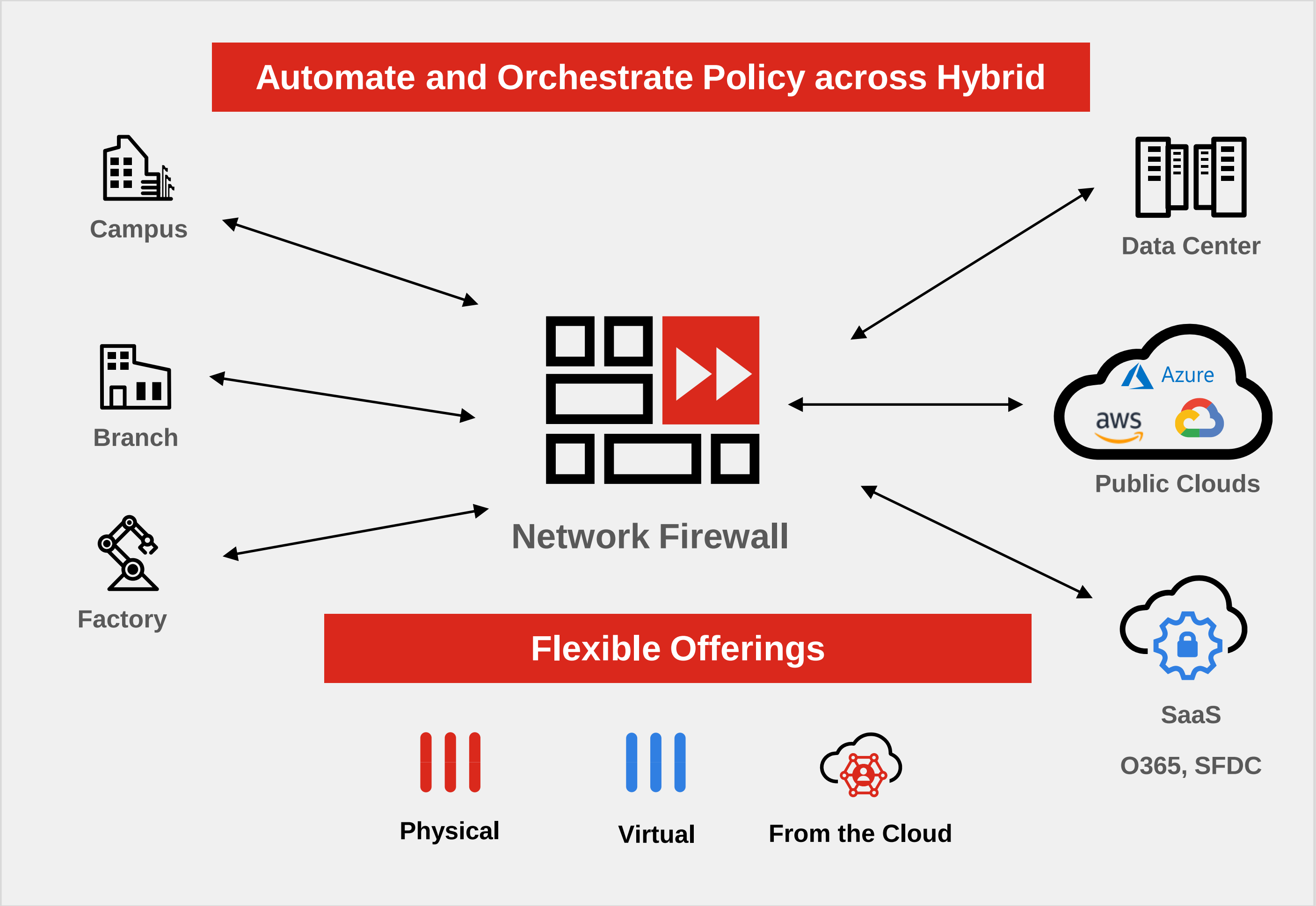
- This includes Salesforce CRM, Oracle Financials, MS Office 365, and Salesforce Service Cloud.

- FFI's system will not be accessible by Fortinet Employees. Only FFI employees and/or vetted contractors will be allowed access to ensure customer information integrity and security.

Fortinet Federal Security Fabric & CSMA

FORTINET FEDERAL

Next Generation Firewall - FortiGate



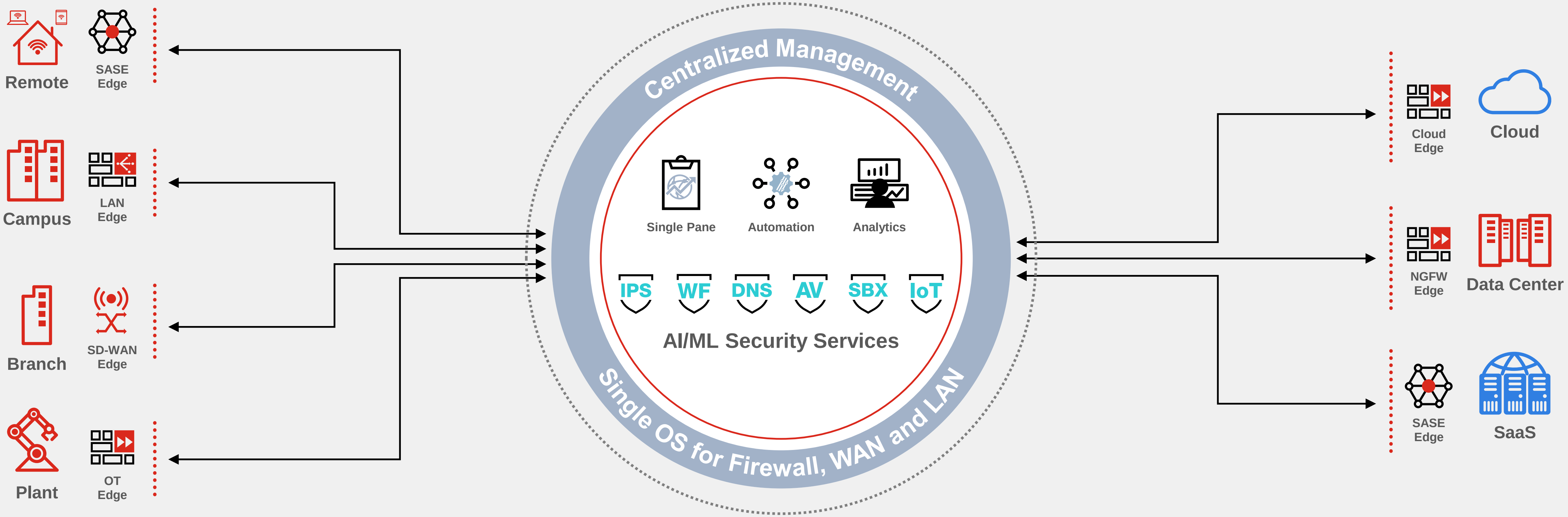
PROTECT | Network Segmentation
Threat Protection

