

The Fortinet logo consists of the word "FORTINET" in a bold, black, sans-serif font. The letter "O" is replaced by a red square containing a white grid of dots, which is a stylized representation of a network or fabric. A registered trademark symbol (®) is located to the upper right of the word.

FORTINET®

Security Under One Fabric

November 9th, 2023



Trends and Market Drivers



Cybersecurity Market & Industry Drivers

Driving Infrastructure Evolution

How we interact with customers, suppliers, infrastructure, and employees is changing

Work from Anywhere



Digital Acceleration



Application Journey



Operational Technology Connectivity



Evolving Threat Landscape

Cybercriminals are adopting APT-like tactics to develop and scale attacks faster than ever

Cloud



Kaseya
VSA

Nation Sponsored



Hermetic
Wiper

Ransom as a Service



REvil

Growing Attack Surface



SolarWinds | Log4j

AI-enabled



Swarmbot

OT



Wipers | Colonial Pipeline



© Fortinet Inc. All Rights Reserved. | 3

- Securing and connecting work-from-anywhere users.
- Enabling digital acceleration.
- Managing applications moving to the edge or to the cloud.
- Securing OT environments, which are converging with IT networks.

Meanwhile the threat landscape continues to evolve and cyber risk is escalating for all organizations. As cybercrime converges with advanced persistent threat methods, cybercriminals are finding ways to weaponize new technologies at scale to enable more disruption and destruction. At the same time, they are spending more time on reconnaissance to attempt to evade detection, intelligence, and controls.

All of this means cyber risk continues to escalate and that CISOs need to be just as nimble and methodical as the adversary.

Complexity is Slowing Digital Initiatives



Today's Challenges

- Applications are distributed
- Users are working from anywhere
- More devices are attaching to applications
- Too many IT and security stacks
- Too many vendors
- Cybersecurity skills shortage

© Fortinet Inc. All Rights Reserved. | 4

Today, complexity is slowing down digital initiatives.

- Applications are distributed in the cloud, in the data center, and as a service.
- Users are working from anywhere, whether from home, the office, or on the road for travel.
- More devices than ever are attaching to applications.

In response, most organizations add new networking or security point solutions, leading to too many IT and security stacks, too many vendors, and too many products that operate in a silo with their own policies and their own management consoles.

This operational complexity is the number one challenge teams can start solving right now to take back control of their environments.

Security Architecture

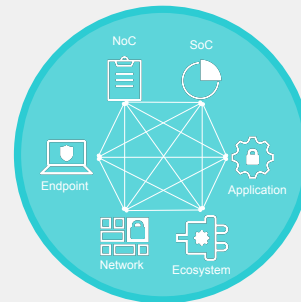
Best-of-Breed vs. Security Platform

Best-of-Breed Approach



30+ Vendors

Security Platform Approach



2-3 Platforms



© Fortinet Inc. All Rights Reserved. | 5

In the debate over adopting an all-in-one cybersecurity platform versus assembling best-of-breed solutions, there's only one answer: It depends,

The questions are:

How many tools can you afford, and is the software in your stack designed for security?

Do you have skilled resources to manage?

Does this approach make sense now that we have a greater number of users outside the organization, and services we use are in the cloud?

Security Architecture

Advantages and Disadvantages

Best-of-Breed Disadvantages

Cumbersome - Implementing best-of-breed security technology at every layer becomes cumbersome.

Silos- Integrating multiple vendor security technologies in the detection and response layer is challenging and proven to lack interoperability and integration.

Complexity – A patchwork of products increases complexity and increases the trained resources required to manage security operations.

Cost - Adding best-of-breed security technology at every problem increases cost and makes management challenging.

Platform Approach Advantages

Reduced complexity –Detection, response and management of vulnerabilities, misconfigurations etc can be performed efficiently and effectively.

Simplified management - easier to monitor, manage, update systems and easier for security teams to analyze exposures, track status and measure performance.

Integration of tools - Security gaps are reduced, data exchange between different tools is eased and the overall security of the entire organization is improved.

Cost: A platform solution allows for cost saving from a product and vendor reduction.



© Fortinet Inc. All Rights Reserved. | 6

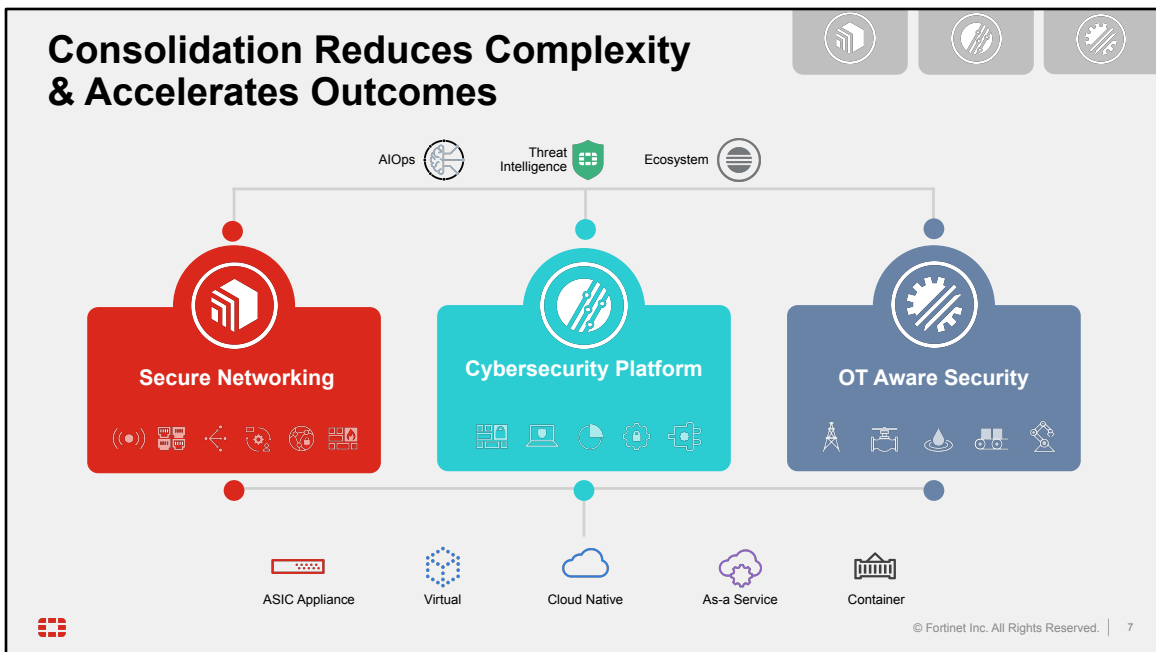
In the debate over adopting an all-in-one cybersecurity platform versus assembling best-of-breed solutions, there's only one answer: It depends,

