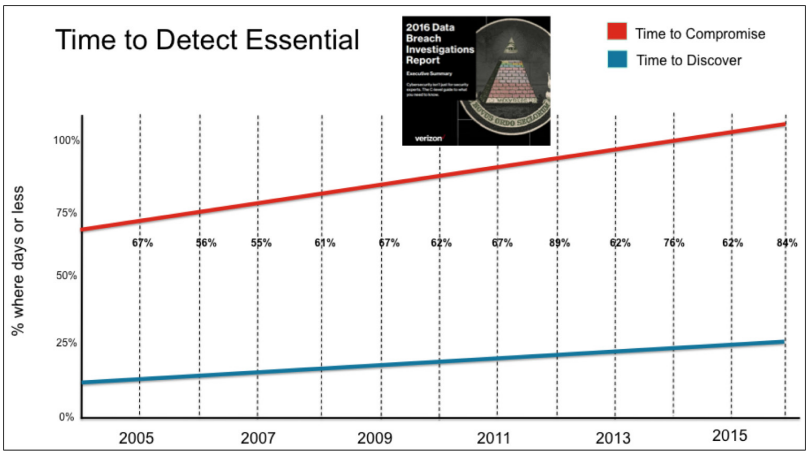
Fortinet Security Fabric and the Threat Landscape

Introduction

The irony of the evolution of the network is that as we make applications, data, and services flow faster across an increasingly diverse landscape of users, devices, and domains, we have compounded the complexity of securing this new environment.

That's because our tendency has been to just keep adding new security devices to an already overburdened security closet. But as the continued increase of network compromises indicates, this approach isn't solving the problem. The fact is that while the new devices you are buying and deploying may decrease the time it takes to discover new threats, data shows that the time required for an attack to compromise your network has decreased even faster, and you aren't keeping up.



Part of the challenge 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. What is needed is a collaborative ecosystem of security tools distributed across your network, from IoT to the cloud, designed to work together as a seamless defense—monitoring devices and traffic, intelligently segmenting your network, sharing and correlating local and global threat intelligence, and working together cooperatively to remove threats occurring anywhere along the attack chain.

The Fortinet Security Fabric

What is needed is a completely new approach to security. The Fortinet Security Fabric is an architectural approach to security that for the first time allows you to tie together all of your discrete security solutions into an integrated whole. This fabric-based approach is built around five key attributes:

1. **Scalable**—Because the Security Fabric weaves security and networking technologies together, security policy and enforcement can be scaled across your entire distributed network to more effectively secure evolving network environments and solve new threat challenges.

2. **Aware**—By integrating security for the endpoint, access layer, network, applications, data center, content, and cloud into a single collaborative solution, the Security Fabric is able to share threat intelligence, identify sophisticated threats most individual security solutions miss, and automatically coordinate an effective response.

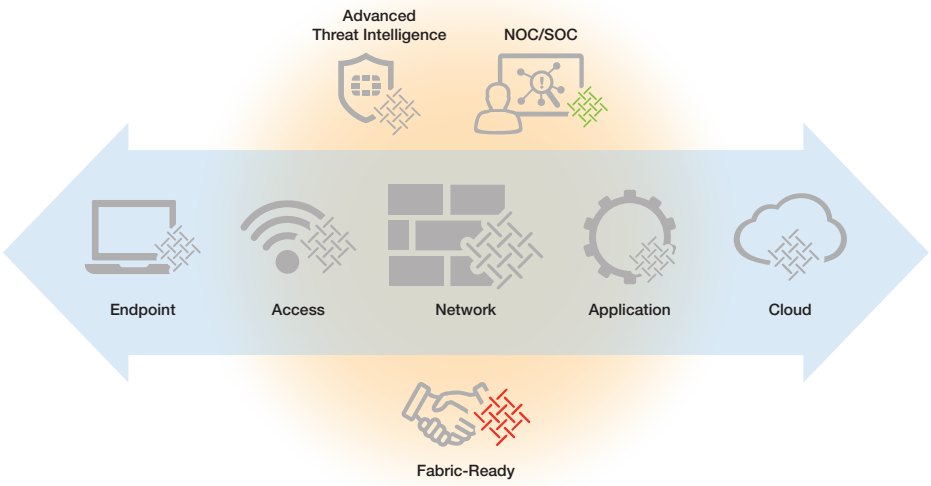
3. **Secure**—The Fortinet Security Fabric enables an unprecedented layered defense approach to protecting your distributed assets. By combining next-generation detection and response systems, intelligent network segmentation, and single-pane-of-glass orchestration, the Security Fabric is able to see and respond to today's most sophisticated threats while dynamically adapting to evolving network architectures.

