



Fortify Your Cybersecurity

Kevin Lopez

Major Account Manager – State/Local Gov, Education

Brant Davis

System Engineer – State/Local Gov, Education

Summary

Cybersecurity isn't just one thing; it's a mindset and must be considered in all digital environments. With many complex environments comes many threat attack vectors and protecting those environments will require multiple approaches. With that said, there are minimum considerations that can be utilized when it comes to School Safety regarding digital systems.

From reports that have been posted in the media about recent breaches, cybersecurity best practices are top of mind. For one company providing services to public schools, hackers gained access through a company's support portal with valid credentials. From these reports, access to "all" of the historical student and teacher data stored in their student information systems were obtained. It was called out that the main reason this data was accessed was that the company did not secure their affected system with **basic protections, such as multi-factor authentication.**

Other reports of breaches that have occurred within Utah at local school districts would have required some other form of protection. As understood in those situations, an unauthorized actor gained access to certain computer systems and acquired files stored on those systems. This protection method would have been better served by having some type of **Endpoint Detection and Response service** that proactively monitors laptops and devices 24/7.



Best Practices

When looking at best practices there are 4 elements to consider:

1. The individual users. In this case, students, staff members and parents.
 - That includes the user and their devices.
2. The systems that are built and controlled by our schools.
 - These are generally managed by the school's IT teams.
3. Supply chain and the systems that are provided by vendors. These can be cloud and SaaS type technology services.
4. Finally, the network connection that provides the pathway accessing either type of system that connects the users to these applications must be protected.



For the Individual Users

1. Identity Management tools that can enable multifactor authentication. Everyone uses this type of validation when you access an app that asks to send you a text with a code.
 - Industry experts have reported that implementing Multi-Factor Authentication (MFA) can significantly increase security by reducing the risk of account compromise by up to 99.9%, meaning it can effectively block a vast majority of hacking attempts even if a password is compromised
2. Device protection for the devices that those individuals are using. Adding tools on the device that can inspect, detect and classify events for potential threat vulnerabilities can provide valuable threat insights all day, every day.
 - An Endpoint Detection and Response tool can be implemented that can provide this proactive protection along with response teams to help mitigate the risks and provide analysis of potential threat attacks.
3. Zero Trust Network Access or ZTNA methods should be enabled that take identity and match it to the application across any network connection.
 - Additional tools fall under this methodology like the use of network access controls, segmentation to limit users to specific applications and device management.



For the School Built Systems

1. Protect these systems with next generation firewalls
 - This has been table stakes for most school systems and IT organizations. This is a basic tool, but many firewalls are not fully utilizing all available services like network segmentation, deep packet inspection or cloud monitoring tools that can give IT teams more detail on where threats may be coming from.
2. Utilize tools that support role-based access like a privileged access management tool.
 - These tools will monitor who has access to what systems and track the changes made by those individuals. This can provide a record of changes made and even undo unwanted changes made to systems.
3. IT Teams should manage and create the Zero Trust framework for users. This gives controls to specific applications and can be matched up to identity and the user devices.
 - Network segmentation and Zero Trust is one of the highest recommended practices by industry experts.
4. Follow the compliance guidelines like NIST standards that provide security frameworks in IT Systems
5. Consider doing a risk assessment of your IT systems



For Vendor Systems

1. Hold vendors accountable. Consider doing so in contracts that require them to follow compliance standards like SOC2 compliance and other NIST policies
 - These standards are focused around protecting user data and ensuring companies are using those best practices.
2. Ask or require vendors to follow role-based access standards and utilization of privileged access management tool.
 - As mentioned, these tools will monitor who has access to what systems and track the changes made by those individuals. Unwanted changes can be reversed.
3. Manage and control network and user access to these systems through security tools like network firewalls for inspecting traffic and detecting threats. Also consider enabling limited access by identification of users with Zero Trust policies
 - This is taking recommendations about the user and matching it to the vendor systems for allowing only approved access on encrypted tunnels that are secure no matter where users are.
4. Require or ask vendors to consider providing any risk assessment reports



Overall Safety Considerations

1. Explore using cybersecurity tools that give organizations insights to risk exposure across public internet and dark web data
 - These tools enable organizations to monitor the use or selling of data on the dark web that may have been obtained illegally even after potentially paying any ransom demands.
2. Network based cameras to monitor physical safety of students. These tools can integrate back into the secure network fabric for monitoring and school safety measures.
3. Ensuring there is sufficient bandwidth to support the various systems and controls.
4. Avoid deploying multiple point solutions that can make controls more complex.
5. With shortage of IT skills sets there are several practices to consider
 1. Integrate and Automate as many processes and systems as possible to avoid human error. This can assist with doing more with less.
 2. Training for various levels of cybersecurity
 - Many free programs are available in the industry for K12 schools



The Broadest, Most Integrated AI-Driven Cybersecurity Platform in Industry

50+ tightly integrated product lines

The Fortinet cybersecurity platform protects the entire attack surface while integrating tightly into your current and future infrastructure

Secure Networking

Network Firewall
Wireless and Wired LAN
5G
OT Security
NAC

300+ Ecosystem Partners

Google Cloud Microsoft

CROWDSTRIKE servicenow

aws

Security Operations

SOC Platform
Endpoint Protection
Network Detection & Response
CNAPP
Data Protection
Identity
Exposure Assessment

Unified SASE

SD-WAN
SSE
Single-Vendor SASE
ZTNA
DEM
Cloud Firewall
WAF





The Broadest Platform in Cybersecurity

Secure Networking

- FortiGate**
NGFW with ASIC acceleration and industry leading Convergence
- FortiSwitch**
Protected Ethernet connectivity via Secure Networking convergence with FortiGate
- FortiAP**
Protected Wi-Fi connectivity via Secure Networking convergence with FortiGate
- FortiManager**
Centralized management of your Fortinet security infrastructure
- FortiNAC**
Visibility, access control and automated responses for all networked devices
- FortiExtender**
Extend scalable and resilient LTE and LAN connectivity
- FortiGate Cloud**
SaaS platform offering zero-touch deployment, network management and security analytics
- FortiEdge Cloud**
Cloud management for standalone LAN, WLAN and 5G gateway equipment
- FortiAIops**
AI based insights for rapid analysis and remediation of network issues
- FortiFone**
Robust IP phones and softclient to stay connected from anywhere
- FortiVoice**
Unified communications with secure voice, chat, conferencing, and fax
- FortiCamera**
Physical security with intelligent motion detection in any light condition
- FortiRecorder**
Secure NVR with smart AI analysis and centralized visibility
- FortiConverter**
Secure and automated firewall migration from a broad spectrum of vendors
- FGaaS**
Hardware as a service for FortiGate

Resources

- Product Matrix**
Specifications for top selling models
- 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
- FortiCare**
Support and mitigation services

Unified SASE

SASE

- FortiGate SD-WAN**
Application-centric, scalable, and Secure SD-WAN with NGFW
- FortiClient EPP Agent**
Endpoint Protection Agent with AV, URL and Sand-box
- FortiClient ZTA Agent**
Remote access, application access, and risk reduction
- FortiSASE**
Cloud-delivered Security Services Edge
- FortiProxy**
Enforce internet compliance and granular application control
- FortiMonitor**
SaaS based DEM platform, performance monitoring
- FortiCASB**
Prevent misconfigurations of SaaS apps and meet compliance

CLOUD

- FortiGate VM**
NGFW w/ SOC acceleration and industry-leading secure SD-WAN
- FortiGate CNF**
Hosted cloud-native firewall for simplified cloud network security
- FortiWeb**
Prevent web application attacks against critical web assets
- FortiADC**
Application-aware intelligence for distribution of application traffic
- FortiGSLB**
Ensure business continuity during unexpected network downtime
- FortiDDoS**
Machine-learning quickly inspects traffic at layers 3, 4, and 7
- FortiFlex**
Flexible daily usage-based consumption licensing for a broad catalog of solution
- FortiPoints**
Simplified, flexible licensing for annual contracts, renewals, upgrades, and co-terms