The questions are:

How many tools can you afford, and is the software in your stack designed for security?

Do you have skilled resources to manage?

Does this approach make sense now that we have a greater number of users outside the organization, and services we use are in the cloud?



Fortinet's answer is to support our customers with convergence and consolidation into a platform approach.

By focusing on consolidating vendors and point products – across both security and networking – you can reduce complexity to close security gaps, improve operational efficiency, optimize user experience, and accelerate outcomes. Three key concepts to achieve consolidation are:

- 1) **Secure Networking:** The convergence of networking and security into a secure networking solution
- 2) **Cybersecurity Platform:** Consolidating point products into an integrated cybersecurity platform
- 3) **OT-Aware Security:** Leveraging security that is purpose-built for operational technology environments

For Fortinet, all three of these areas include AIOps, Threat Intelligence, and an open ecosystem, and consist of solutions and products that can be deployed either as an appliance, as a virtual machine, as native cloud, as a service or containerized.

Consolidation Reduces Complexity & Accelerates Outcomes



And here you'll see the goals of leveraging these three forms of consolidation.

With Secure Networking, you're able to improve the digital experience.

With a Cybersecurity Platform, you're able to manage digital risk.

And with OT-Aware Security, you're able to manage cyber-physical risk.

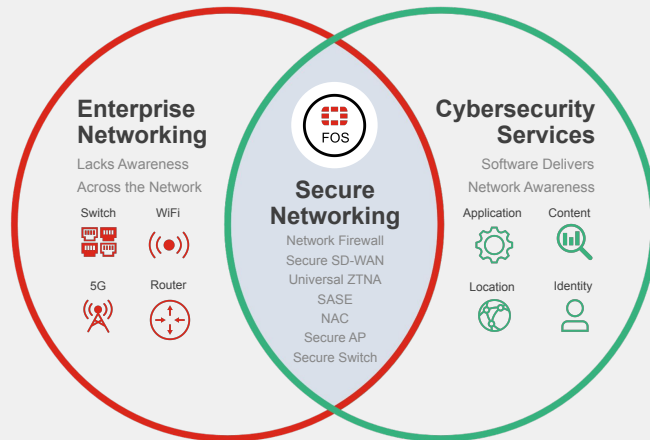
And below each of these sections are the technologies to achieve these goals.

Convergence of Networking & Security

Secure
Networking



FortiOS Everywhere



Convergence Benefits

- Reduced complexity eliminating multiple products
- Efficient operations with single console
- End-to-end digital experience measurement
- Cost savings from product and vendor reduction



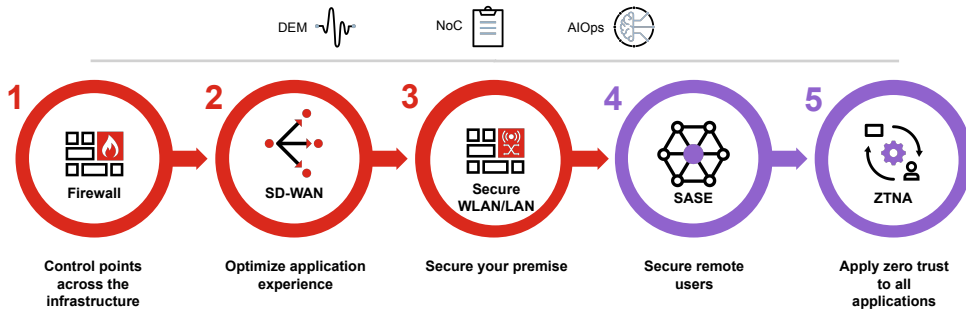
© Fortinet Inc. All Rights Reserved. | 9

Fortinet was founded on this concept 22 years ago, and we're starting to see more and more areas converge. The next-generation firewall was a key example, but we're also seeing SASE, which converges cloud-delivered security and networking, as well as Secure SD-WAN, ZTNA, NAC, Secure AP and Secure Switches.

Fortinet uniquely converges networking and security features in FortiOS, the industry's most mature and prolific operating system. Delivering convergence via a single operating system enables efficient operations and ensures that user experience and security is consistent no matter where users or applications are distributed.

Secure Networking Journey

The convergence of networking and security across WLAN, LAN, SD-WAN, ZTNA, SASE, and network firewall enables networking that is location, user, device, content, and application aware.

