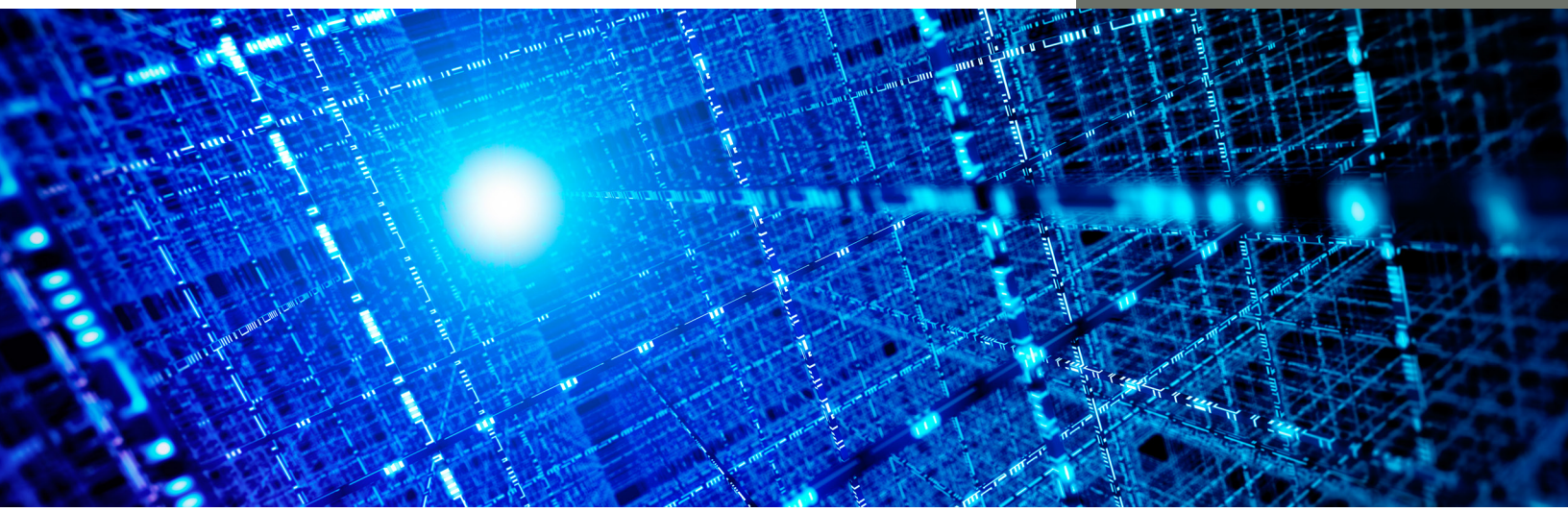


Fortinet Security Fabric

End-to-End Segmentation

Networks are currently undergoing more dramatic change than at any time in the past thirty years. Organizations are simultaneously wrestling with issues such as BYOD, IoT, virtualization, SDN, cloud, the proliferation of applications, Big Data, and the expectations of the next generation of employees to blend their work and their personal lives on a single device of their choosing, with instant access to any data at any time from any location.

This has exponentially increased the attack surface that organizations need to be concerned with. For example:

- IoT and cloud solutions mean organizations need to worry about an attack surface that many times may not be visible to IT.
- Many IoT devices are headless, run simple communications protocols, and are unable to run a client or even be patched. They rely exclusively on the access network for security.
- Critical and proprietary business data is being moved into the cloud and managed by third parties. Known as Shadow IT, this trend is expanding, with many organizations simply unaware of where data is currently located or what security measures are in place to protect it.
- The transformation to a digital business model has extended the network beyond the perimeter, which means that today's networks and their related security are becoming borderless.
- BYOD devices are highly mobile, blend personal and work profiles, and represent real risk as critical data is accessed from public locations, or when devices are lost or stolen.