AI-Powered FortiGuard Security

- WF** Web Filtering
- IPS** IPS
- AV** AV
- SBX** Sandbox
- IL MPS** IL MPS
- APP CTRL** Application Control
- ATTK SIFFC** Attack Surface
- DLP** DLP
- OT** OT Security Services
- IoC** IoC
- IL CASB** IL CASB

Security Operations

- FortiAnalyzer**
Security Fabric log management, monitoring and response
- FortiMail**
AI-powered, protection against email-borne threats
- FortiSIEM**
Enterprise-wide monitoring, threat detection, and response
- FortiSandbox**
AI-powered real-time protection against unknown and 0-day threats
- FortiEDR/XDR**
Automated endpoint protection and correlated incident response
- FortiToken**
Cloud/HW/Mobile MFA provide passwordless adaptive authentication
- FortiSOAR**
Automated security operations, investigation, and response
- FortiAuthenticator**
Centralized identity and access management solution
- FortiNDR**
AI-driven analysis to detect and respond to threats
- FortiGuard MDR Service**
Managed threat detection, investigation, and response
- SOaaS**
Continuous security monitoring, incident triage, and escalation
- FortiRecon**
Proactive digital risk protection service and external/internal threat monitoring
- IR Services**
Rapid detection, containment, and recovery of cyberattacks
- FortiPAM**
Privileged identity and access management, and session monitoring
- FortiDeceptor**
Active deception platform for early in-network attack detection and response
- FortiTester**
Network performance testing and breach attack simulation (BAS)
- FortiTrust Identity**
Identity and Access Management as a Service (IDaaS)
- FortiDevSec**
Orchestrated and automated continuous application security testing
- FortiGuest**
Access management solution for temporary access to guests and visitors
- FortiDAST**
Automated black-box dynamic application security testing
- FortiCNAPP**
Secure code to cloud with a single, data-driven platform
- FortiScanner Cloud**
Cyber Asset Attack Surface Management Service
- FortiNextDLP**
Endpoint DLP and Insider Risk management
- FortiAI**
Integrated GenAI Assist for SOC and NOC

OT Security Platform

- OT Security Service**
FortiGuard subscription for FortiGate NGFW enables protection against OT-specific threats
- Ruggedized Products**
Rugged NGFW, switch, AP, and 5G extenders provide secure connectivity in harsh outdoor environments
- FortiSRA**
Agentless secure remote access offers robust remote access control, management, session logging, monitoring, and recording
- SecOps for OT**
Advanced cybersecurity controls bring OT networks into the SOC and incident response plans

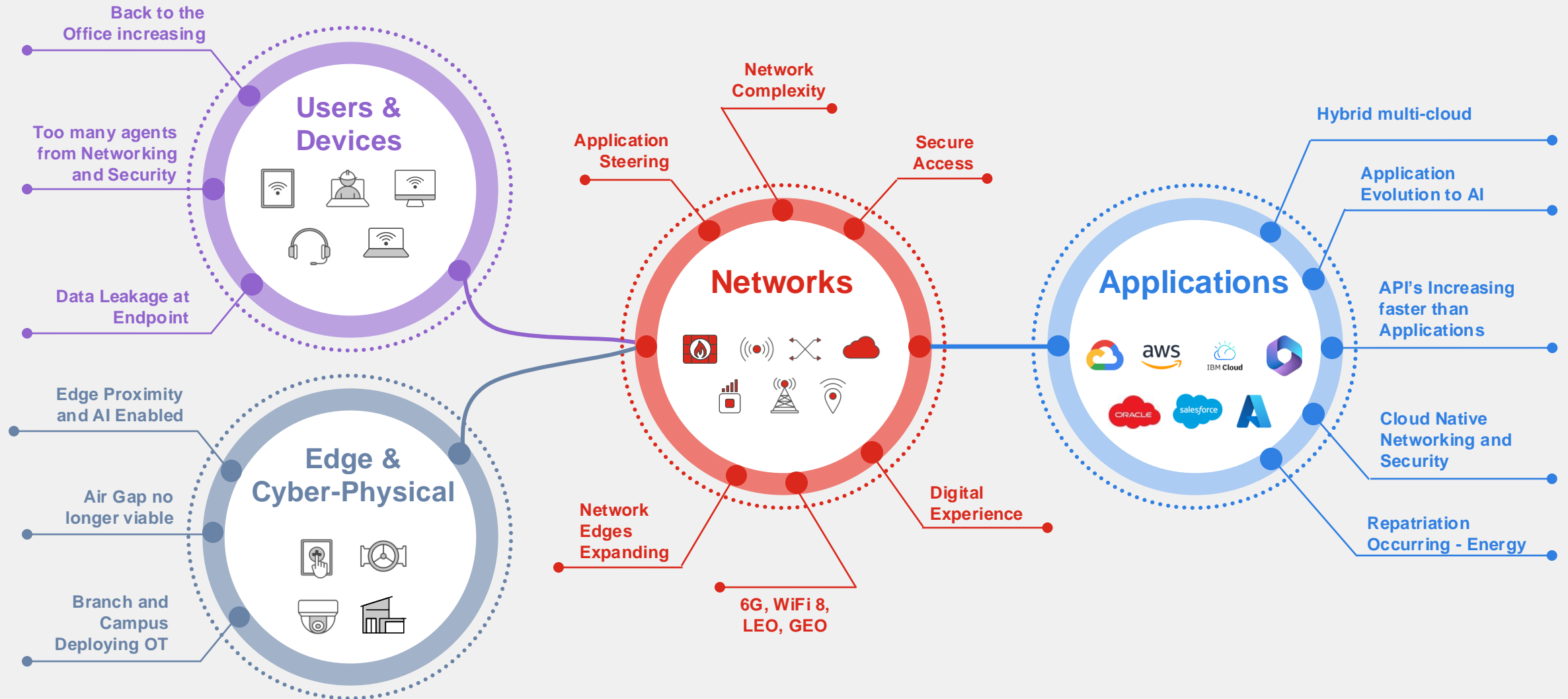
Open Ecosystem

- FNDN**
Advanced tools for Fortinet community to develop custom solutions
- Fabric Connectors**
Fortinet-developed integrations for automation and security
- Fabric API**
Partner-developed integrations for end-to-end visibility and protection
- DevOps Tools**
Community-driven scripts automate network/security tasks
- Extended Ecosystem**
Integrates with third-party systems and orgs for sharing threat-intel



Digital Networking & Infrastructure Evolution Accelerating

The attack surface continues to expand

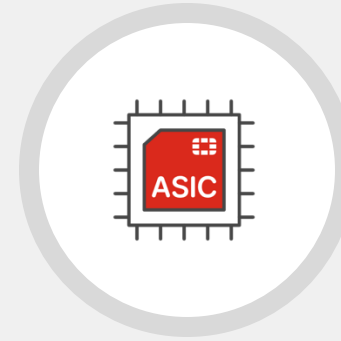


Delivering Unrivaled Security and Performance Through Innovation

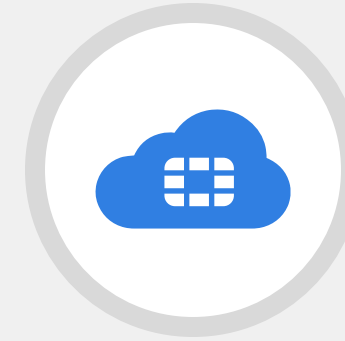
Fortinet's competitive differentiation lies in our core technologies, which together provide unprecedented performance, unrivaled security, maximum flexibility, and seamless integration across diverse environments.