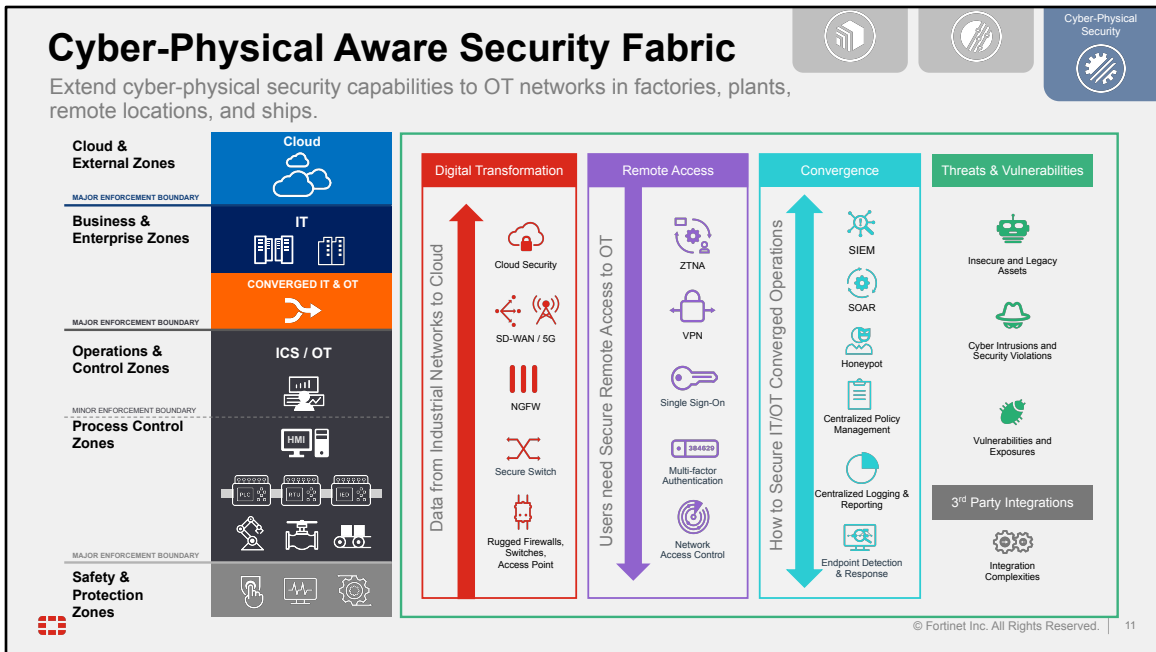


© Fortinet Inc. All Rights Reserved. | 10

This is an overview of our customers' secure networking journey, the goal being to eventually converge networking and security across WLAN, LAN, SD-WAN, ZTNA, SASE, and network firewall to enable networking that is location, user, device, content, and application aware.

Convergence brings together the network and its security infrastructure into a single layer and it is expanding to more areas. Today, convergence is happening with SASE, which converges cloud-delivered security and networking, as well as Secure SD-WAN, zero-trust network access (ZTNA), network access control (NAC), secure access points, and secure switches.

Convergence also is happening in different formats. Now security convergence is happening in appliances, virtual machines, cloud-delivered services, and containers. Convergence through the use of a single operating system facilitates integration and automation, improving operational efficiency and security consistency no matter where users or applications are distributed. Integration between the different security technologies allows them to function collaboratively. And automation leverages the built-in intelligence that integration enables across different solutions to actively detect and respond to threats by coordinating all available resources.



Today, every network is an OT network, which is why deploying a Cyber-Physical Aware Security Fabric is so critical.

The left-hand side overlays the Purdue model across these domains of IT, IT/OT Convergence and OT. The Purdue Model is a well-recognized logical architecture around all the different systems in an OT environment. What I like about it is it's common to different verticals, so whether you're in a manufacturing facility or at an oil and gas facility or up tower at a wind farm or looking at a gas turbine maintenance window, or even in an ICU in a hospital, typically the OT people understand this architecture and can talk about it and it's a common language or nomenclature that most OT people understand.

At the very bottom we have the Safety System which is paramount in OT and at the top the cloud or data center. In between we find different layers of technology including the enterprise network in the IT side, and PLCs, SCADA, and field devices down below.

First: Digital Transformation:

When asset owners connect their industrial control systems to the cloud it is imperative that they protect those environments with next generation firewalls, and we suggest ruggedized switches and access points that can enable secure

connectivity down to the level of those PLCs. SD-WAN enables them to lower connectivity costs and provided enhanced network reliability. Recalling how these networks are brittle to change one way asset owners can enhance the security here is by picking a vendor who through convergence of network and security can enable security directly in the network infrastructure. Look for vendors with standard AND rugged switches and Access Points who can enable security at multiple levels of in the Purdue Model, simplifying operations.

Although the Digital Transformation arrow is pointing up, we may consider that another use case for Digital Transformation is delivering edge analytics from the cloud to the edge of the industrial network and here I would note that the exact same technologies are required to do this with security in mind from the beginning.

2nd: Remote Access:

Another use case driving connectivity is Remote Access for experts who need to access distributed industrial assets. In this case, asset owners want to enable their employees and trusted third parties such as OEMs to remotely access their systems to perform SCADA maintenance and enable remote monitoring and diagnostics of their industrial investment. I want to reiterate this section is much more about remote access for employees AND the supply chain accessing the industrial environment network from far away. In this case, it's critical to provide protected communications leveraging Zero Trust capabilities such as VPN, single sign-on and multifactor authentication.