4. **Actionable**—Through the real-time sharing of global and local threat intelligence—orchestrated through a unified analysis and management interface—the Security Fabric empowers a dynamic response to the capabilities of criminals as they implement new threat strategies and zero-day attacks.

5. **Open**—The Security Fabric is designed around a series of open APIs (application programming interfaces), open authentication technology, and standardized telemetry data that allow organizations to integrate existing security investments from alliance partners into the Fortinet Security Fabric. These solutions can actively collect and share threat information and distribute mitigation instructions to improve threat intelligence, enhance threat awareness, and broaden threat response from end to end.

Responding to the Threat Life Cycle

Attacks tend to follow a four-step process. The four Ps of the threat life cycle—Prepare, Penetrate, Persist, and Propagate—are based on attack capabilities that allow criminals to make an extended assessment of the network, exploit a discovered vulnerability to get inside, lay down a rootkit or something similar to avoid being seen, and then expand into the network looking for data or resources to exploit or steal. Each step of the process uses specific tools and technologies, shares exploit information, and is usually centrally managed by your attacker.



In order to mount an effective response, your security deployment needs to be able to map its capabilities to those being used by attackers. The Fortinet Security Fabric integrates the following critical security functionality together into a threat-oriented architecture designed to see and thwart even the most sophisticated attacks targeting the most remote corners of your enterprise:

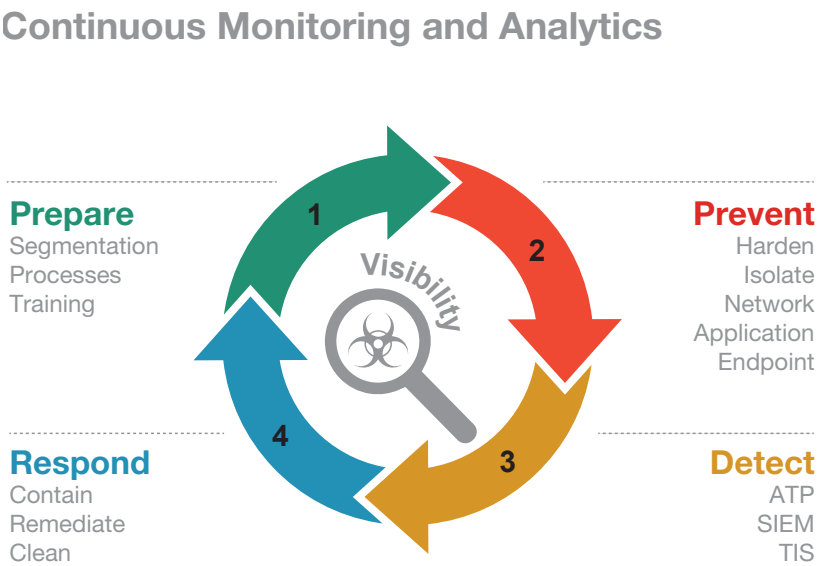
Visibility—You can't defend what you can't see. The Fortinet Security Fabric allows you to identify every element on your network, visualize how these components interact in order to identify potential attack vectors, and establish and enforce more effective policies and mitigation strategies.

Segmentation—The Security Fabric can intelligently segment your network 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.

Automated Operations—The Security Fabric dynamically shares local and global threat intelligence between security devices, and can use that information to centrally orchestrate a coordinated threat response between devices to stop a threat anywhere along the attack chain.

Security Audit—The Security Fabric's centralized management and next-generation SIEM technology can determine and monitor trust levels between network segments, collect real-time threat information, establish a unified security policy, make recommendations based on security posture, and orchestrate appropriate policy enforcement anywhere across the expanded network.