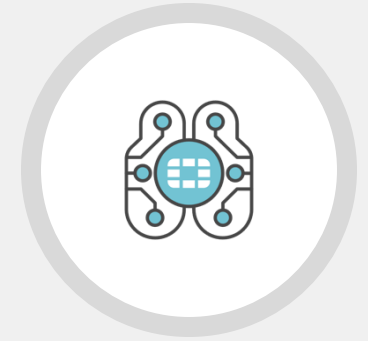
FortiOS
NETWORKING SECURITY
OPERATING SYSTEM



FortiASIC
ASIC
POWERED



FortiCloud
CLOUD
INFRASTRUCTURE



FortiAI
AI/ML THREAT INTELLIGENCE
& GENERATIVE AI



FortiClient
UNIFIED
CLIENT



OT Security
DEDICATED OT
SOLUTIONS



Ecosystem
EXTENSIVE PARTNER
ECOSYSTEM





The **Most Trusted** US-based Cybersecurity Company

Fortinet is ranked #7 in the Forbes Most Trusted Companies



Fortinet Secures **Over 805,000** Organizations Worldwide

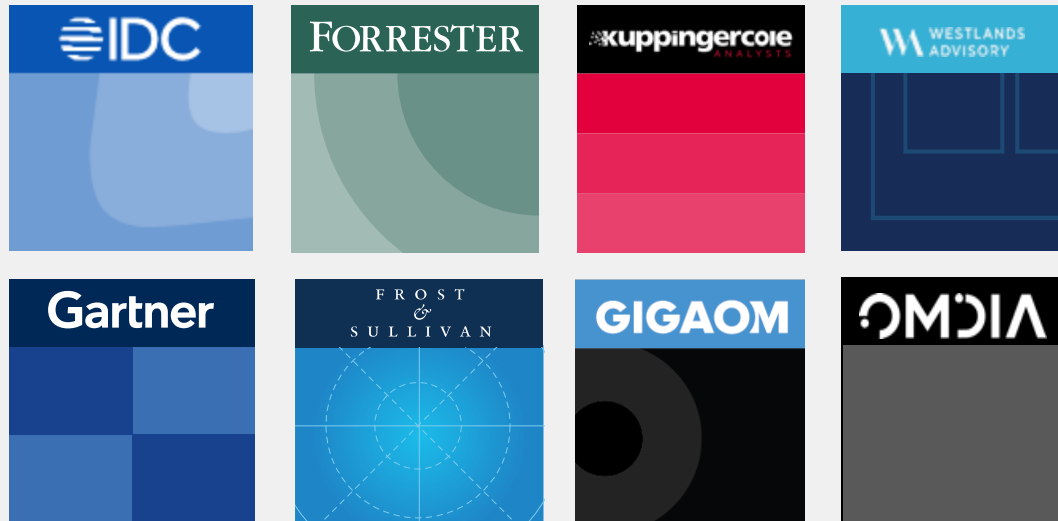
77% of the Fortune 100 and **71%** of the Global 2000 depend on Fortinet to stay secure



130+

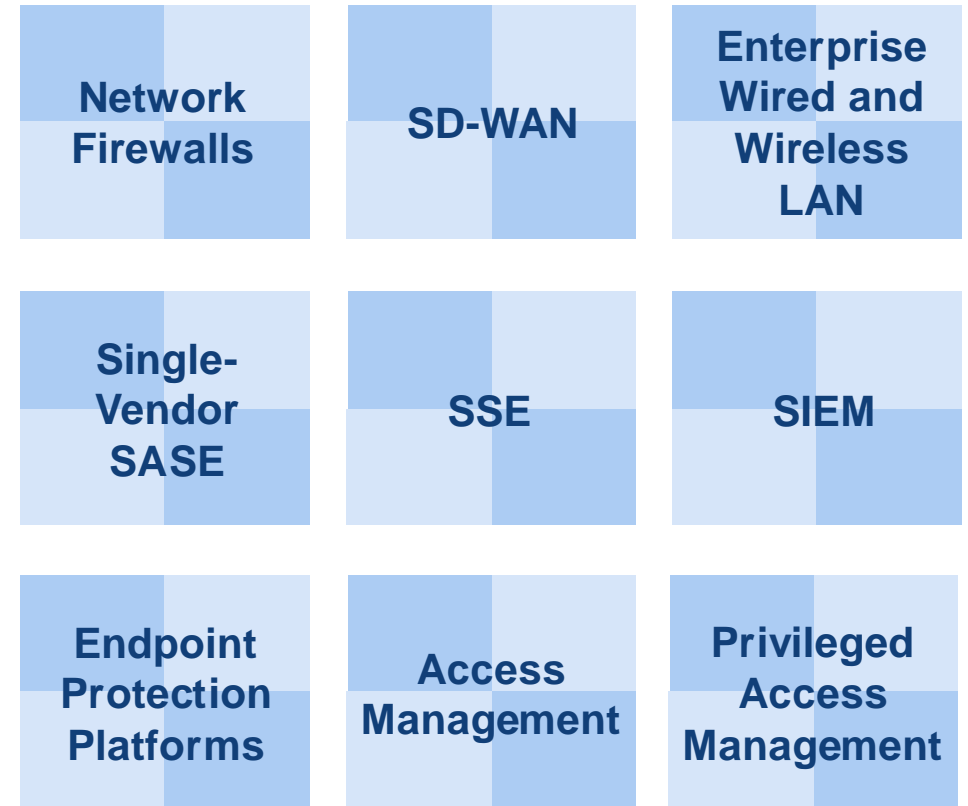
Industry Analyst Research Validates Fortinet Across Networking & Security

Fortinet is one of the most validated cybersecurity companies in the world. Fortinet is continually positioned in a leadership position across more than 100+ research reports from the major industry analyst firms like Gartner, IDC and Forrester, and is recognized in **9** Gartner Magic Quadrants.



Gartner®

 Magic Quadrant



Magic Quadrant for Endpoint Protection Platforms - Published 31 December 2023 - G00789052
Magic Quadrant for Security Information and Event Management - Published 10 October 2022 - ID G00755317
Magic Quadrant for SD-WAN - Published 27 September 2023 - ID G00778908
Magic Quadrant for Enterprise Wired and Wireless LAN Infrastructure - Published 06 March 2024 - G00785075
Magic Quadrant for Network Firewalls - Published 19 December 2022 - ID G00761497
Magic Quadrant for Security Service Edge - Published 10 April 2023 - ID G00766751
Magic Quadrant for Access Management - Published 16 November 2023 G 00781727
Magic Quadrant for Single-Vendor SASE - Published 16 August 2023 - ID G00785023

Global Reach & Support

Majority of our R&D is based in North America

13,900+
Employees
Worldwide

150+
Global Cloud
Locations



Fortinet AI Innovations

Contextual Gen AI

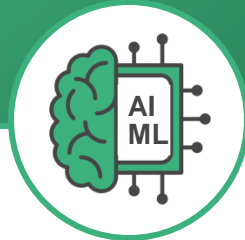


Generative AI to improve product optimization



Security Analytics

Big Data AI



Process and analyze trillions of events using AI/ML



Threat Intelligence

Network Operations AI

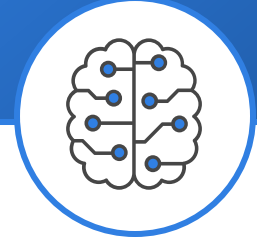


Self-healing networks end-to-end



AI for Networking

AI for LLM Leakage



Protection against data leakage into LLM



AI for Data Security

Leading Innovator with Large Investment in Innovation

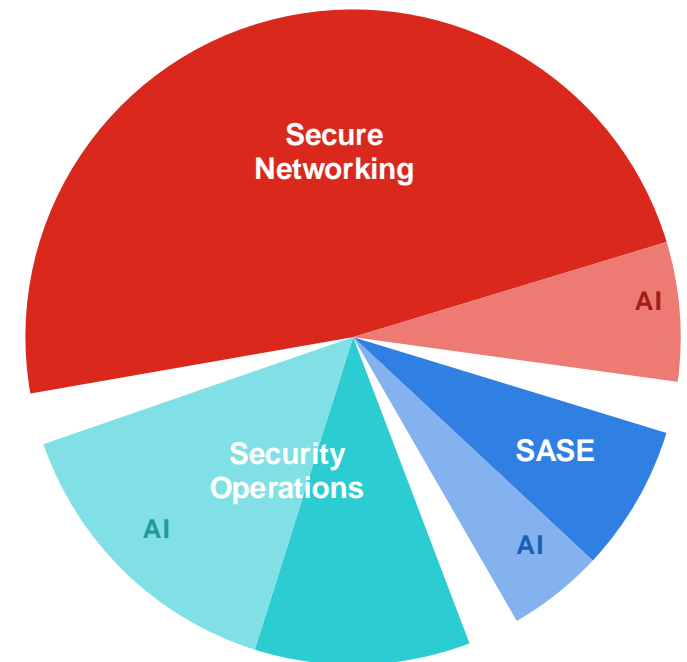
With 2x more patents than comparable cybersecurity companies