The problem is compounded by the proliferation of point security products embedded across the distributed network. The tendency as our networks become more complicated is to add new security devices to an already overburdened wiring closet. But the truth is that complexity is the enemy of security. Siloed security solutions with separate management interfaces and no meaningful way to gather or share threat information with other devices on your network are only marginally useful. The truth is, many new solutions never actually get fully deployed because there simply isn't enough manpower to assign to installing, managing, optimizing, and updating another complicated device.

Instead, the response to increasingly complicated networked environments needs to be simplicity. Securing these evolving environments requires three things:

1. Segmentation – Networks need to be intelligently segmented into functional security zones. End to end segmentation, from IoT to the cloud, and across physical and virtual environments, provides deep visibility into traffic that moves laterally across the distributed network, limits the spread of malware, and allows for the identification and quarantining of infected devices.
2. Collaborative intelligence – Local and global threat intelligence needs to be shared between security devices, and a coordinated response between devices needs to be orchestrated centrally.
3. Universal policy – A centralized security policy engine that determines trust levels between network segments, collects real time threat information, establishes a unified security policy, and distributes appropriate orchestrated policy enforcement.

Fortinet's Security Fabric integrates technologies for the endpoint, access layer, network, applications, data center, content, and cloud into a single collaborative security solution that can be orchestrated through a single management interface. It is based on five key principles:

- **Scalable: The Fortinet Security Fabric protects the Enterprise from IoT to the Cloud.**

  A comprehensive security strategy needs both depth (performance and deep inspection) and breadth (end to end.) Security not only needs to scale to meet volume and performance demands, it needs to scale laterally, seamlessly tracking and securing data from IoT and endpoints, across the distributed network and data center, and into the cloud. The Fortinet Security Fabric provides seamless, ubiquitous protection across the distributed Enterprise, from IoT to the Cloud, as well as inspection of packet data, application protocols, and deep analysis of unstructured content – all at wire speeds.

- **Aware: The Fabric behaves as a single entity from a Policy and Logging perspective, enabling end-to-end Segmentation in order to reduce the risk from advanced threats.**

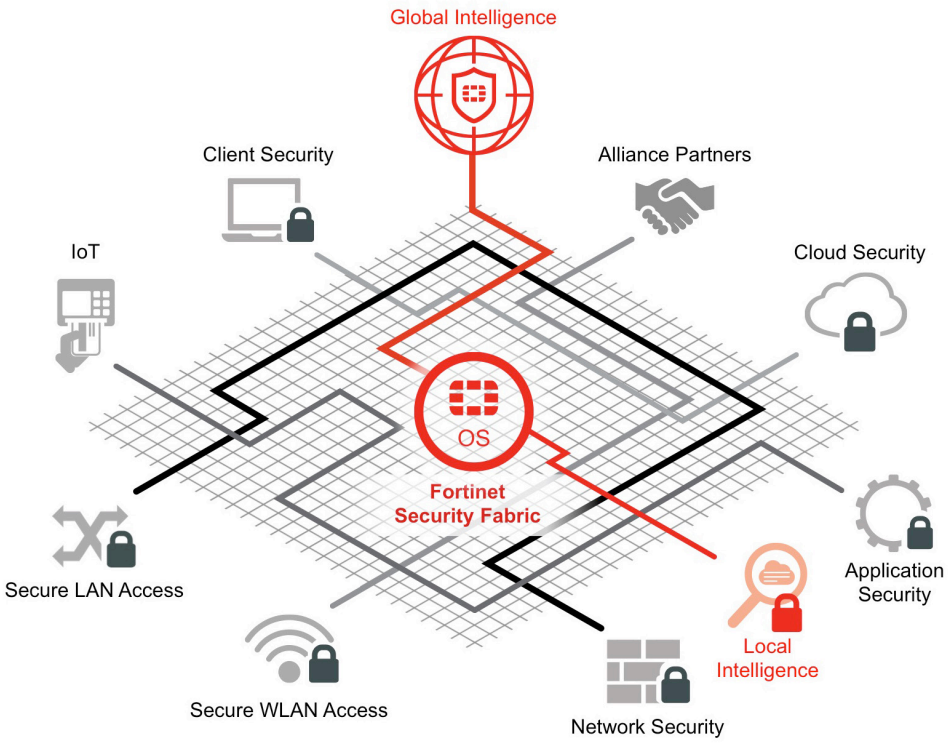
  You not only need to see data that flows into and out of your network, but how that data traverses the network once it's inside the perimeter. The Fortinet Security Fabric enables end-to-end network segmentation for deep visibility and inspection of traffic travelling the network, and control of who and what gets to go where, thereby reducing the risk from advanced threats.