3rd Convergence

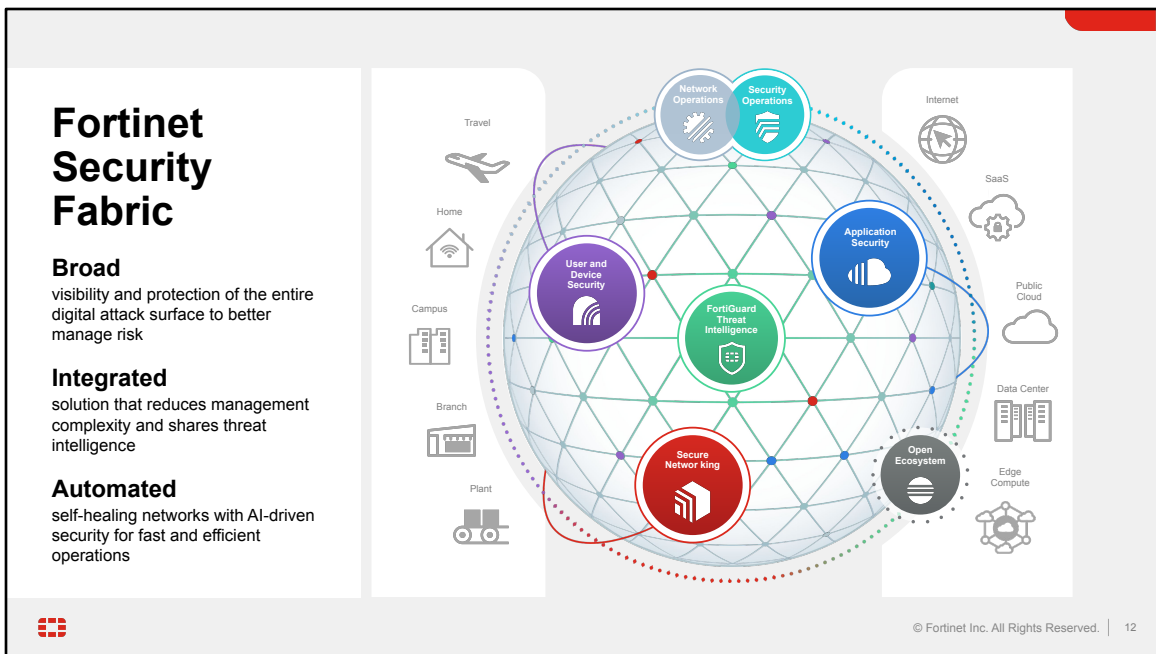
Convergence of IT and OT environments brings some risks, but it also brings some tremendous opportunities for synergistic operations as well. Fortinet's own research has found that top performing asset owners manage their OT security operations in the enterprise SOC. As long as that SOC has trained OT expertise in house this is a great opportunity to ingest data from both IT and OT, to run incident response playbooks across both environments, to deploy deception technology with low impact and low false positives, to manage Firewall and Switch policies, and manage endpoint detection in response across both IT and OT.

4th Threats and Vulnerabilities:

Recall how those OT PLCs are insecure by design; lacking authentication, authorization and encryption and just blindly follow orders? That's why its incredibly important to find a platform offering that includes an OT application protocol control capability so commands you don't want (reset to firmware, e.g.) simply won't be able to traverse the network. Similarly, vulnerabilities in OT environments require OT-specific IPS signatures to limit the risk of exploitation in the ICS environment.

Finally, 3rd party integrations.

No one vendor is solving every use case. In fact, most of the customers we talk to are struggling to manage the dozens of vendors they're using across IT and OT. Look for vendors who focus on integrating a rich ecosystem of partners to simplify the burden of technical debt and interoperability confusion.



This is what it looks like when convergence, platform, and OT-Aware security come together: The Fortinet Security Fabric – Security under one Fabric





Fortinet is committed to delivering convergence in the network, endpoint and cloud, while also supporting the convergence of the NOC and SOC. We connect everything together as part of the Fortinet Security Fabric and apply threat intelligence across while also integrating with an open ecosystem of over 500 solutions from over 350 vendors.

The result:

- **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

Maximize your existing investments

Fortinet integrates with 500+ security and networking solutions

 Fabric Connectors	Fortinet-developed deep integration automating security operations and policies	 Microsoft Azure	 Symantec	 ORACLE	 aws	 nugenetworks	 openstack
 Fabric APIs	Partner-developed integration using Fabric APIs providing broad visibility with end-to-end solutions	 vmware	 servicenow	 Google Cloud	 CISCO	 IBM Cloud	
 Fabric DevOps	Community-driven DevOps scripts automating network and security provisioning, configuration, and orchestration	 aws	 ORACLE	 HashiCorp	 Microsoft Azure	 Alibaba Cloud	
 Extended Ecosystem	Integrations with other vendor technologies & open systems	 Google Cloud	 Red Hat	 refactor	 openstack	 vmware	

Figures as of Dec 1, 2022
Note: Logos are a representative subset of the Security Fabric Ecosystem

© Fortinet Inc. All Rights Reserved. | 15

We also realize you already have existing investments from other vendors. That's why Fortinet's products and solutions integrate with your existing investments thanks to the industry's largest open ecosystem of over 500 products from over 350 technology alliance partners. This is another example of Fortinet's dedication to supporting our customers in building integration and automation regardless of who they're currently working with.