US Patents



Source: U.S. Patent Office, as of September 30, 2024

Innovation Across Pillars



Fortinet Contributes to the Sustainability of Society

Addressing Cybersecurity Risk to Society



Global Partnerships and Collaboration



Respecting the Environment



Pledge
NET ZERO

by 2030
Fortinet owned facilities

88%
less power consumption over industry-standard CPUs

by 2050
across value chain



Closing the Cybersecurity Skills Gap



Pledge
1 Million
people trained in cybersecurity by
2026



600+
schools across 98 countries

Promoting Responsible Business



100%

of our key contract manufacturers trained on our compliance and ethics standards

FORTINET
Trusted Resource Center





Market Trends & Vision



More External Forces Than Ever Are Driving Security Decisions



DIGITAL EVOLUTION

Digital innovation is creating tremendous opportunity, but more risk



TECHNOLOGY DISRUPTION

More companies are rapidly implementing AI to transform business operations



ECONOMIC HEADWINDS

Budget changes and skills shortage are resulting in more delays and more risk



SKILLS SHORTAGE

With 4.8M unfilled jobs, the struggle to recruit and retain cybersecurity talent creates additional cyber risks



ENVIRONMENTAL, SOCIAL, & GOVERNANCE

Consumers and boards are putting more pressure to deliver on ESG initiatives



REGULATORY AND COMPLIANCE

Companies are reacting to more frequent reporting and regulatory changes

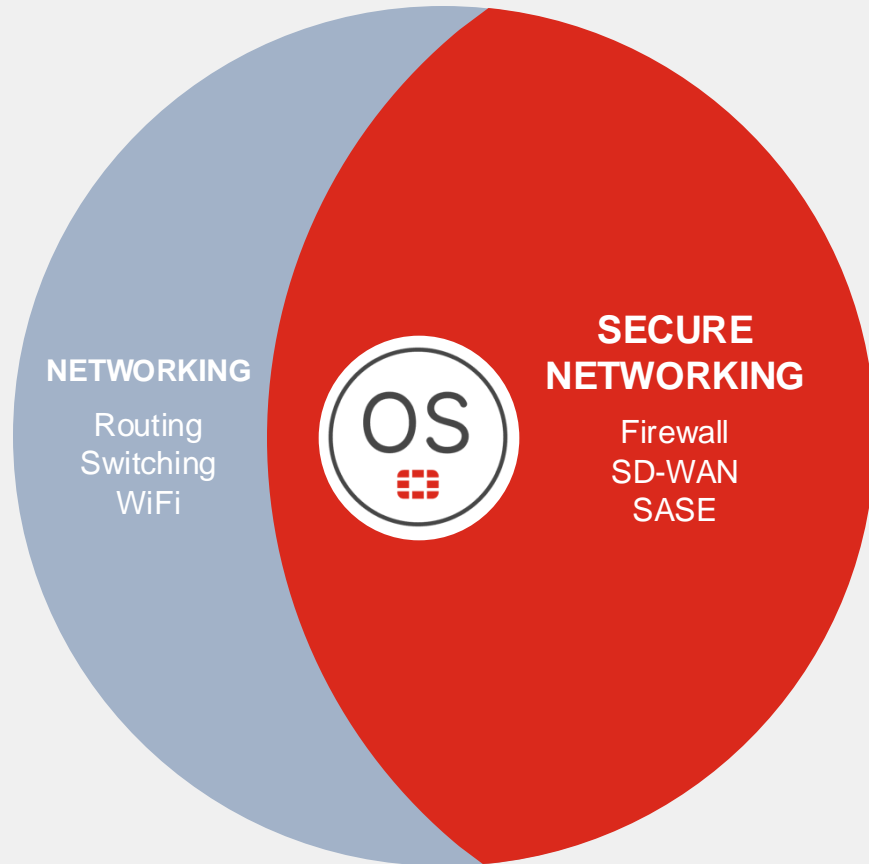


THREAT LANDSCAPE

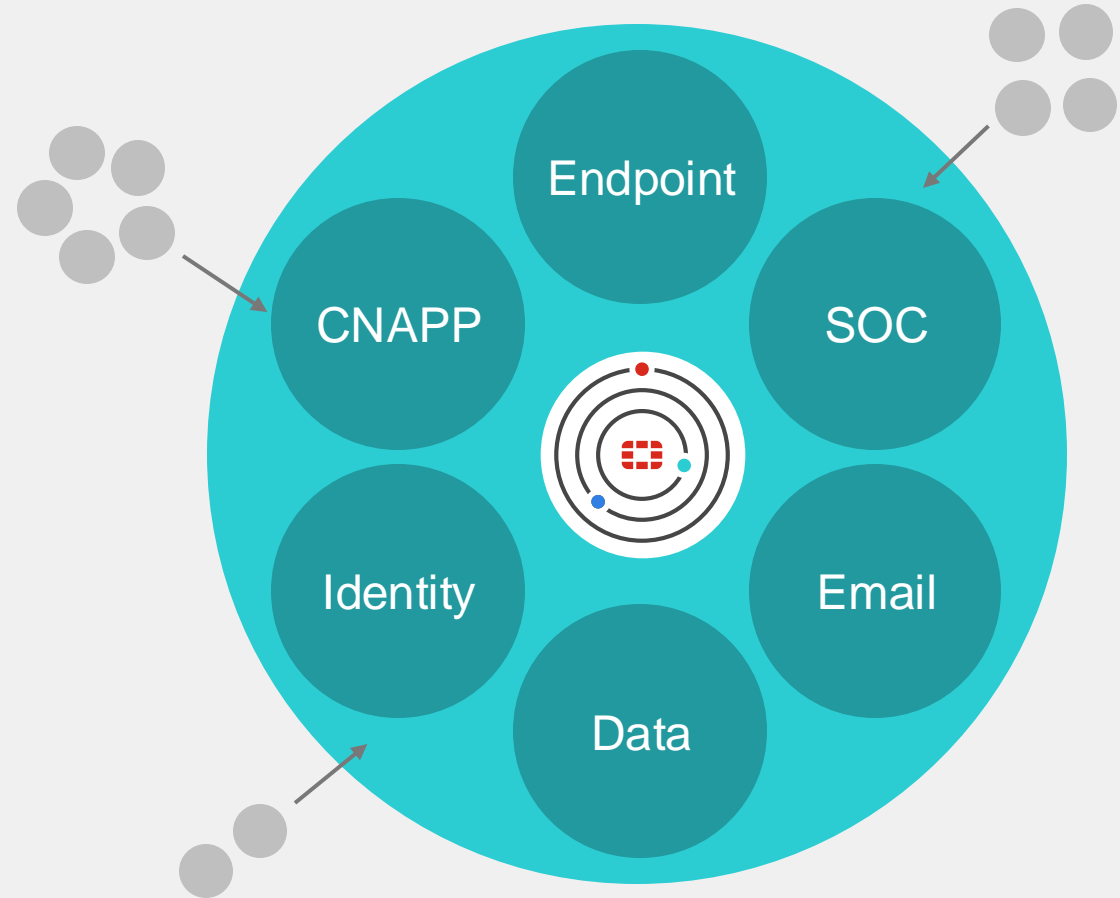
Attacks are growing in sophistication and frequency

Long-lived Exploits
Industrial Ransomware
Supply Chain Attacks
Cloud Risks
APT Threat Actors
New Vulnerabilities
Targeted Attacks On The Rise
Insider Risk