- **Secure: Global and Local threat intelligence and mitigation information can be shared across individual products to decrease Time to Protect.**

  Not only does security need to include powerful security tools for the various places and functions of your network, but true visibility and control requires that these discrete elements work together as an integrated security system. Fortinet's Security Fabric behaves as a single collaborative entity from a Policy and Logging perspective, allowing individual product elements to share Global and Local threat intelligence and threat mitigation information.

- **Actionable: Big Data cloud systems correlate threat information and network data to deliver Actionable Threat Intelligence in real time.**

  It's not enough to detect bad traffic or block malware using discrete security devices. You need a common set of threat intelligence and centralized orchestration that allows your security to dynamically adapt as a threat is discovered anywhere, not just in your network, but anywhere in the world. Fortinet's Big Data cloud systems centralize and correlate threat information and network data to deliver actionable threat intelligence to every security device in your network's security fabric in real time.



- **Open: Well-defined, open APIs allow leading technology partners to become part of the fabric.**

  Of course, a true security fabric will let you maximize your existing investment in security technologies. Which is why Fortinet has developed a series of well-defined, open APIs that allow technology partners to become part of the Fortinet Security Fabric.

  Combined, the Fortinet Security Fabric is able to dynamically adapt to the evolving network architecture as well as the changing threat landscape

  Let's take a more detailed look at the five key elements of the Fortinet Security Fabric: Scalable, Aware, Secure, Actionable, and Open.

1. Scalable

Security not only needs to scale to meet volume and performance demands, it needs to scale laterally, seamlessly tracking and securing data from IoT and endpoints, across the distributed network and data center, and into the cloud.

The Fortinet Security Fabric provide three essential elements:

1. A single, unified platform that shares common threat intelligence, enables intelligent collaboration between security devices, and dynamically adapts to new threats
2. Single-pane-of-glass management across all security technologies, wherever they are deployed, for centralized policy orchestration, threat response coordination, and real-time distributed enforcement.
3. A single source for security intelligence and updates that combines local information with global intelligence services for real time response to established and emerging threats.

Scalability into the Cloud

The adoption of virtualization and cloud-based services is transforming networks. This migration to the cloud has a number of distinct security challenges that can only be addressed using a secure fabric approach:

1. **Virtualization and Private Cloud.** While virtualization has been underway for some time, it is still a vulnerable and largely unprotected area of many networks. A strategy for securing your virtualized environments needs to take a number of things into account.

   The first is that about 40% of organizations adopting virtualization end up deploying multiple hypervisors. To ensure seamless and consistent security between these virtualized environments, your security solutions need to operate across all the major hypervisors.

   Another challenge is that some virtualization solutions create a gap between physical and virtual resources. Security needs to bridge that gap to ensure consistent threat awareness and security enforcement regardless of the devices processing data.

   A number of new attacks have been targeted specifically at virtual machines, including virtual rootkits to mask their presence. In many organizations, traffic between virtual machines is rarely inspected, leaving virtual machines, workloads, and transactions highly vulnerable to attack.

   Finally, virtualization allows for the rapid deployment of new workload resources and dynamic scalability to manage unexpected data bursts. Security for virtualized environments needs to be provisioned quickly, and scale rapidly so that critical business transactions and workflows are never interrupted or needlessly rerouted for inspection.