We have four different categories of technology alliance partners:

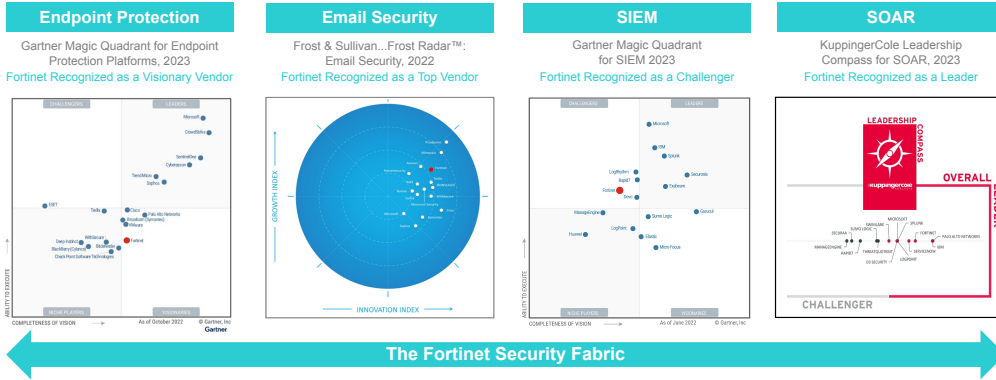
- **Fabric Connectors:** Fortinet-developed deep integrations into technology partner platforms that automate operations, policies, and processes.
- **Fabric APIs:** Partner-developed Fabric [API](#) integrations for a broad range of ecosystem solutions to secure the entire digital attack surface.
- **Fabric [DevOps](#):** Community-driven set of security automation and orchestration tools and scripts developed by Fortinet, partners, and customers.
- **Extended Ecosystem:** Threat intelligence sharing collaborations and other vendor technology integrations, even competitors.

This last category of our extended ecosystem is the most interesting of the four in that Fortinet talks and integrates into some of our key competitors. Listed in this slide are just a few examples, but you'll see this is something very different, a lot of our

competitors won't integrate into Fortinet. But we proactively keep our ecosystem as open as possible, so that we can integrate not only with our partners, but also our competitors. To us, this openness is the best way to meet our customers where they are at and support them in consolidating point products and vendors to build a broad, integrated and automated platform.

One Platform

Enterprise “best of breed” and “platform” are not mutually exclusive



© Fortinet Inc. All Rights Reserved. | 17

The power of the Fortinet Security Fabric and its ability to deliver top ranking security solutions that are integrated is best exemplified by Fortinet’s inclusion in the above analyst reports

All these solutions are built to integrate together across endpoint, email security, SIEM, and SOAR

With Fortinet you don’t have to decide between a Best-of-Breed or a Platform approach, as the power of the Security Fabric you get both . With Fortinet, organizations who want to purchase “best-of-breed" don't have to forego their ability to build an integrated platform.

All these solutions are built to integrate together across endpoint, email security, SIEM, and SOAR

FortiOS, Fortinet’s operating system, is the foundation of the Fortinet Security Fabric the industry’s highest-performing and most expansive cybersecurity platform, organically built on a common management and security framework. FortiOS ties all the Security Fabric’s security and networking components together to ensure seamless integration.

One Platform

Enterprise “best of breed” and “platform” are not mutually exclusive

Secure
Networking



Network Firewall

Dec. 2022 Magic Quadrant for
Network Firewalls

Fortinet Recognized as a Leader



SD-WAN

Sept. 2022 Magic Quadrant for
SD-WAN

Fortinet Recognized as a Leader



Wired and Wireless LAN

Nov. 2022 Magic Quadrant for
Wired and Wireless LAN

Fortinet Recognized as a Visionary



FortiOS Operating System



© Fortinet Inc. All Rights Reserved. | 19

The power of FortiOS and its ability to converge networking and security is best exemplified by Fortinet’s inclusion in the Gartner Magic Quadrants for Network Firewall, SD-WAN, and Wired and Wireless LAN Infrastructure – all for a secure networking solution that run on FortiOS. With Fortinet, organizations who want to purchase “best-of-breed” don't have to forego their ability to build an integrated platform.

Additional/alternate talking point context from John Maddison:

Now one pushback I do get from some customers and some of our competitors is that how can you do all this on one operating system and still be best of breed? Well, this is the proof. Here you'll see three Gartner Magic Quadrants, one for network firewall where Fortinet is a clear leader, also for SD-WAN, again, a clear leader, and wired and wireless LAN where we're a strong visionary. So for most of our competition, these three technologies represent multiple products, multiple operating systems, but for Fortinet it is the same company, the same product, the same operating system, but again with best of breed capabilities.

Note: Image is For Internal Use Only – This does not adhere to Gartner's Quote and Compliance Policy

Gartner does not allow any modifications to the Magic Quadrant graphic



Fortinet Security Fabric

Cybersecurity Platform to Enable Digital Innovation

FortiOS
The Heart of the
Fortinet Security Fabric



Zero Trust Access



- FortiNAC**
Enforce dynamic network access control and network segmentation
- FortiAuthenticator**
Identify users wherever they are and enforce strong authentication
- FortiClient**
Endpoint integration, visibility, and protection across entire network
- FortiToken Mobile**
One-time password application with push notification

Surveillance & Communications



- FortiRecorder**
Platform for management of cameras, systems, and storage
- FortiCamera**
Centrally-manage HDTV-quality security coverage reliability
- FortiVoice**
Centralized control and simplified management of phone systems
- FortiFone**
Robust IP Phones w/ HD Audio for versatile deployments

Security-Driven Networking



- FortiGate SD-WAN**
Application-centric, scalable, and Secure SD-WAN with NGFW
- FortiGate**
NGFW w/ SOC acceleration and industry-leading secure SD-WAN
- FortiSwitch**
Deliver security, performance, and manageable access to data
- FortiAP**
Protect LAN Edge deployments with wireless connectivity
- FortiExtender**
Extend scalable and resilient LTE and LAA connectivity
- FortiSASE**
Secure access service edge to deliver security everywhere
- FortiProxy**
Enforce internet compliance and granular application control
- FortiIsolator**
Maintain an "air-gap" between browser and web content
- FortiPresence**
Real-time location trends, visitor analytics, and heat mapped flows