CONSOLIDATE | AI/ML FortiGuard Services
IPS, Web and Video Filtering

HYPERSCALE | NP 7 powered ultra-fast FW
HW assisted anti-DDoS

Security-Driven Networking: Our Unique Approach

Consistent Security Across all Network Edges



Convergence of Security and Networking Using Purpose-built HW

Automation-driven Single Pane Management and Analytics

Convergence of Security and Networking Using VM and SASE

FORTINET FEDERAL

Fortinet Federal Security Fabric

Broad

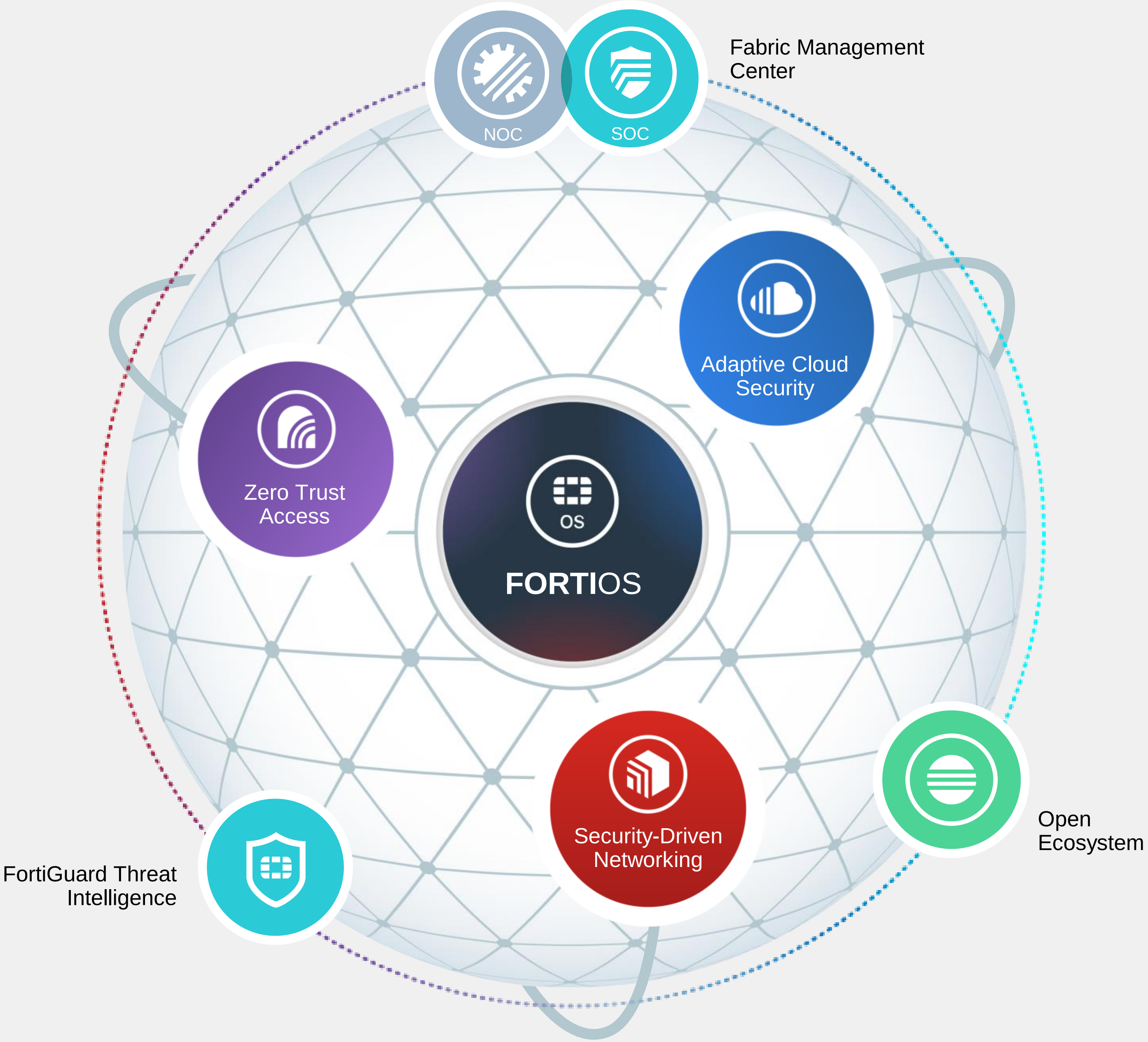
visibility and protection of the entire digital attack surface to better manage risk