   A fabric-based security approach allows organizations to create seamless security policies between their physical, virtual, and private cloud environments.

2. **Next-gen SDN Data centers.** Data centers are undergoing rapid changes, including the implementation of next-gen, software defined networks and private cloud environments. These new architectures allow for instantaneous provisioning of resources, chaining together services, and the acceleration of workflows while abstracting away the overhead related to managing the physical layer of ports, servers, and switches.

   These new data centers require purpose-built security solutions designed for their unique architectures. In addition, these new environments run alongside traditional data centers, making a single security standard difficult. To complicate things further, some SDN solutions make it difficult to bridge between virtual and physical environments, so establishing and enforcing consistent security policies can be challenging.

   The advantage is that being able to stitch security services directly into transaction chains allows security to operate inline to automatically provision East-West security and dynamically scale security resources.

   As with virtualization, a secure fabric strategy allows organizations to place security devices into different architectural environments, yet still maintain centralized threat intelligence and consistent policy enforcement.

3. **Public and Hybrid cloud.** Many organizations are adopting public cloud services for everything from on demand off-loading of high-volume traffic, a process known as cloud bursting, to moving some or all of their infrastructure into the cloud with some sort Software, Platform, or Infrastructure as a service.

   From a security perspective, the challenge is how to establish and maintain consistent security policy and policy enforcement as data moves back and forth between local and cloud environments.

   For this to work, two things need to happen. First, you need to work with a service provider who can assign your cloud environment the same security technology you use in-house. Which means you need to select an in-house solution that has been widely adopted by the service provider community. And second, you need a cloud-based security management and orchestration tool that can pass policy and security intelligence between security devices deployed across distributed environments.

The Fortinet Security Fabric provides solutions for each of these environments, including the most widely adopted service provider security solutions in the market, that can be woven together into a single, seamless security fabric for complete visibility and control across the entire distributed environment.

Scalability for the Network

With more devices and applications accessing network resources, performance is critical and slow is broken. Far too often, when security becomes a bottleneck, users and administrators begin to look for workarounds

Traditional security solutions that depend on CPU-based processing simply cannot scale to meet escalating demand.

- Security devices take huge performance hits when additional inspection tools are added
- Daisy-chaining security devices for serial traffic inspection introduces additional problems of latency and the redundant inspection of the same data or application content

Fortinet's security devices and Security Fabric leverage patented high-performance ASICs that provide Parallel Path Processing. This means that:

- Packet processing can be offloaded to a network processor to accelerate packet inspection
- Content can be offloaded to Fortinet's new content processor for deep resource-intensive inspection of unstructured data
- The CPU only needs to be used for traditional data processing and policy management
- Threat intelligence updates and policy coordination can happen without impacting critical business operations

The result is higher performance at a lower cost, less latency, less power consumption, and less rack space required.