This functionality is woven into Fortinet's four-step threat life cycle strategy that has been designed to address the attack strategy used by cybercriminals. These four steps are: **Prepare, Prevent, Detect,** and **Respond**.



Prepare

It is still quite surprising to learn how many organizations have failed to develop a complete security strategy. Far too many don't even have a written security policy. Instead, they often simply add security devices to their networks as needed, and almost as an afterthought. It becomes the classic "accidental architecture" challenge, where security consists primarily of siloed security technologies bought one at a time to solve different issues, and which provide little collective visibility.

Instead, preparing a dynamic yet secure network needs to start with these three essential elements:

1. End-to-End Segmentation

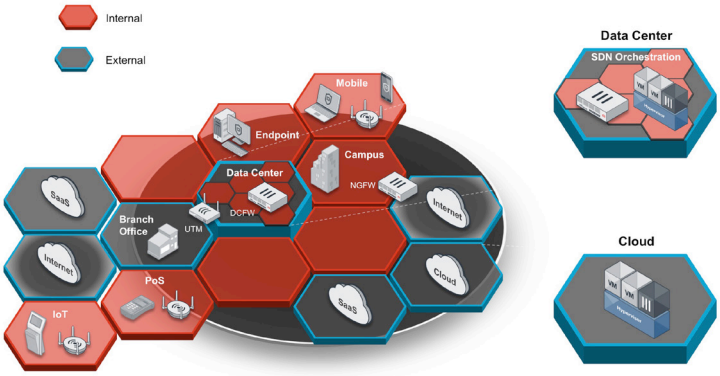
Network segmentation not only logically separates data and resources, it allows for advanced visibility of data and threats as they move from one network zone to the other. From a threat perspective, network segmentation divides your network into security zones to aid in compliance, monitor internal traffic and devices, prevent unauthorized access to restricted data and resources, and control the spread of intruders and malware.

The Fortinet Internal Segmentation Firewall (ISFW), part of the Security Fabric architecture, prevents the proliferation of threats once they get past your network's outer defenses by intelligently segmenting and defending the network inside the perimeter. The ISFW may also sit in front of specific servers that contain valuable intellectual property, or protect a set of user devices or web applications sitting in the cloud.

2. Processes

Once your network has been organized into discrete security zones, the next step is to understand your network processes and procedures. Here are some essential questions you should ask as part of your preparation process:

- **User identification**—Who is on the network? What are they allowed to do? When did they join the network? What credentials are required for access?
- **Device identification**—What devices are on the network? Who do they belong to? What are they allowed to do? How do I find out if and when they start behaving badly?
- **Physical Topology**—How are these devices connected to the network? What other 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?



The next essential step is to select security solutions designed to address these procedural concerns. Ideally, they should work together as a system to map, monitor, and secure your distributed network, from IoT to the cloud. The need for comprehensive visibility across the distributed enterprise, combined with granular control and coordinated response between different security devices, was a key driver behind Fortinet's development of the Security Fabric. It ties together data, applications, devices, and workflows to provide a level of awareness and responsiveness that has never been available from any security provider.

The Fortinet Security Fabric includes:

- 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

Not only are the components of the Fortinet Security Fabric designed to work together as a holistic security system, we have also developed a series of APIs that allows Fortinet Alliance Partners to collect and share information with the Fortinet Security Fabric in order to further enhance your organization's visibility, control, and response.

Security Fabric API integration points include:

- Cloud
- Virtualization
- SDN Orchestration
- Endpoint & IoT
- Vulnerability Management
- SIEM
- Management
- Network & Security Operations

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

3. Training

Of course, any security preparation needs to include training. This can vary from technical certifications to simple awareness campaigns for your employees—because the vast majority of compromises in a network still happen because someone clicked on an email link or attachment that they shouldn't have.

Additionally, it is essential that you ensure that your IT and security teams receive vendor-based training to enable them to maximize the functionality and features of your security technology investments. This training also needs to include how to leverage open APIs to allow different devices to better share threat intelligence and respond to threats.