Integrated

solution that reduces management complexity and shares threat intelligence

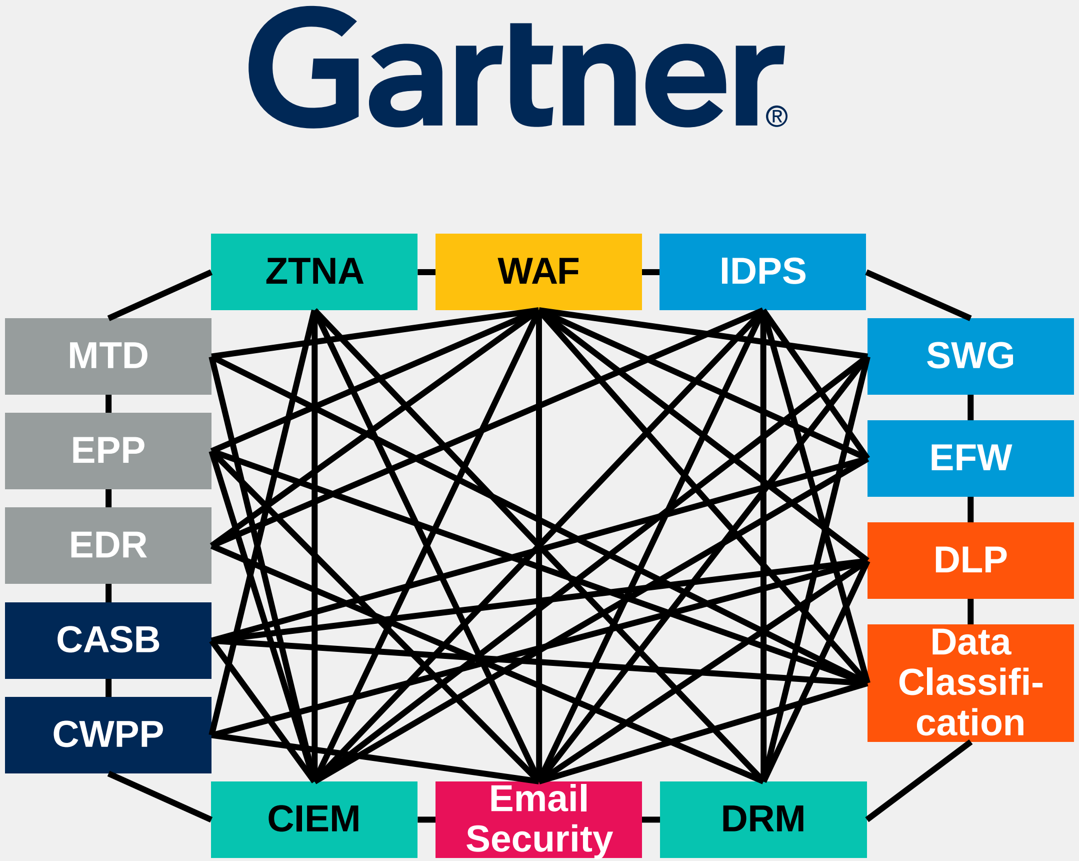
Automated

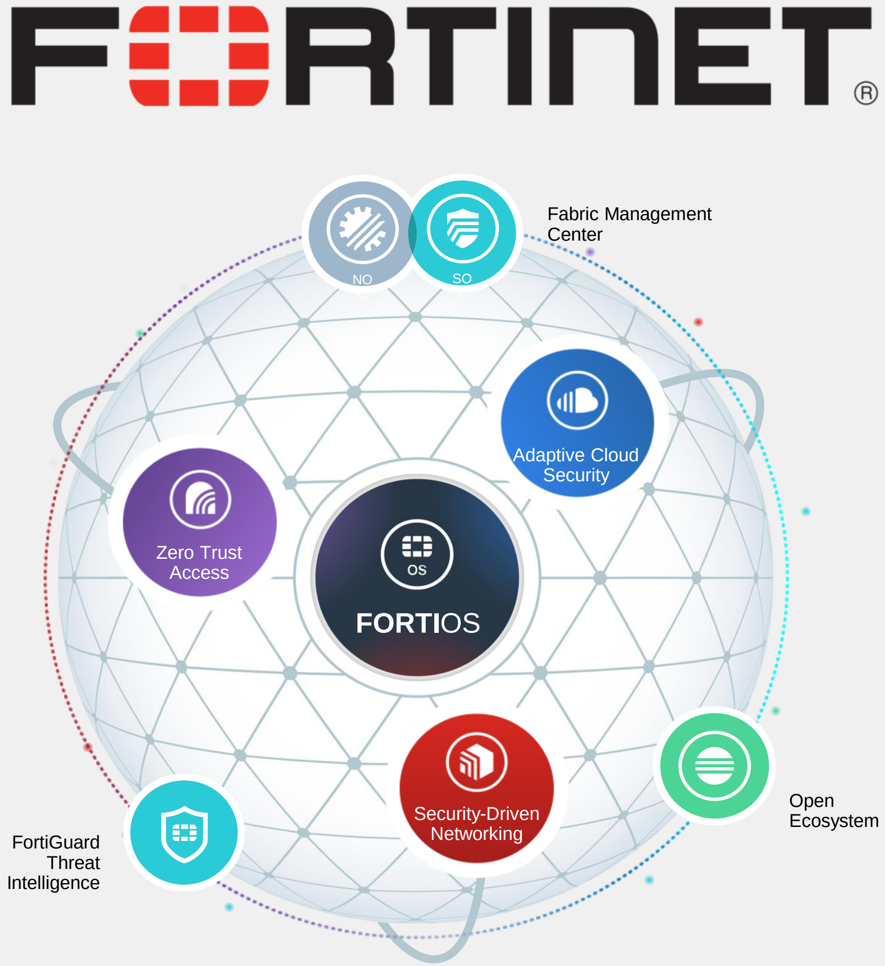
self-healing networks with AI-driven security for fast and efficient operations



FORTINET FEDERAL

Gartner Cybersecurity Mesh Architecture





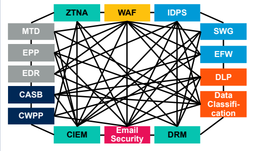
Executive Guide to Cybersecurity Mesh, 2022

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

This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from Fortinet.

Fortinet Federal Security Fabric IS a Cybersecurity Mesh Platform

Gartner CSMA



Identity, Access, & Content Control

Security Intelligence, Analytics, Detection & Response

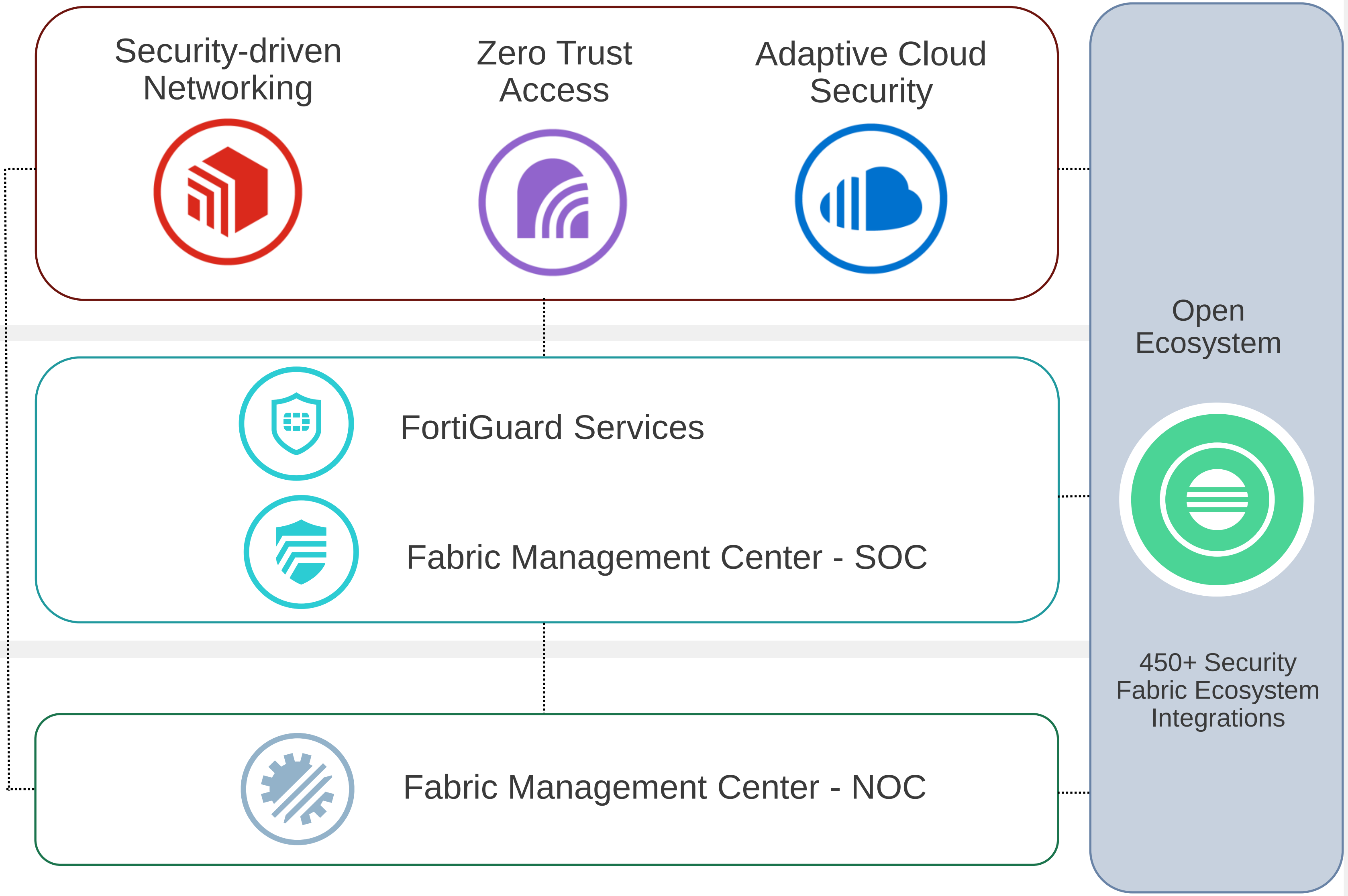
Policy Management & Orchestration, Dashboards

Executive Guide to Cybersecurity Mesh, 2022

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

This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from Fortinet.