Scalable Secure Access

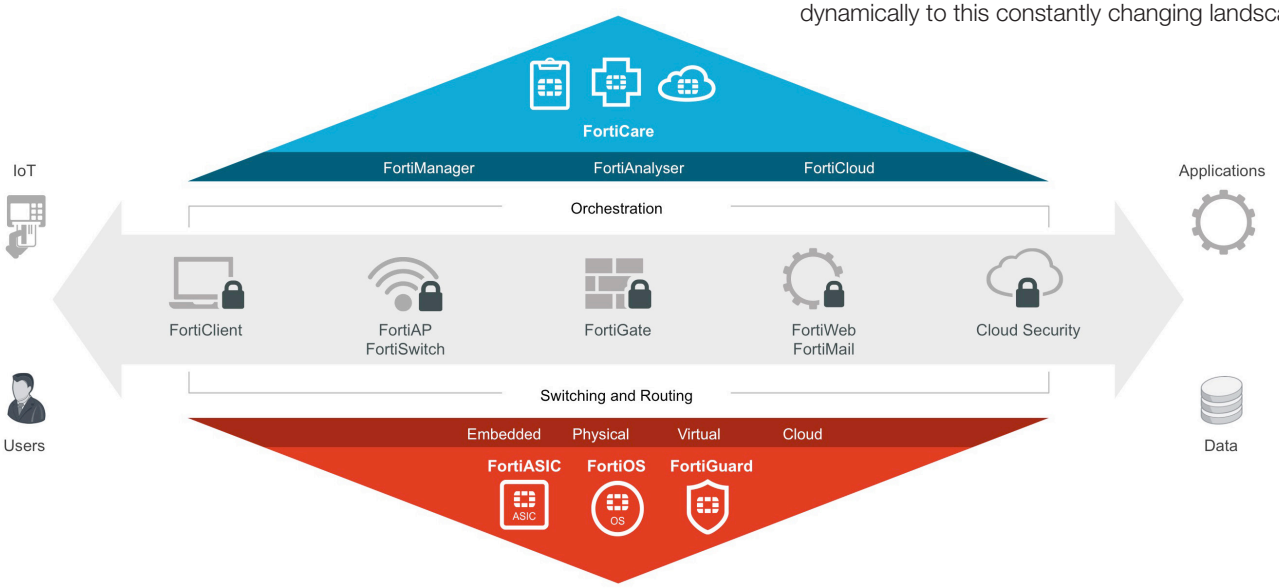
Access control is a critical component of any security strategy. When it is part of a security fabric, devices that attach to the network, whether from outside or inside the perimeter, can be identified, tracked, and protected as they traverse the networked environment.

BYOD brought the first wave of new devices becoming part of the network. But with the advent of the Internet of Things (IoT), organizations are now looking at billions of new IP-enabled, non-user devices coming online over the next couple of years. More than ever, the first stage of security has to be secure access, because

- Many of these devices cannot be independently secured
- Most IoT devices are headless – which means you can't install a clients, bad or insecure code cannot be patched, and there is no mechanism for updates
- Many new BYOD devices also can't have a client installed

And as the edges of our networks continue to blur, secure access is more than just perimeter access.

- Devices can be local or remote, outside or inside the perimeter
- Applications tunnel from remote devices directly into the data center or cloud
- Secure access between network segments is critical to ensure that critical resources are only accessed by authorized users and devices, and so that infected devices can't spread malware laterally across the network
- Security policies and enforcement will need to adapt dynamically to this constantly changing landscape



The response to a more complicated problem needs to be simplicity. A fabric-based approach to security allows an organization to create and monitor a consistent and unified strategy across all access methods, whether wired, wireless, or VPN.

2. Aware

Visibility is critical. Unfortunately, the fact is that many organizations have very little insight as to what users and devices are on their networks at any given time. That may have been adequate a long time ago when network borders were rigid and clearly defined. But with the advent of BYOD, IoT, virtualization, cloud, and off the shelf applications flowing across the network, poor visibility is a formula for disaster. An effective awareness strategy needs to include:

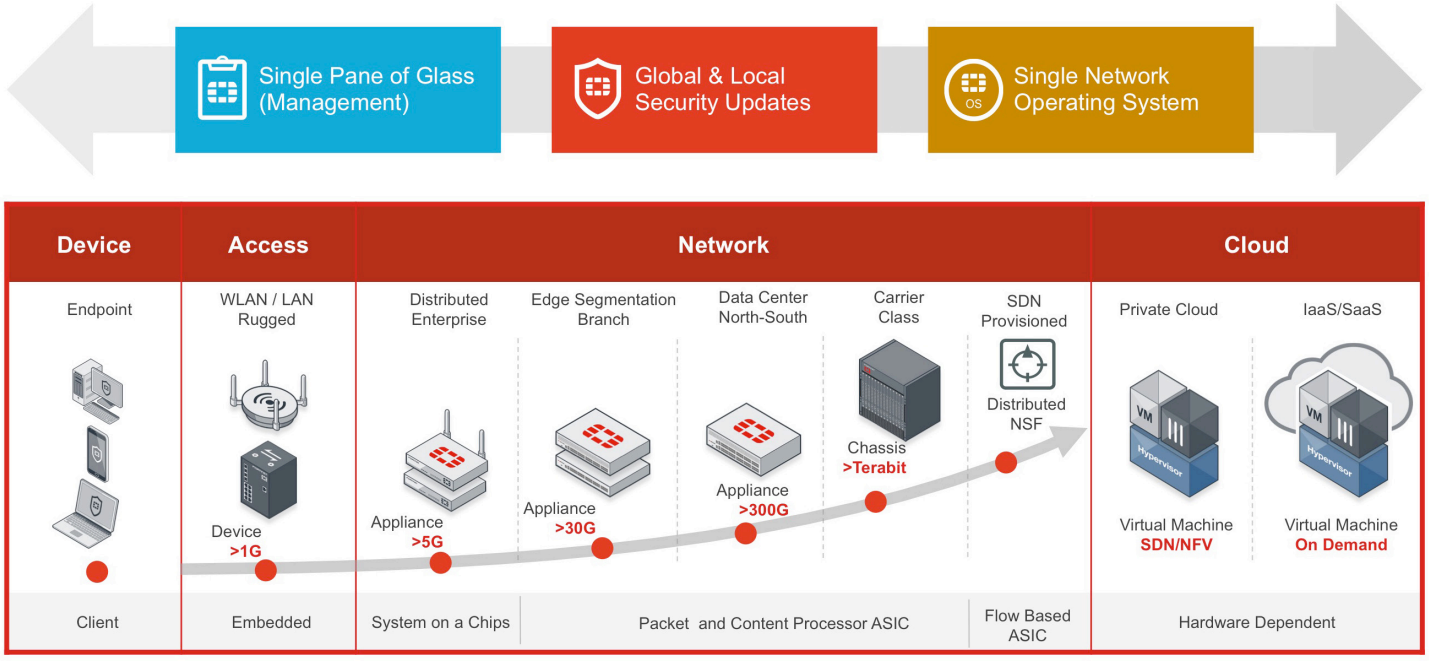
- User identification – Who is on the network? What are they allowed to do? When did they join the network?
- Device identification – What devices are on the network? Who do they belong to? What are they allowed to do? How do I find out when they start behaving badly?
- Physical Topology – How are these devices connected to the network? What devices are they allowed and not allowed to interact with?
- Network and Application Topology – What policies do we need? How are they distributed and enforced? Do we have a single view across the network? How do we know when a policy has been violated? Can a violation detected on one device trigger an automated response on another device?

Being able to answer these questions can serve as a catalyst for planning, designing, implementing, and optimizing an effective awareness strategy. It can also serve as a critical measuring stick for evaluating security technologies you choose for your network.

Awareness – The Advantages of the Fortinet Security Fabric

The need for comprehensive visibility across the distributed enterprise, coupled with granular control and automated response across multiple security devices was a key driver behind Fortinet's development of the Security Fabric. This fabric ties together data, applications, devices, and workflows to provide a level of awareness that has never been available from any security solutions provider. The Fortinet Security fabric covers:

- Endpoint client security
- Secure (wired, wireless, and VPN) access
- Network security
- Data center security (physical and virtual)
- Application (OTS and custom) security
- Cloud security
- Content (email and web) security
- Infrastructure (switching and routing) security



The Fortinet Security Fabric is designed to provide integrated, collaborative, and adaptive enforcement across the distributed network, and can dynamically convert live data, logs, and events into policy.