Fabric Management Center | SOC



- FortiXDR**
Collect, normalize, and correlate data across security controls
- FortiEDR**
Automated protection and orchestrated incident response
- FortiSIEM**
Integrated security, performance, and availability monitoring
- FortiSOAR**
Automated security operations, analytics, and response
- FortiAnalyzer**
Correlation, reporting, and log management in Security Fabric
- FortiSandbox**
Secure virtual runtime environment to expose unknown threats
- FortiDeceptor**
Discover active attackers inside with decoy assets
- FortiAI**
Accelerate mitigation of evolving threats and threat investigation
- FortiGuard MDR Service**
Monitor and hunt for threats, analyze events, leverage alerts

Adaptive Cloud Security



- FortiGate VM**
NGFW w/ SOC acceleration and industry-leading secure SD-WAN
- FortiMail**
Secure mail gateway to protect against SPAM and virus attacks
- FortiWeb**
Prevent web application attacks against critical web assets
- FortiCASB**
Prevent misconfigurations of SaaS applications and meet compliance
- FortiADC**
Application-aware intelligence for distribution of application traffic
- FortiCWP**
Manage risk and compliance through multi-cloud infrastructures
- FortiGSLB**
Ensure business continuity during unexpected network downtime
- FortiDDoS**
Machine-learning quickly inspects all Layer 3, 4, and 7 packets
- FortiCloud Networking**
Manage network access, assets, and services through single-pane
- FortiPhish**
Informative simulation to educate internal users of potential threats

Fabric Management Center | NOC



- FortiManager**
Centralized management of your Fortinet security infrastructure
- FortiCloud**
Connect, protect, and deliver data and apps in Cloud and on premise
- FortiMonitor**
Analysis tool to provide NOC and SOC monitoring capabilities
- FortiAIOps**
Network inspection to rapidly analyze, enable, and correlate

Open Ecosystem



Extended Fabric Ecosystem

- FortiGuard Security Services**

- Content Security
- Web Security
- Advanced SOC/NOC
- User Security
- Device Security
- SOC & NOC
- User Security




Questions





Fortinet Security Fabric Solutions

Over 50 products and services, along with hundreds of partners integrate within the Fortinet Security Fabric.

[Click on any of these solutions in presentation mode to learn more.](#) 



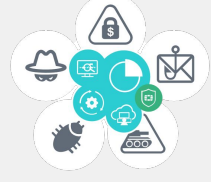
Access and Endpoint Security



Secure Networking



Automated SOC



Secure Application Journey



OT Security



End

© Fortinet Inc. All Rights Reserved. | 18



Access and Endpoint Security



Fabric Solution: Access and Endpoint Security



Universal ZTNA

Explicit application access with continuous verification for secure connectivity



Secure Access Services Edge (SASE)

Cloud-delivered convergence to secure remote users with better user experience



Identity & Access Management (IAM)

Authenticate and authorize user identities to securely access corporate resources



Endpoint Detection & Response (EDR)

Modern endpoint security to stop ransomware and advanced cyber-attacks



AI-powered Security Services

Counter threats in real-time with AI-powered protection natively integrated into the Fabric



[Go Back](#)

[End](#)

© Fortinet Inc. All Rights Reserved. | 20

Secure Networking



Fabric Solution: Secure Networking



Network Firewall

Comprehensive, integrated, and automated cybersecurity solution



Secure SD-WAN & 5G

Transform and secure WAN, enhancing user experience and mitigating risk.



Secure Wireless & Wired LAN

Wi-Fi and Ethernet network equipment secured by a cybersecurity mesh



Secure Access Services Edge (SASE)

Cloud-delivered security and superior user experience for remote users



AI-powered Security Services

Counter threats in real-time with AI-powered protection natively integrated into the Fabric



[Go Back](#)

[End](#)

© Fortinet Inc. All Rights Reserved. | 22



Automated Security Operations



Fabric Solution: Automated SOC

AI-driven coordinated protection across an expanded attack surface



Early Detection (EDR | NDR | Deception | Recon)

Endpoint and other behavior-based sensors to detect and stop attacks along the kill chain



SIEM/FAZ

Normalized data analytics with ML to detect incidents across the attack surface



SOAR

Orchestration / automation for faster, synergistic response



SOC Augmentation Services

Specialized skills (IR), attack assessment and training supplement in-house teams



AI-powered Security Services

Intelligence and engines to detect and respond faster




[Go Back](#)

[End](#)

© Fortinet Inc. All Rights Reserved. | 24

Fortinet Security Fabric in Action



OUTBREAK ALERTS

Zerobot Attack

Go-based malware exploiting multiple vulnerabilities

<https://www.fortinet.com/blog/threat-research/zerobot-new-go-based-botnet-campaign-targets-multiple-vulnerabilities>
CVEs: CVE-2017-17105, CVE-2019-10655, CVE-2020-25223, CVE-2021-42013, CVE-2022-31137, CVE-2022-33891

Zerobot is a Go-based botnet that spreads primarily through IoT and web application vulnerabilities. According to Fortinet research analysis the most recent distribution of Zerobot includes additional capabilities such as a new DDoS attack capabilities and exploiting Apache vulnerabilities.

Background

In November 2022, FortiGuard Labs observed a unique botnet written in the Go language known as Zerobot which contains several modules, including self-replication, attacks for different protocols, and self-propagation. For more information on Zerobot, see the link to Fortinet blog below.