Prevent

Most organizations spend the majority of their security dollars on perimeter security, trying to prevent bad actors and malware from breaching their network defenses. But with some experts predicting that global annual cybercrime costs will grow to as much as $6 trillion by 2021, organizations may want to rethink how those security dollars are being spent.

This challenge is compounded by the fact that networks have become highly distributed, which means that a perimeter-based security strategy is increasingly difficult to define and deploy. To defend an organization against today's sophisticated cyberthreats, an effective prevention strategy needs to include the following things:

- **Access Control**—This needs to be implemented both at the traditional access layer of the network, as well as every time data, applications, or workloads attempt to cross between network zones.
- **Hardening Edge Devices**—In addition to firewalls and VPNs, organizations need to consider deploying routers, switches, and wireless access points designed with security in mind. Any device that is not contributing to the security health and intelligence of the network represents a risk.
- **Isolation and Remediation**—Compromised devices need to be quickly identified and removed from the network for remediation.
- **Network Segmentation**—As access becomes more ubiquitous across an organization, it is essential that the network be dynamically segmented into security zones as new devices, such as IoT, join the network in order to prevent the spread of malware or limit free access to data and resources inside the traditional network perimeter.
- **Securing Applications**—Application traffic, workloads, and structured and unstructured data all need to be inspected and monitored. To be done effectively, this process requires significant processing overhead that most security solutions struggle to provide.
- **Securing Endpoint Devices**—Endpoint devices, especially BYOD and IoT, continue to represent a real challenge for many organizations. They are often a conduit for things like malware, and need to be appropriately hardened, either through installing a client, inspecting through a cloud-based service, or imposing strict access control and inspection. As much as possible, from a security standpoint they need to be treated as an extension of the distributed network.

- **Extending Security into the Cloud**—Security can't end as traffic, resources, and applications move into the cloud. Implementing consistent visibility, policy enforcement, and threat coordination between your traditional, virtual, and cloud networks is essential.

The Fortinet 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.

Detect

As organizations embrace the latest digital business technologies, such as IoT, mobility, and cloud services and infrastructures, traditional network boundaries are becoming increasingly complex to control and secure.

Organizations cannot assume that perimeter defenses will be enough. There are now so many different ways into an enterprise network that the question of a breach is not if it will happen but when. And far too often, once a hacker gains access to the network, they have free access to the entire enterprise network—including all its valuable assets. Furthermore, cybercriminals can remain dormant inside a network for long periods of time, allowing them to explore and map information, plant malware, and steal data, resulting in disastrous consequences for the victim organization.

The Fortinet Security Fabric includes three critical security components designed to aid in detecting even the most sophisticated threats:

Advanced Threat Protection (ATP)—The Fortinet ATP solution is designed to prevent, detect, and mitigate today's most advanced threats. It includes the FortiGate firewall, the FortiMail secure email gateway, the FortiWeb web application firewall, FortiClient endpoint protection, and proactive advanced threat detection using FortiSandbox technology. The leading security intelligence of FortiGuard Labs is complemented by the local intelligence of FortiSandbox dynamically shared across the interconnected security infrastructure. This allows an ATP deployment to automatically respond to the latest targeted attacks, continually improve an organization's security posture, close natural gaps between multi-vendor point products, and reduce the time spent managing IT security.

FortiSIEM—On average, security breaches take nearly eight months to detect, and even then are usually only discovered by third parties. Part of the reason is that many enterprise security teams have well over a dozen different security monitoring and management consoles to track, and they still have to hand-correlate events and data to detect today's evasive advanced threats.

FortiSIEM is an all-in-one platform that provides deep, coordinated insight into what's happening on your network, letting you rapidly find and fix security threats and manage compliance standards—all while reducing complexity, increasing critical application availability, and enhancing IT management efficiency.

Threat Intelligence Services—The Fortinet Security Fabric is powered by the security services developed by FortiGuard Labs, consisting of more than 200 expert researchers and analysts stationed around the world. These researchers work with world-class, in-house developed tools and technology, combined with data collected from more than two million sensors around the globe, to study, discover, and protect against new and evolving threats.

This extensive knowledge of the threat landscape, correlated with live local threat intelligence, enables the Fortinet Security Fabric to identify and respond quickly to emerging threats and then automatically coordinate effective countermeasures.