A Unified and Converged Vision For Networking and Security



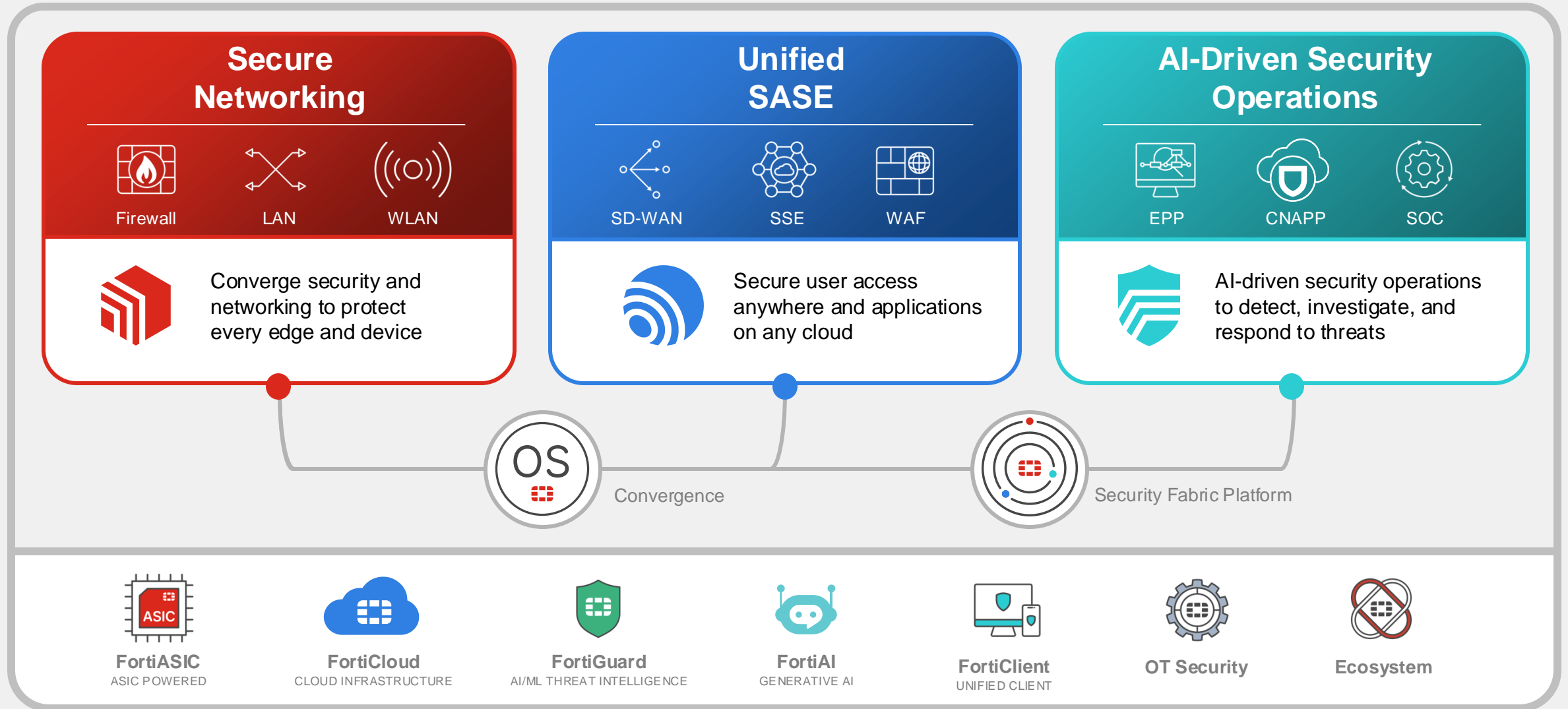
Convergence



Platform



The Most Comprehensive & Advanced Cybersecurity Platform



Fortinet Fabric Portfolio

Secure Networking

Network Security	Enterprise Networking
<ul style="list-style-type: none"> FortiGate Firewall FortiGate VM Virtual Firewall FortiCNF Cloud-native Firewall FGaaS Firewall-aaS FortiGate Rugged NGFW 	<ul style="list-style-type: none"> FortiSwitch Switching FortiAIops AI For Networking FortiAP Access Point FortiNAC NAC FortiSwitch Rugged Switch FortiExtender LTE/5G FortiAP Rugged AP FortiExtender Rugged Extender
<p>FortiManager Centralized Management</p>	

Unified SASE

Secure Access	Cloud Security
<ul style="list-style-type: none"> FortiSASE SSE FortiGate SD-WAN FortiClient ZTNA FortiProxy SWG FortiMonitor DEM FortiCASB CASB 	<ul style="list-style-type: none"> FortiGate VM Virtual Firewall FortiWeb (WAAP) FortiGate CNF Cloud-native Firewall FortiADC Application Delivery

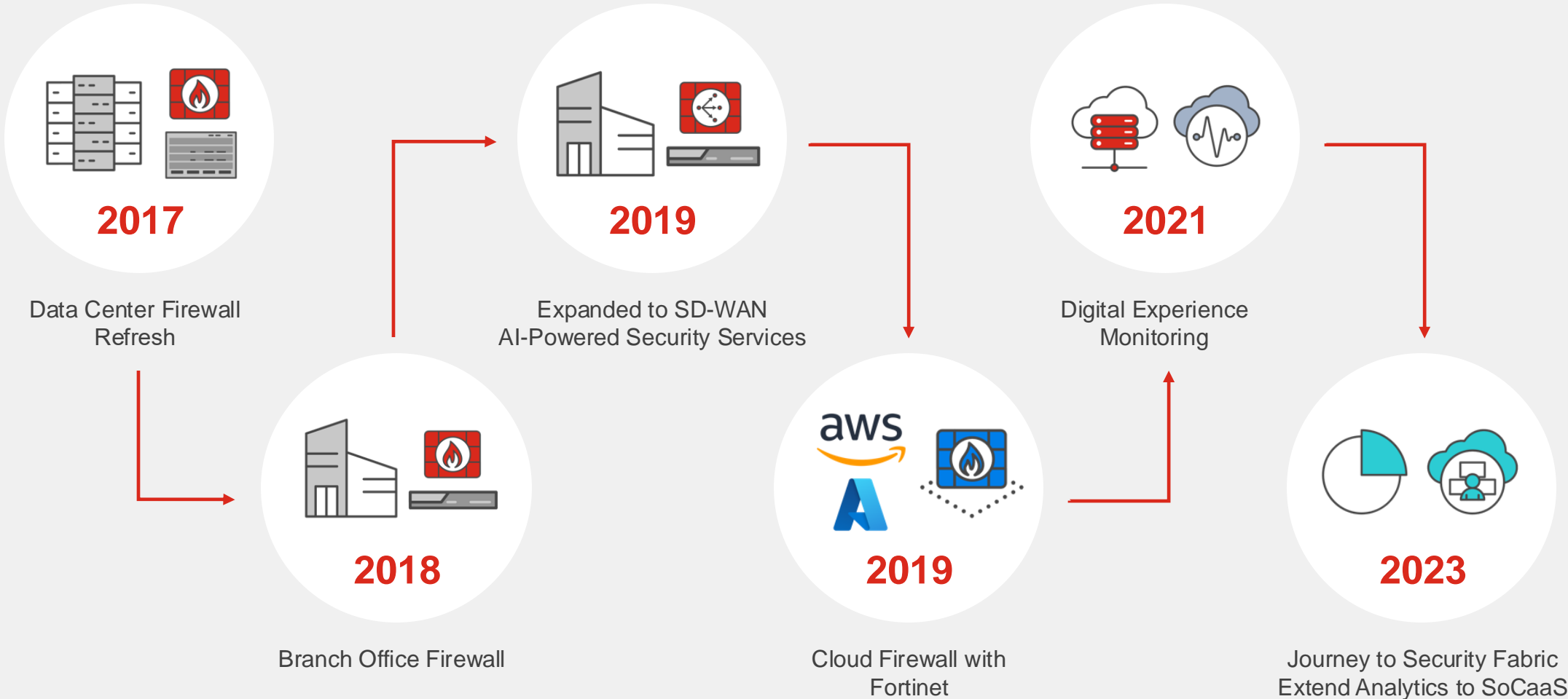
Security Operations

<ul style="list-style-type: none"> Lacework FortiCNAPP FortiEDR/XDR EDR/XDR FortiDeceptor Deception FortiRecon DRPS FortiAuthenticator Cloud FortiToken MFA 	<ul style="list-style-type: none"> FortiNDR NDR FortiSIEM SIEM FortiSOAR SOAR FortiSandbox Sandbox FortiPAM PAM FortiDLP DLP 	<ul style="list-style-type: none"> FortiAnalyzer Analytics SO CaaS MDR Service IR Service FortiMail SEG FortiTrust Identity
---	--	---