Fortinet Security Fabric



Security-driven Networking

Zero Trust Access

Adaptive Cloud Security

FortiGuard Services

Fabric Management Center - SOC

Fabric Management Center - NOC

Open Ecosystem

450+ Security Fabric Ecosystem Integrations

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

Open Ecosystem

500+ Best-in-class integrated solutions for comprehensive protection

Fabric Connectors	Fortinet-developed deep integration automating security operations and policies	aws aruba a Hewlett Packard Enterprise company cisco Google Cloud IBM Cloud Microsoft Azure ORACLE servicenow Symantec.
Fabric APIs	Partner-developed integration using Fabric APIs providing broad visibility with end-to-end solutions	ARISTA ASAVIE DELL DRAGOS EQUINIX intel SIEMENS Ingenuity for life splunk> TIGERA tufin
Fabric DevOps	Community-driven DevOps scripts automating network and security provisioning, configuration, and orchestration	aws Google Cloud HashiCorp Microsoft Azure openstack. ORACLE RED HAT ANSIBLE Automation refactr vmware
Extended Ecosystem	Integrations with threat sharing initiatives and other vendor technologies	CYBER THREAT ALLIANCE MITRE STIX INTERPOL OT CSA Firewalls Switching Wireless Endpoint Security

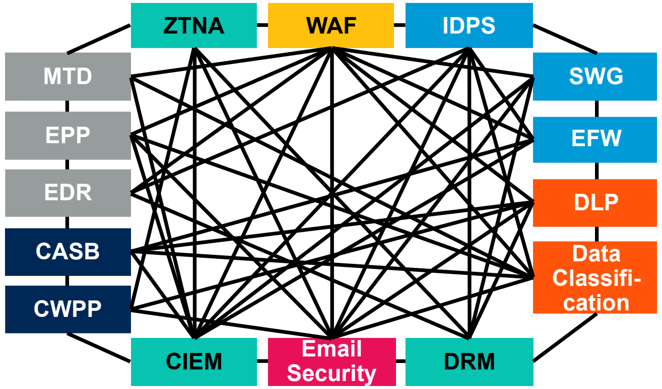
Figures as of March 31, 2021

Note: Logos are a representative subset of the Security Fabric Ecosystem

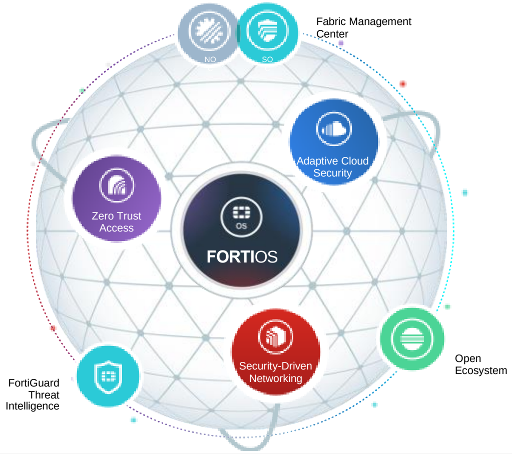
FORTINET FEDERAL.

Key Takeaways

Gartner



FORTINET



“By 2024, organizations adopting a cybersecurity mesh architecture to integrate security tools to work as a collaborative ecosystem will reduce the financial impact of individual security incidents by an average of 90%”

“Top Strategic Technology Trends for 2022: Cybersecurity Mesh, Felix Gaehtgens, James Hoover, Henrique Teixeira, Claudio Neiva, Michael Kelley, Mary Ruddy, Patrick Hevesi, 18 October 2021”

Executive Guide to Cybersecurity Mesh, 2022
Felix Gaehtgens, James Hoover, Henrique Teixeira, Claudio Neiva, Michael Kelley, Mary Ruddy, Patrick Hevesi. As of October 2021

This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from Fortinet.

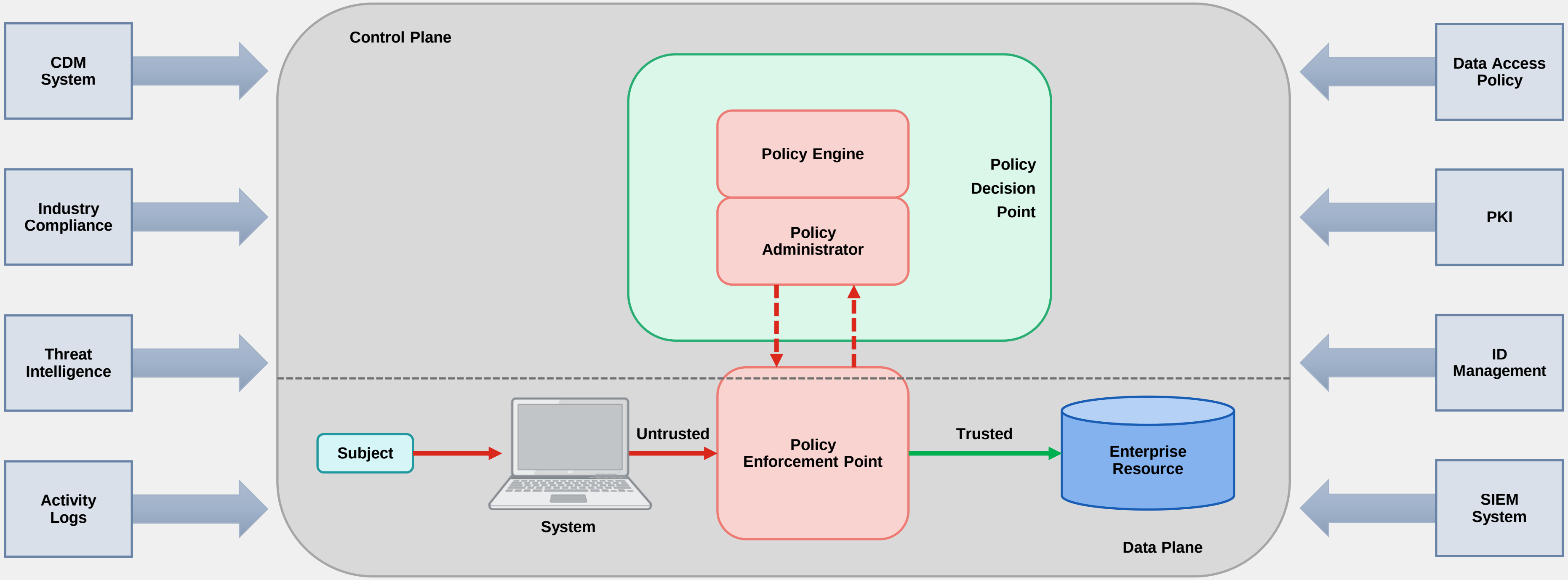
Fortinet Federal Security Fabric delivers benefits of a cybersecurity mesh architecture today

- Deep visibility across all edges
- Centrally managing distributed solutions
- Consistent enforcement of policies
- Real-time global threat intelligence across Security Fabric deployments
- Automating actionable responses
  Broadest, most integrated open ecosystem