3. Secure

For an integrated security strategy to be successful, it needs a single source of truth. Complex, multi-vendor environments suffer from two issues:

- An inconsistent understanding of the threats they are seeing or looking for
- The inability to share actionable threat information with other security devices

Threat Intelligence Needs to Be Global

Knowledge is power. The effectiveness of any security strategy or solution is its ability to recognize and respond to threats, especially threats it has never seen before. Constant actionable updates from a trusted intelligence source that gathers real time information from around the globe allow solutions to be tuned to the latest threats. This works even better when every device in your security fabric shares the same information.

FortiGuard's threat research lab provides Security Fabric devices with critical security awareness from:

- The Threat Intelligence Exchange: The Cyber Threat Alliance is a consortium of leading security vendors who have come together to share threat intelligence on advanced attacks, their motivations, and the tactics of the malicious actors behind them. Combined, they provide the most comprehensive threat intelligence available in the market.
- Fortinet threat researchers: In addition, Fortinet's team of threat researchers provide deep investigations into emerging threats and vulnerabilities in order to provide organizations with thorough and actionable security intelligence. The Fortinet team has discovered and reported on more zero-day attacks than any other organization in the world.
- Live feeds from Fortinet solutions: Fortinet also has millions of devices around the world that detect and pinpoint threats and malware in order to provide real-time information on activities, trends, and emerging issues.

The intelligence gathered from these resources is collected, correlated, and converted into actionable updates that are constantly being pushed to Fortinet's entire portfolio of security solutions. This ensures that the security fabric can detect and respond to the latest threats regardless of where they appear across your distributed network.

Threat Intelligence Also Needs to Be Local

In addition to global intelligence, security solutions need to take into account what is happening on the local network. Anomalous behavior, malware, unknown devices, and unauthorized users all need to be quickly identified so the security fabric can provide immediate countermeasures in order to protect the network, limit the spread of an outbreak, and provide useful forensic information.

An effective local intelligence strategy needs to include the following elements:

- Threat intelligence needs to be gathered and correlated from the network in real-time. Many threats, such as Advanced Persistent Threats (APTs), can only be detected when a series of seemingly unrelated, low-level events are correlated and analyzed
- Threat intelligence needs to collected from traffic entering and leaving (north-south) the network, data that moves laterally (east-west) across the network, and data the moves horizontally across the network (end to end)
- Threat intelligence needs to be shared between different devices for coordinated response. When siloed security solutions are looking for different things, alert in different ways using different protocols, and can't share or correlate threat information with other devices, the ability to detect and respond to attacks is severely limited
- A single management tool allows for centralized policy creation, unified orchestration, and distributed enforcement across a variety of security solutions

This sort of cooperative detection and response is difficult if not impossible to achieve from a collection of individual products, even from the same vendor, if they don't share common intelligence, common management, and common policy enforcement. To respond effectively to today's sophisticated threat landscape, an integrated and collaborative security fabric is essential.

Security Certification

Industry certification is a good indicator of a vendor's commitment to building and maintaining effective security solutions. Fortinet aggressively certifies its products through all the major, independent certification organizations in order to assure customers that our technologies meet rigid security standards, comply with regulatory requirements, and ensure that our solutions address the latest threats and threat vectors.

When reviewing vendor certifications, it is important that organizations are educated on which certifications provide real value. For example, there are a number of "pay to play" testing and certification organizations who, for a fee, will create a report showing that a vendor's product is a best in class solution. Such reports are unreliable, and Fortinet does not participate in them.

In addition to third-party certifications, test bed bake-offs give your organization a sense of what a security solution is actually capable of doing inside your unique environment monitoring your unique traffic. Fortinet highly recommends these sorts of comparisons as they let you separate functionality from marketing and sales hype.

Fortinet's entire suite of security solutions consistently achieve top scores from rigorous independent testers like NSS Labs, and have earned more certifications from regulatory organizations than any other vendor in the security market.