It's a Journey – Fortune 50 Customer Expands into Integrated Secure Solutions

FortiOS and The Security Fabric deliver new capabilities across the network and SOC






Solutions

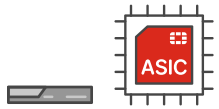


Fortinet's Network Firewall Solution

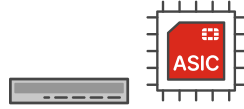
Management & Analytics

 FortiAnalyzer
  FortiAI
  FortiManager

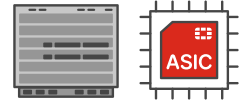
Branch


FortiGate 40-90 Series




Campus


FortiGate 100-900 Series















Data Center



FortiGate 1000-7000 Series

VM / Cloud / FWaaS





 FortiGate VM
  FortiCNF
  FGaaS

Networking Operating System Everywhere

 OS
  Firewall
  VPN
  NGFW
  Segmentation
  Distributed NGFW
  DDoS
  Low Latency
  Integrated W/LAN
  5G/LTE
  HW SSL Inspection
  Secure SD-WAN
  Hyperscale
  ZTNA


FortiGuard Labs AI-Powered Threat Intelligence

Network and File Security

 SBX
  AV
  APP CTRL
  IPS




Detect Malicious Files SSL Inspection

Zero-Day Prevention

 IL MPS





Inline Malware prevention

Web Security

 URL
  DNS
  BOT

Stop DNS and Bot Attacks
Block Malicious URLs

SaaS & Data Security

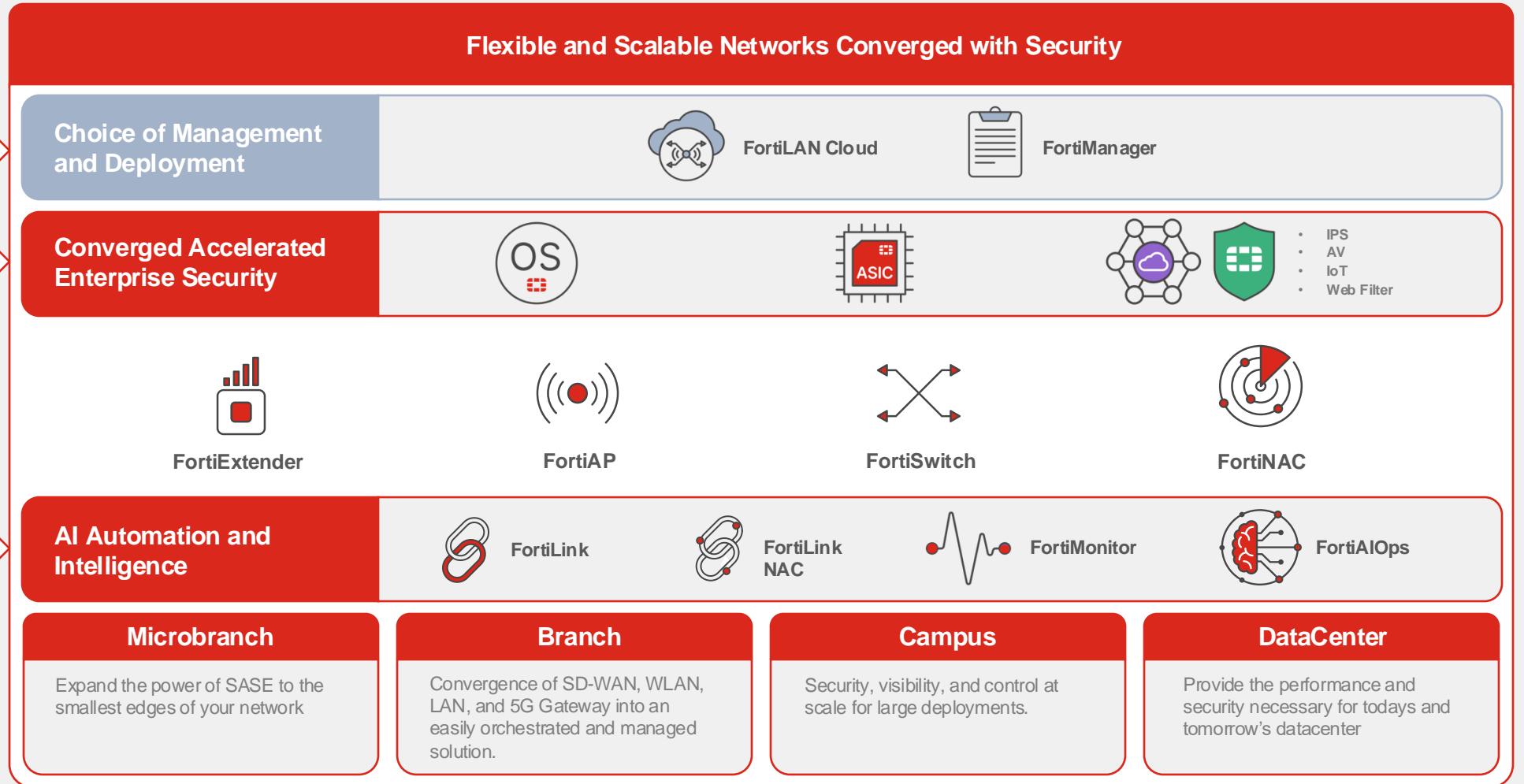
 DLP
  ANTI-SPAM
  IL CASB
  ATTK SRFC

Stop Data Exfiltration Spam & SaaS Threat Protection IoT Security & Security Best Practices



Fortinet's Secure LAN Edge Solution

The power of convergence with a single platform



Flexible
Can be managed via cloud, virtual machine, or appliance

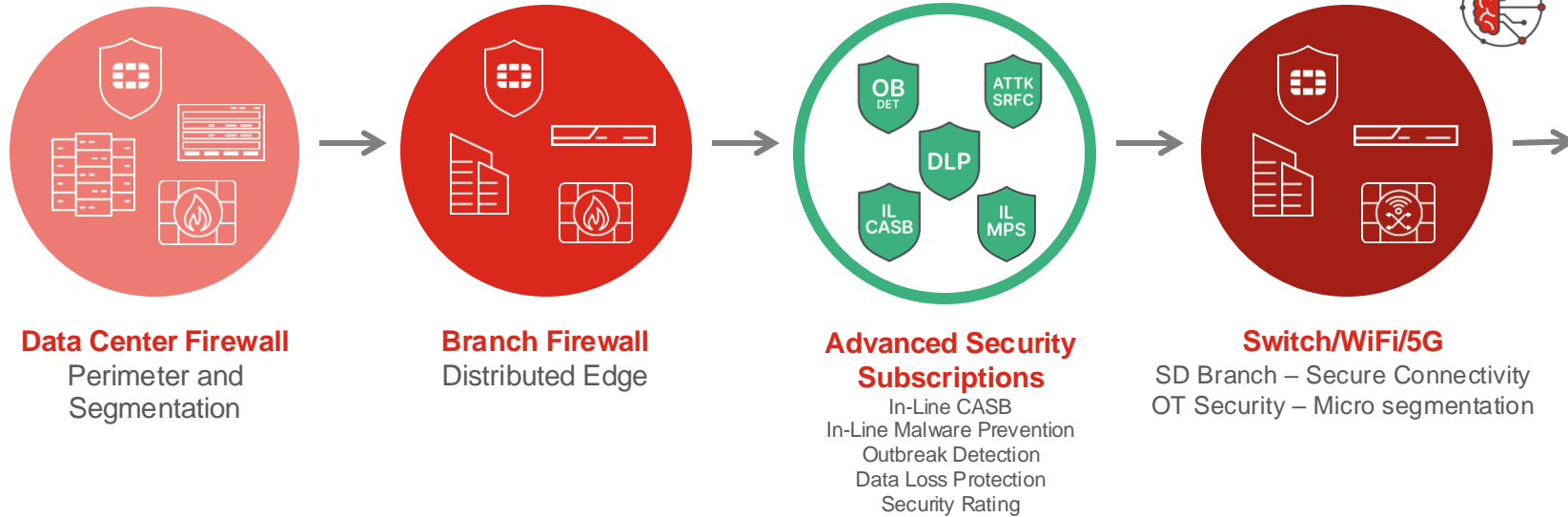
NGFW Security & Control
Best of Breed Security extended to the LAN