Fortinet Federal Zero Trust Architecture

NIST ZT Architecture

Core Zero Trust Logical Components

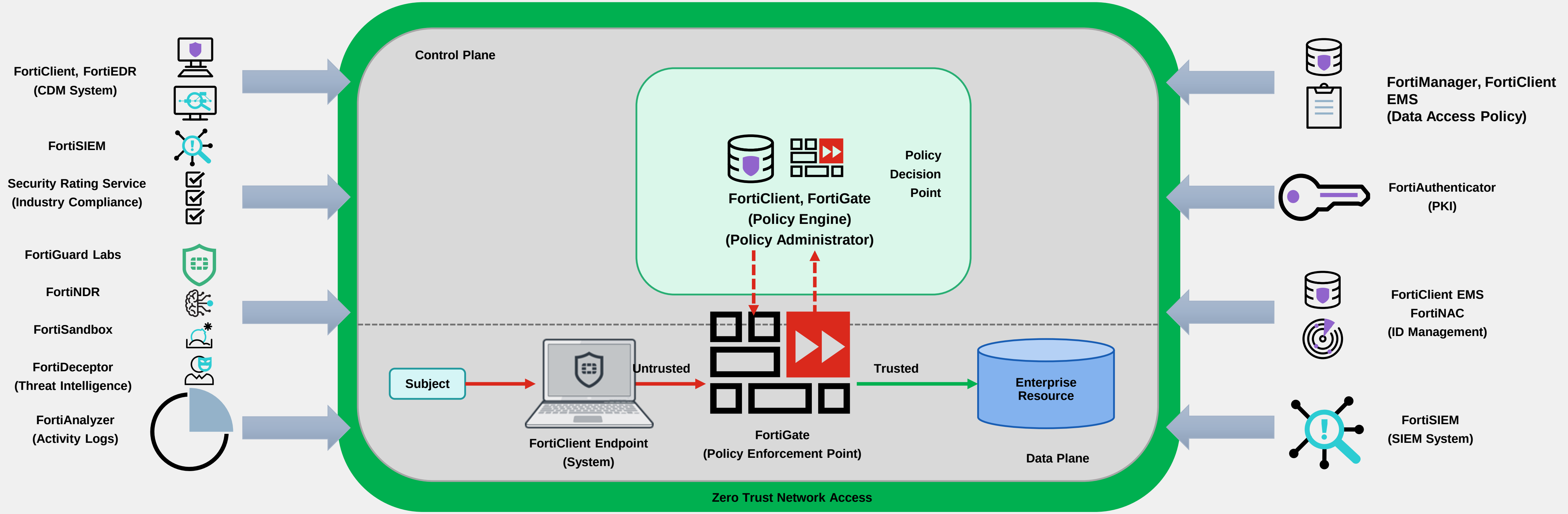


FORTINET FEDERAL

(Rose, Borchert, Mitchell and Connelly, 2020)

Delivering NIST ZTA

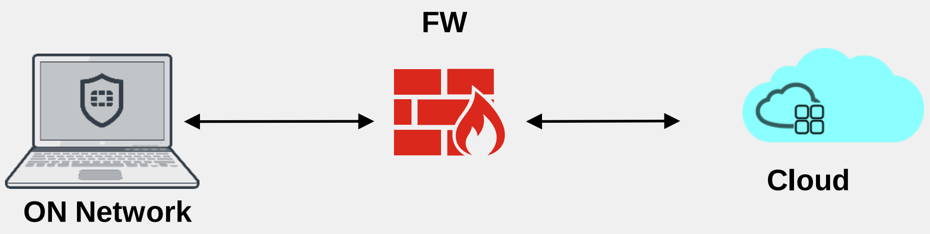
Fortinet Federal Zero Trust Solutions



FORTINET FEDERAL

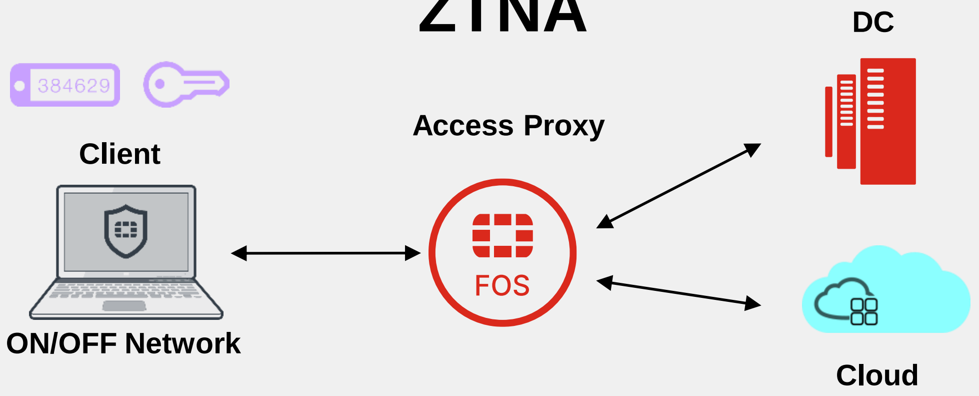
Evolution from Traditional FW to ZTNA

Traditional FW



- IP based firewall matching criteria
- Clients have unfettered access within broadcast domains
- Security is provided only when traffic must traverse the Gateway/Proxy

ZTNA



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

Fortinet Federal ZTNA

What's it made of?

CORE ELEMENTS

ZTNA Application Gateway

FortiOS

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

ZTNA Agent & Policy Orchestration

FortiClient/Central Management

FortiClient Central Management configures the ZTNA agent; FortiClient for the encrypted tunnel, posture assessment (FortiClient 7.0+)