Announced


December 06, 2022: Fortinet posted a security blog research about Zerobot at <https://www.fortinet.com/blog/threat-research/zerobot-new-go-based-botnet-campaign-targets-multiple-vulnerabilities>

Latest Developments

December 13, 2022: Microsoft uncovers new Zerobot 1.1 capabilities and posted a blog at <https://www.microsoft.com/en-us/security/blog/2022/12/13/microsoft-research-zerobot-1-1/>

Release Date	Dec 27, 2022
Last Revised	Dec 27, 2022
Outbreak Alert	Zerobot Attack
Severity	Critical
CVE ID	CVE-2017-17105 CVE-2019-10655 CVE-2020-25223 CVE-2021-42013 CVE-2022-31137 CVE-2022-33891 CVE-2022-30525
PDF	Download

Click on each chart to view data in detail



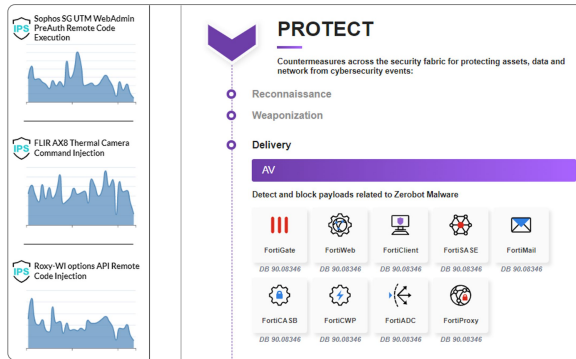
ZyXEL Firewall ZTP Command Injection

Research

- In-house threat team
- Actionable insights
- Provide protection



Fortinet Security Fabric in Action

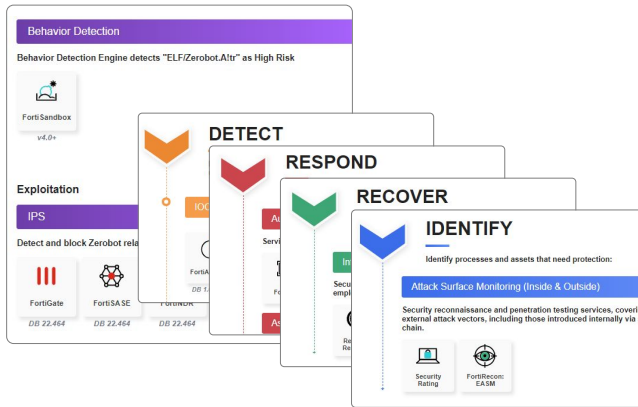


Protect

- Unified protections
- Known and unknown
- Autonomous security



Fortinet Security Fabric in Action





Secure Application Journey



Fabric Solution: Secure Application Journey

Consistent, secured, and optimized experience to build, deploy, and run cloud applications across all cloud and hybrid deployments.



Hybrid Security

Protect and connect networks across clouds, data centers, hybrid clouds, and edge compute



Web Application & API Protection

Simplify securing applications and APIs with AI/ML and automation



Cloud-native Protection

Reduce friction across cloud deployments with security that integrates with and works natively with cloud services



Workload Protection

Seamlessly protect critical workloads



FortiGuard Services

Real-time protection for applications and workloads no matter where they live



[Go Back](#)

[End](#)

© Fortinet Inc. All Rights Reserved. | 29



**Operational Technology (OT)
Security**



Challenge: Securing Operational Technology



Most industrial control systems lack security by design and are sensitive to change.



The attack surface for cyber-physical assets is expanding as a dependence on air-gap protection diminishes with Digital Transformation initiatives driving IT-OT network convergence.



Increasing adoption of new technologies, such as 5G, IoT, and Cloud.



Remote access requirements for third-parties and employees causing additional risks.



Asset owners' reliance on OEMs and SIs exposes critical systems to additional risks.



Asset owners must comply with industry-specific regulations



[Go Back](#)

[End](#)

© Fortinet Inc. All Rights Reserved. | 36

I'm going to talk about some of the challenges securing operational technology.

The first one is that at the very heart of operational technology in the industrial control system, there's this thing called the programmable logic controller, and it's just inherently insecure.

Most programmable logic controllers deployed are not following any kind of Zero Trust approach, rather they're following an Assumed Trust philosophy, which is to say, if a programmable logic controller or PLC receives a message and it's on the network where the PLC is and it's formatted in the language that the PLC expects it. If it's in the right protocol, most PLC's just follow those orders. They'll turn things on, they'll turn things off, they'll reset themselves to factory baseline, there's no asking questions like:

- Who are you?
- Are you authorized?
- Is this a secure encrypted channel?

... like that's just not there, so they just follow orders, so industrial control systems are inherently insecure and they're brittle to change. It's not on the

slide, but I should also call out that they're deployed for a long time, so when someone puts a wind farm into production, you know they're expecting that the PLC's and the SCADA system are going to last for 25 or 30 years.

As long as they're expecting that industrial piece of equipment to last, they don't expect to refresh those things and they're brittle to change.

OEMs are the the manufacturers of the industrial equipment.

They say "hey you can't, you can't go tinkering in this network or you'll void your warranty," and sometimes these PLC's can go offline if you do like an nmap scan on them, so they're sort of sensitive environments and historically, they were able to be secured by virtue of being air gapped.

But "digital transformation" or "digital acceleration" or "industry 4.0" ... all of these different terms mean that we're connecting these industrial environments up to either the data center or the cloud to get data out of them.

So "digital transformation" I'm just going to unpack that term for a moment. What is digital transformation when it comes to industrial environments?