Security – Better Together

The Fortinet Security Fabric allows different security technologies to work together to more effectively secure evolving network environments and solve new threat challenges

- Firewalls – Fortinet provides an extensive range of market-leading firewall solutions, including high-performance appliances, virtual firewalls, and cloud options
- Advanced Threat Protection framework – Fortinet ATP provides advanced security solutions such as sandbox, email, web, and client security
- Data Center security – High speed security appliances for North/South traffic, dynamically scalable virtualized devices to inspect and secure East/West traffic, and application security with deep content inspection to secure workflows and transactions. These solutions are also fully integrated with leading SDN and ACI next-gen data center architectures
- Cloud security – Fortinet provides solutions to protect private cloud environments, public clouds such as AWS and Azure, SP-provided cloud services such as XaaS and cloud-bursting solutions, and hybrid on-prem/off-prem cloud solutions
- Secure Access architecture – a variety of access control, secure switching, and policy enforcement tools for consistent, high performance wired and wireless access management
- Connected UTM – a powerful solution for small to medium businesses and branch offices, Fortinet's UTM solutions provide an all in one security solutions combined with cloud-based management for remote deployments lacking on-site technical resources

4. Actionable

The Fortinet Security Fabric is designed to respond and adapt to threats in real time by leveraging actionable threat intelligence. It provides collaborative, cooperative functionality between Fortinet's suite of security technologies for increased visibility and response, FortiGate's single security OS across all implementations to simplify control, and a cloud-based management and orchestration tool that allows for centralized control across a dynamic and widely distributed network environment.

Critical components of the Fortinet Security Fabric include:

- FortiManager – provides single pane-of-glass management and orchestration
- FortiCare – delivers critical incident response services
- FortiCloud, FortiGuard+, Cloud FortiSandbox – extends the security fabric into the cloud
- Virtualized versions of Fortinet's security solutions that work with all leading hypervisors
- Full integration with all the leading SDN and Cloud architectures
- The single most adopted security by service providers for seamless policy enforcement between on-prem and off-prem infrastructure.

5. Open – Fortinet's Partner Alliance Ecosystem

Of course, organizations have already invested in an infrastructure of networking and security platforms and products that are an essential part of their defense capability. Extending the functionality and intelligence of the Fortinet Security Fabric to leading third-party solutions is critical for many enterprises.

Fortinet is committed to a collaborative and interactive community of security solutions. It's one reason why we are an active member of the Cyber Threat Alliance, and why we have also developed a robust partner alliance program that pulls together leading security technology vendors to help address complex threat challenges.

Fortinet has developed a series of APIs that allow alliance partners to connect to the Fortinet Security Fabric in order to further enhance your organization's visibility, control, and response. These API integration points include:

- Hypervisor
- SDN Orchestration
- Cloud
- Sandbox
- Logging
- Policy management

Integration goes beyond simply allowing third-party solutions to collect or redirect data and traffic. Alliance solutions that integrate with the Fortinet Security Fabric are able to actively collect and share threat information and mitigation instructions in order to improve threat intelligence, enhance overall threat awareness, and broaden threat response from end to end.

Summary

The evolving enterprise network and its transition to a digital business model is one of the most challenging aspects of network security today. As significant trends in computing and networking continue to drive changes across many critical business infrastructures, architectures, and practices, organizations are looking for innovative network security solutions to help them embrace those changes.

The Fortinet Security Fabric can provide the scalability, security, awareness, actionable intelligence, and open API strategy your organization needs, enabling the security, flexibility, scalability, collaboration, adaptability, and manageability you demand across your physical, virtual, and cloud environments, from end to end.

For more information on the Fortinet Security Fabric, please go to http://www.fortinet.com/aboutus/why-fortinet.html

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
Valbonee
06560, Aples-Maritimes,
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA SALES OFFICE
Paseo de la Reforma 412 piso 16
Col. Juarez
C.P. 06600
México D.F.
Tel: 011-52-(55) 5524-8428

April 22, 2016