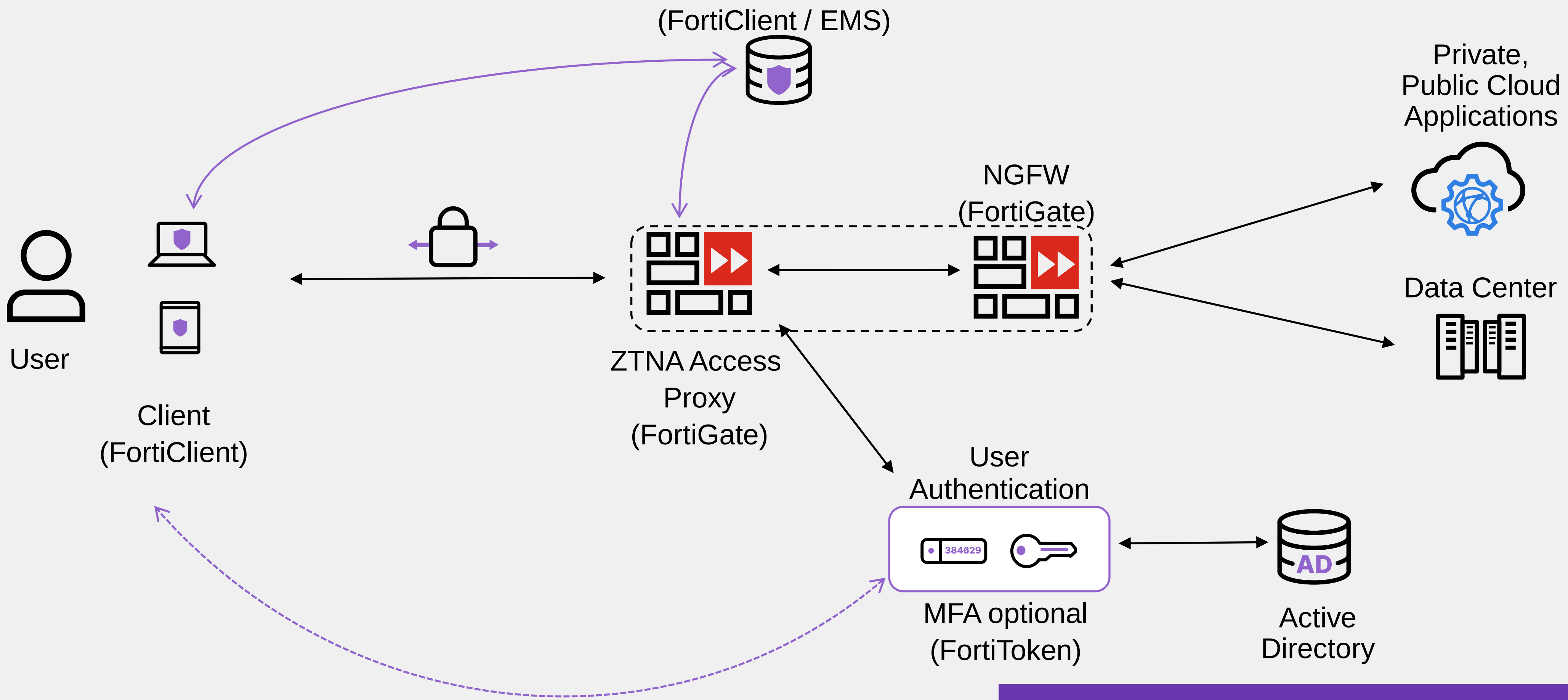
Authentication Solution

FortiAuthenticator

FortiToken

any 3rd party ID providers supported by the Security Fabric

Zero Trust Network Access (ZTNA) Architecture



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

FORTINET
FEDERAL.

ZTNA Benefits Summary

Granular Risk Mitigation

1

- Identify & Authenticate device
- Authorized device or BYOD?
- Approved for access? revoked?

2

- User identity should be verified
- Strong MFA
- Role-based access controls

3

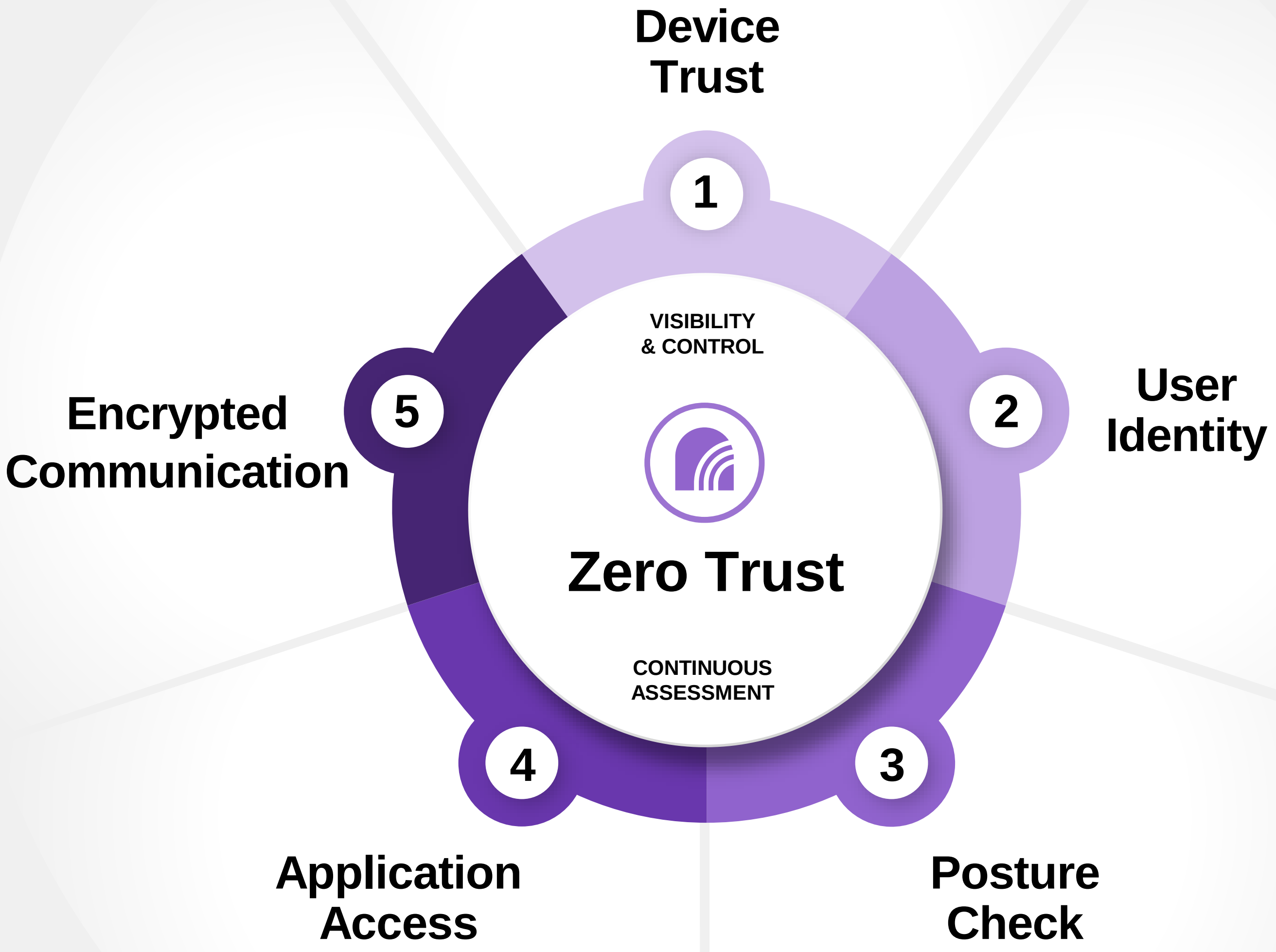
- Adaptive and conditional access
- Security Compliance
- Device Vulnerabilities

4

- Verify Application Access
- Application Specific Access
- Application not available to internet