Organizations that own heavy pieces of industrial equipment. They want to know when it's going to break before it breaks. They want to be able to anticipate failure, and to do that they build what's called a digital twin, which typically runs in the cloud or data center. The digital twin requires a lot of data.

It models the physics, and it looks at what's happening in the environment to say this equipment is vibrating too much. It's shaking or it's getting too hot.

Something here isn't right, and it's different than the other ones that we own.

So that's where there's a problem.

That kind of analysis, or digital transformation or digital twin analytics takes a lot of data. You do it in the cloud and that essentially means you've got to connect those assets up outside of the OT zone.

Another example would be moving from calendar-based maintenance to condition-based maintenance. So, calendar-based maintenance means every six months a technician climbs up a third of the way and tightens the nuts and bolts, climbs up another third of the way, and tightens the nuts and bolts that connect the steel segments of the tower, and they do that because the manufacturer of the equipment says you've got to do this to maintain your

warranty and for the asset to be healthy.

What they'd rather do is climb the turbine and tighten the nuts and bolts when they're loose, not just because six months have gone by, so there's like safety margin built into all these recommendations in the OEM manuals and by moving to condition-based maintenance they were able to squeeze some of that margin out and improve their profitability.

That's another example of digital transformation and it's another reason why assets are getting connected.

And you know, if there we've got a bunch of new technologies like 5G IoT, Industrial Internet of Things and cloud, all of these new technologies bring new risks.

They all have complicated supply chains. Some of them are not as mature, so there's just more risk with the more you connect.

All these different environments and you know on top of digital transformation.

We also have a need for secure remote access, so.

If you own pump jacks, which are those those things that take oil out of the ground? You might own hundreds of them in Texas. You know you can't have a person at each pump Jack. It's just not efficient.

You can't have a person in each wind turbine, it's just not efficient.

So, you need a secure way to enable both your employees and your trusted third parties like that Original Equipment Manufacturer, or perhaps the system integrator. You need a way for people to get into these environments to do remote monitoring and diagnostics or upgrades or resetting something that's gone offline and all that remote access entails creating additional risk.

An example of that risk was the Oldsmar attack, so in the last year, in 2021 Oldsmar, FL was a water treatment facility near Tampa where you know they had put the SCADA system on Teamviewer, which is not a secure way of creating remote access and a bad actor hacked into it and changed the setpoint which put too much chlorine in the water.

So that's an example of why you need to do this in a secure way, 'cause you don't want that to happen and then even aside from remote access, just the relationship between the asset owners and the system integrators and the

OEM's. There's additional risk there 'cause a lot of times they need the OEM or the system integrator to do maintenance and so those people even when they come on site physically they bring their phones and their laptops, and a bunch of USB sticks and you don't have control over what they're plugging in.

So, there's risk for that reason too.

Those are all the different things going on in OT environments right now, and now I'm going to talk about how Fortinet helps address some of those challenges. (click, next slide)

<old notes>

The attack surface for cyber-physical assets is expanding as a dependence on air-gaps as a protection mechanism diminishes.

- Digital Transformation is driving IT-OT network convergence
- Most industrial control systems lack security by design.
- Remote access requirements causing additional risks.
- Increasing adoption of new technologies, such as 5G, IIoT, and Cloud.
- OT operations teams often lack security mindset & training.

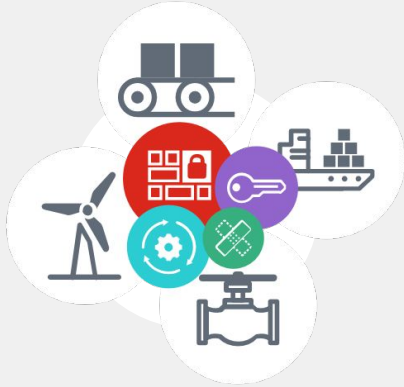
Industrial Control Systems have 20+ year lifecycles

- OT environments include a mix of legacy and new technologies from multiple automation vendors
 - <most endpoint protection solutions won't work in such environments, but ours will>.
- Asset owners are heavily reliant on OEMs.
 - <Customers need to select OT security solutions that control vendors have qualified>
- Asset owners' reliance on OEMs and SIs exposes critical systems to additional risks including:
 - Unsupervised access to the critical systems
 - Lack of endpoint security controls
 - Ineffective logging and monitoring
 - Missing BYOD security
 - Unregulated wireless access
 - Lack of removable media security
- Industrial Control Systems have 20+ year lifecycles

Safety and Availability of cyber-physical systems are of the highest concern – due to these systems being historically running in an air-gap environment, and typically maintained by 3rd-party OEMs through maintenance contracts, they lack,

- Clear and complete ownership
- Regular (or any) software updates/patches
- Configuration change management processes
- Security control implementation – since security is often perceived as an obstacle to production availability

Fabric Solution: Operational Technology Security Solution



Secure Connectivity

Digital Transformation requires secure data exfiltration from OT to Data Centers and Cloud



Secure Remote Access

Zero-trust access for authorized remote technicians and third-parties



Converged Security Operations

Synergistically manage OT and IT networks in a converged SOC.



AI-powered Security Services

OT Security services enable Industrial Control System security to stay ahead of evolving threats



[Go Back](#)

[End](#)

© Fortinet Inc. All Rights Reserved. | 32

The image shows the Fortinet logo centered on a light gray rectangular background. The logo consists of the word "FORTINET" in a bold, black, sans-serif font. The letter "O" is stylized with three horizontal red bars. A small registered trademark symbol (®) is located at the end of the word. In the top right corner of the gray rectangle, there is a small red tab-like shape.

FORTINET®