Full Visibility with Control
NAC functions with policy enforcement built in



Accelerating Secure Networking Market Leadership

Typical Customer Journey



Analyst Recognition

Gartner

Gartner	Gartner
Leader in Magic Quadrant for Network Firewalls	Leader in Magic Quadrant for Enterprise Wired and Wireless LAN

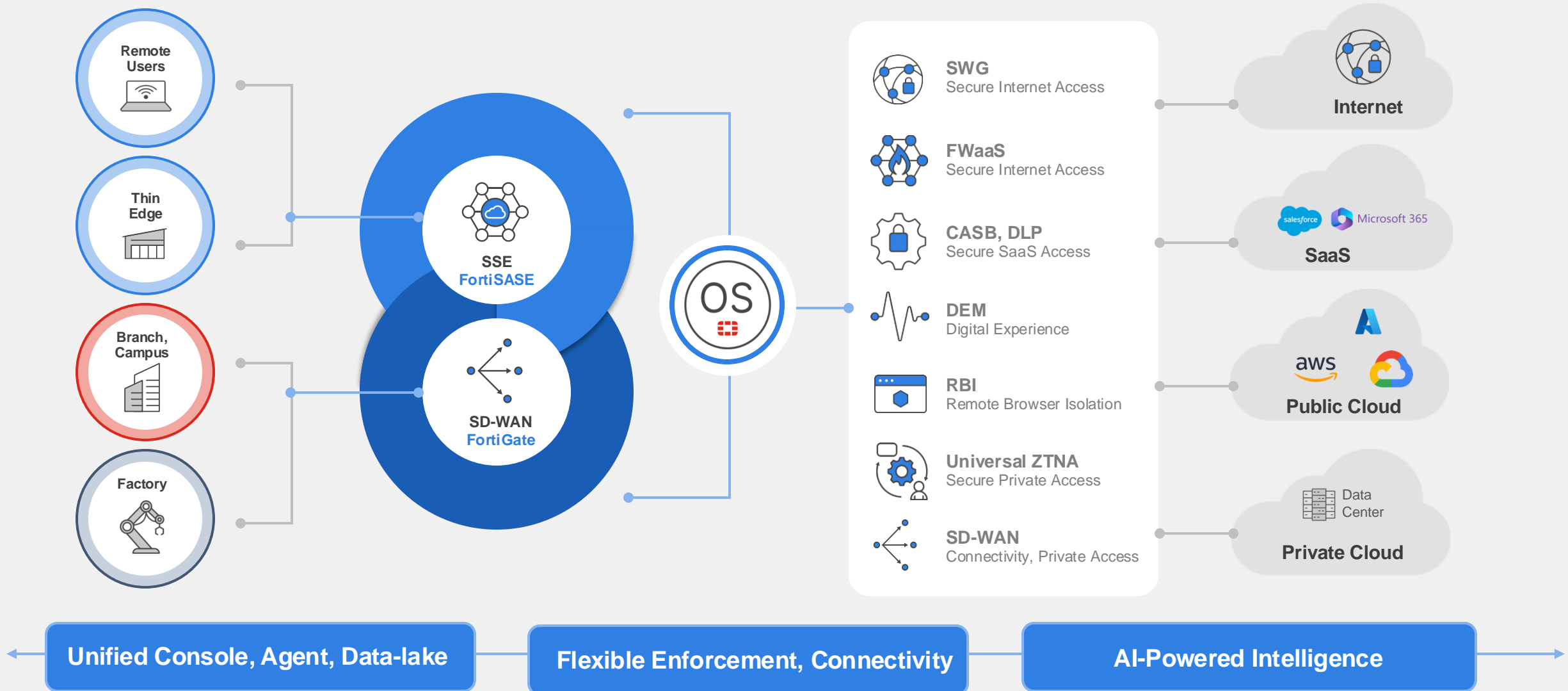
650 GROUP
MARKET INTELLIGENCE RESEARCH

50%+

Firewall Unit Market Share

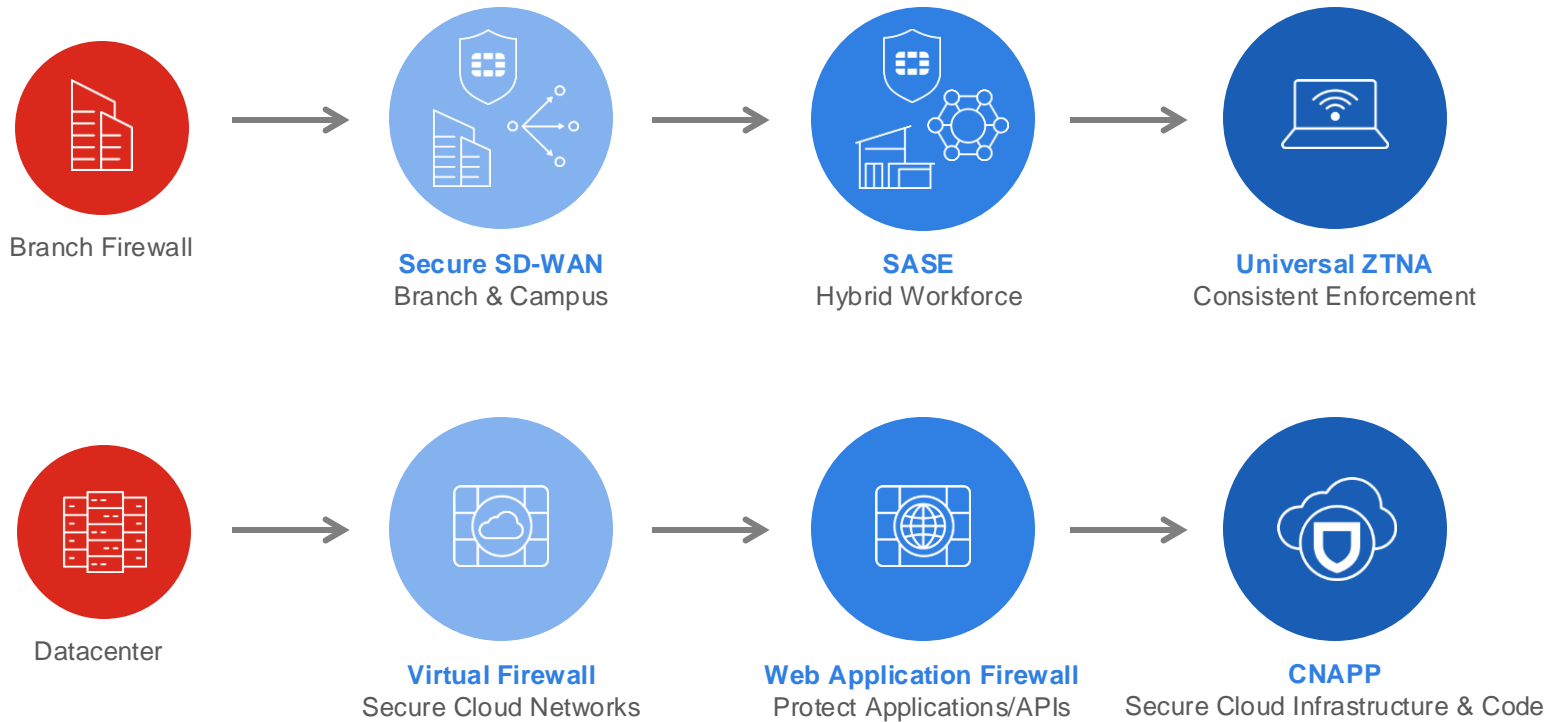


Fortinet's Unified SASE Solution for Secure Access



Triple Digit SASE Growth with Large Increasing Pipeline

Typical Customer Journey



Analyst Recognition



AI-driven Security Operations Solutions



Lacework FortiCNAPP Core Capabilities

A unified platform for code-to-cloud security



DEPLOY

- Scan code and APIs in development
- Address vulnerabilities, malware and misconfigurations
- Prioritize risks with attack path analysis