5

- End-to-end encryption
- Data protection
- All communication is logged

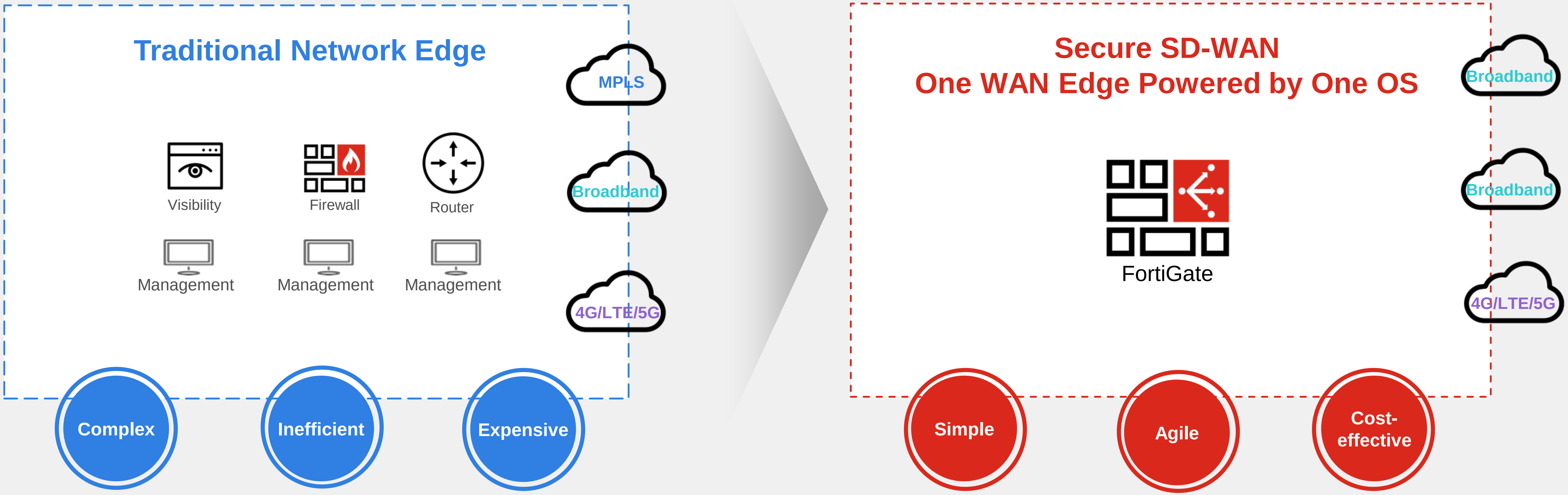


FORTINET FEDERAL

Fortinet Federal Secure SD-WAN

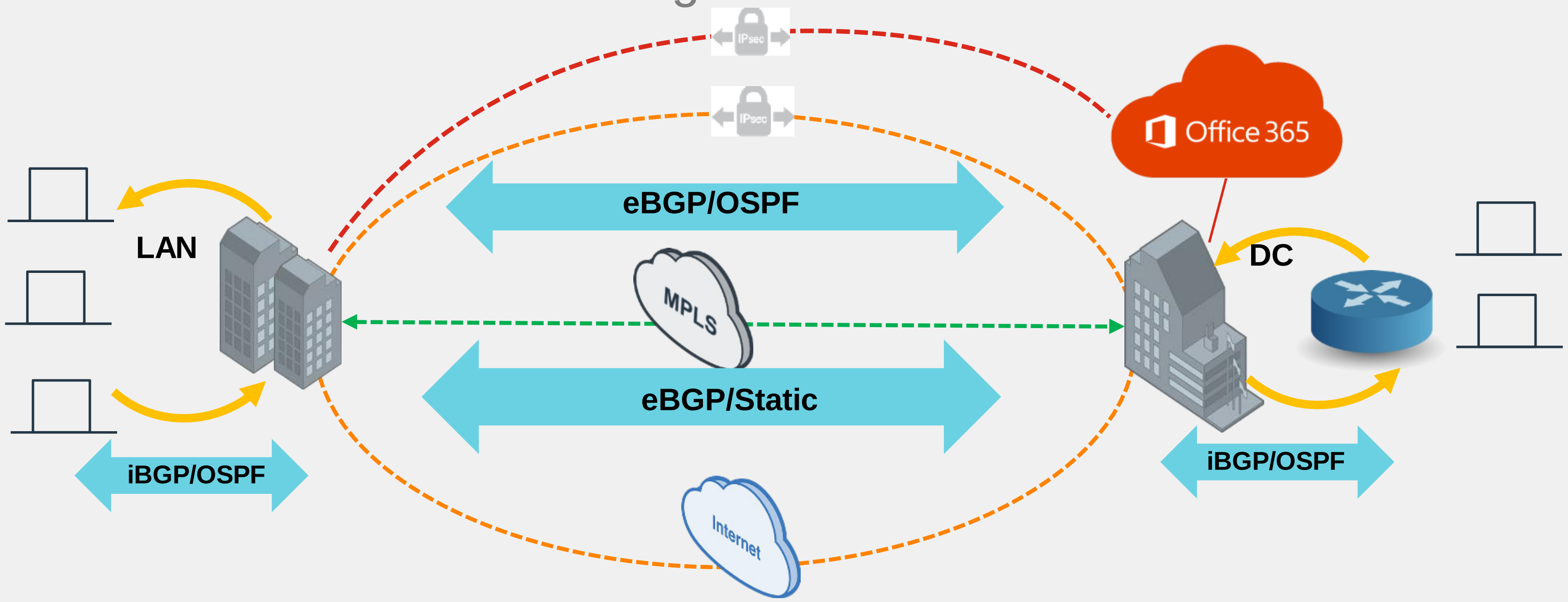
Simplified Architecture and Management

Consolidated Functions into One WAN Edge Powered by One OS



Rich Routing and Networking Capabilities

Replace Legacy routers with Fortinet advanced routing stack



Seamless Interoperability

- Establish peering with any vendor appliance
- RFC standard implementation
- Interoperable with versions

Reachability

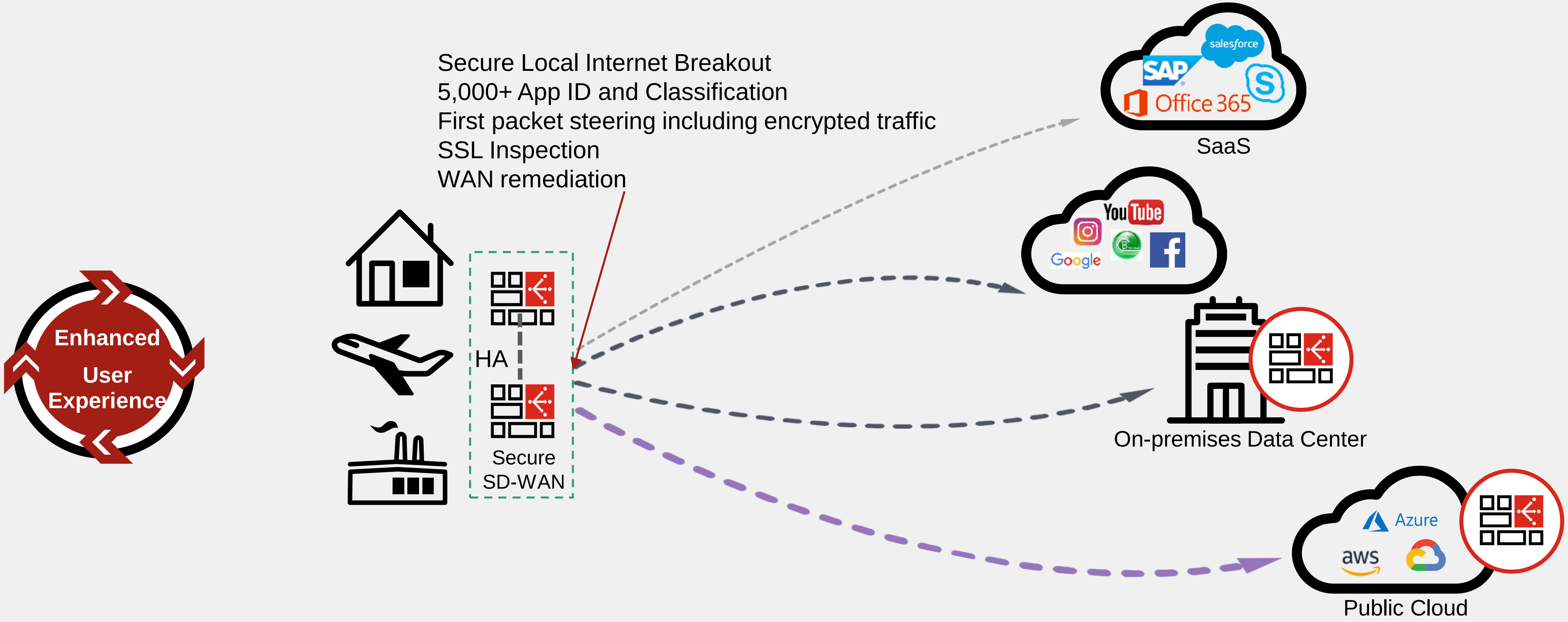
- IGP/EGP redistribution
- Configuration based route aggregation
- Best route selection