CODE SECURITY

SCA

Software Composition Analysis

SAST

Static Application Security Testing

IaC

Infrastructure as Code Security

RUN

- Assess cloud infrastructure configuration
- Evaluate identities and their permissions
- Prevent deployment of non-compliant applications

CLOUD CONFIGURATION

VA

Vulnerability Assessment

CSPM

Security Posture Mgmt

CIEM

Cloud Infrastructure Entitlement Mgmt

CODE

- Continuously monitor for exposures and sensitive data
- Detect unusual behavior and active threats
- Understand running processes and map network connections

RUNTIME PROTECTION

CWP

Cloud Workload Protection

CDR

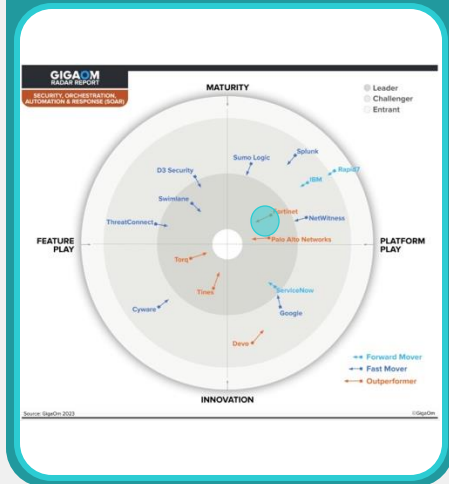
Cloud Detection & Response



The Value of Fortinet Security Fabric Integrations in Various Security Markets

LEADER

SOAR



Fortinet named a leader and outperformer in the GigaOm Radar for SOAR, 2023

LEADER

Cloud Workload Security



Fortinet named a leader in the 2024 GigaOm Radar for Cloud Workload Security (CWS)

STRONG PERFORMER

NETWORK ANALYSIS AND VISIBILITY



Fortinet named a strong performer in the 2023 Forrester WAVE for Network Analysis and Visibility

CHALLENGER

SIEM



Fortinet named a challenger in the 2024 Gartner MQ for Security Information and Event Management (SIEM)

NICHE

EPP



Fortinet named a niche in the 2023 Gartner MQ for Endpoint Protection Platform (EPP)

FORTINET SECURITY FABRIC INTEGRATIONS

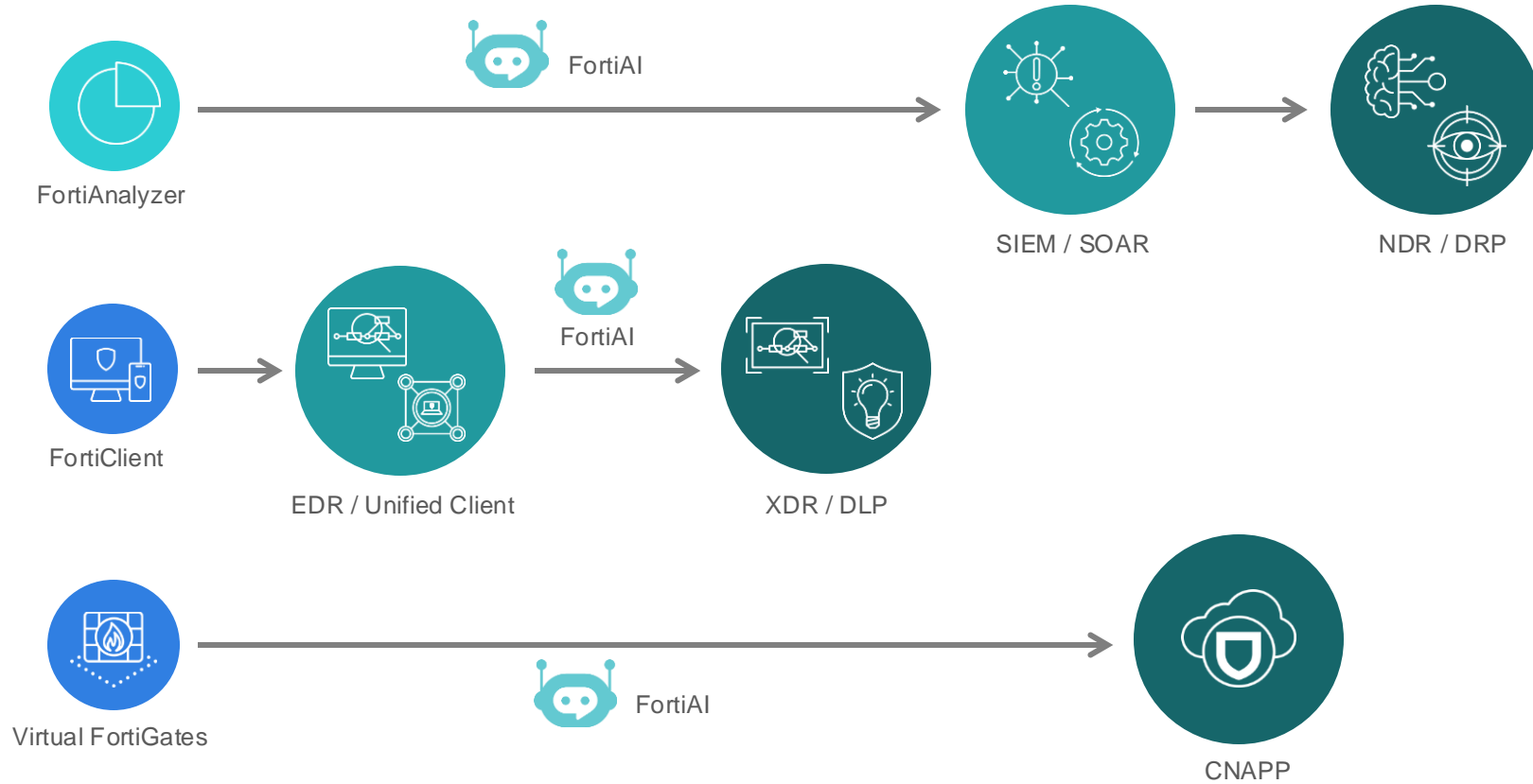


Gartner does not endorse any vendor, product or service depicted in its research publications and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

GARTNER is a registered trademark and service mark, Magic Quadrant is a registered trademark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and are used herein with permission. All rights reserved.

Most Comprehensive Security Operations Portfolio

Typical Customer Journey



Analyst Recognition



The image features the Fortinet logo centered on a black background. The logo consists of the word "FORTINET" in a bold, white, sans-serif font. The letter "O" is stylized with a red and white grid pattern. Surrounding the logo are several decorative elements: a red horizontal bar in the top left, a red horizontal bar in the top right, a red horizontal bar in the bottom left, a red horizontal bar in the middle right, a grid of small white dots in the bottom right, and various dark gray geometric shapes (squares and semi-circles) scattered across the background.

FORTINET