Recovery & Convergence

- Protocol built-in Route loop avoidance
- Powerful hardware acceleration
- RFC defined route dampening and reflectors

Enabling Application Resilience

At Any Remote Edge



Enhanced User Experience

Secure Local Internet Breakout
5,000+ App ID and Classification
First packet steering including encrypted traffic
SSL Inspection
WAN remediation

HA

Secure SD-WAN

SaaS

On-premises Data Center

Public Cloud

Intelligent Steering
Traffic Agnostic

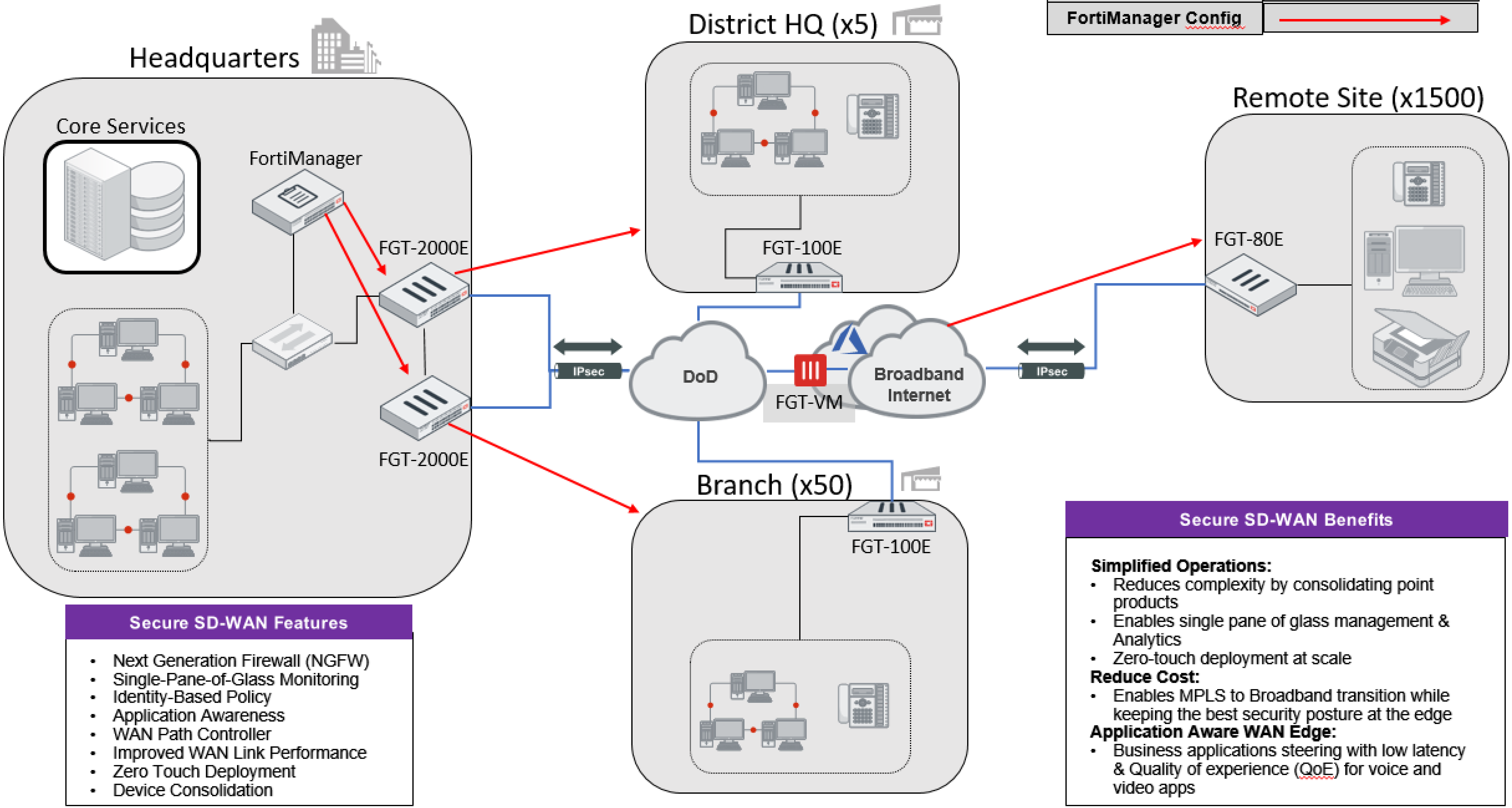
Reliable Accuracy
Including encrypted traffic

Continuous Learning
Broadest support 5k+ apps

Self-healing
Realtime Optimization

DoD Secure SD-WAN with ADVPN Deployment

Legend	
SD-WAN Tunnels	—
FortiManager Config	→



Secure SD-WAN Features

- Next Generation Firewall (NGFW)
- Single-Pane-of-Glass Monitoring
- Identity-Based Policy
- Application Awareness
- WAN Path Controller
- Improved WAN Link Performance
- Zero Touch Deployment
- Device Consolidation

Secure SD-WAN Benefits

Simplified Operations:
- Reduces complexity by consolidating point products
- Enables single pane of glass management & Analytics
- Zero-touch deployment at scale

Reduce Cost:
- Enables MPLS to Broadband transition while keeping the best security posture at the edge

Application Aware WAN Edge:
- Business applications steering with low latency & Quality of experience (QoE) for voice and video apps

Thank you!

- Robert Heriford, President/CEO Innovative Solutions, Inc (SDVOSB)
  - robert.heriford@inn-sols.com
  - P: 719-494-6182
- Mark Wiggins, Director DoD
  - markwiggins@fortinetfederal.com
  - P: 571-562-1521
- John Winters, MAM – Army/IC
  - jwinters@fortinetfederal.com
  - P: 703-628-9807
- Ben Brooks, Systems Engineer DoD
  - bbrooks@fortinetfederal.com
  - P: 443-280-0067

FORTINET FEDERAL®