Respond

Seeing a threat is only half the battle. Once a threat has been identified, you need to be able to answer five critical questions:

1. How did this threat get here?
2. How long has it been here?
3. How many devices have been compromised?
4. How do I remove all of it from every device?
5. How do I ensure that it will not come back?

FortiSandbox—Part of the Fortinet Advanced Threat Protection solution, FortiSandbox is designed to identify unknown and advanced threats. Once a new threat is identified, FortiSandbox provides immediate mitigation by automatically leveraging direct intelligence-sharing between detection and prevention products. It can also provide assisted mitigation, which enables people and technology to work together to resolve complex threat challenges, including cleaning and remediation.

When Fortinet Security Fabric components work together, they provide a powerful response to identified threats through automation and remediation.

Automation—Simply identifying and alerting on threats is no longer enough. The time to compromise is short, and effective malware can begin exfiltrating critical data within minutes. The Fortinet Security Fabric is designed to automatically break the infection chain and dynamically protect network resources as soon as a threat is detected.

Remediation—Remediation strategies include quarantining infected devices, filtering out malware, blocking access to command and control, and locking down critical network resources. These coordinated responses are designed to identify and isolate affected devices so they can be cleaned and placed back online. Additional protections and policies derived from detected threats are then put in place across all segments of the network to improve the organization's security posture and ensure the prevention of future attacks.

A Tiered Approach

The Fortinet Security Fabric is built around a series of tiered interconnectivity and open API strategies that allow Fortinet and third-party solutions from Alliance Partners to collect and share threat intelligence and coordinate a response when anomalous behavior or malware is detected.

Inner Core Network Security—The first step to securing your network is establishing a hardened and proactive inner core of your network. The foundation of the Fortinet Security Fabric accomplishes this through the tight integration and dynamic interoperability purposefully designed between three foundational Fortinet security technologies: FortiGate, FortiManager, and FortiAnalyzer.

Outer Core Security—Once the inner core of the network is hardened and actively monitoring, analyzing, and correlating threat activity, it is essential to expand that functionality to the borderless edges of the network. Things like the cloud, BYOD, and IoT have transformed today's networks. The next tier of the Fortinet Security Fabric is focused on securing the outer core of the network, including all access methods, as well as extending security into the cloud and endpoint devices.

Extended Security—Security also needs to extend to common attack vectors, like email and the web, with a way to carefully and proactively analyze data and traffic for unknown and zero-day threats. This extended protection is a critical function of the Security Fabric and includes the Fortinet Advanced Threat Protection (ATP) solution, which includes FortiSandbox, as well as FortiMail and FortiWeb, designed to close the gap on the most common vectors for malware and data loss.

Global Threat Intelligence—Fortinet's Global Threat Research Team actively monitors the world's networks to find, analyze, and develop protection against known and unknown security threats. Their research delivers continuous, automatic updates for firewall, antivirus, intrusion prevention, web filtering, email, and anti-spam solutions.

Our global, proactive threat library enables comprehensive protection against network, content, and application threats, while our security research leverages intelligence from multiple security disciplines to protect against known and unknown threats. The results are converted into actionable, real-time intelligence designed to keep your defenses ahead of the capabilities of the cybercriminals.

Network and Security Operations—Fortinet's network security and analysis tools are designed to provide a more holistic approach to threat intelligence gathering, the synthesizing and correlating of threat data, and extending the ability to coordinate a threat response to fabric-ready and fabric-compliant partners. Fortinet technologies in this tier include FortiSIEM and the Fortinet suite of hardened network devices, such as FortiAP-U and FortiSwitch.

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 critical business infrastructures, architectures, and practices, organizations are looking for innovative network security solutions to help them embrace that evolution.

The Fortinet Security Fabric was designed around the principles of scalability and security, combined with high awareness and actionable threat intelligence, all resting on a series of open API standards for maximum flexibility and integration. When properly deployed, it provides the collaborative and adaptable protections today's organizations demand across their physical, virtual, and cloud environments.

For more information on the Fortinet Security Fabric, please visit our website.

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
Valbonne
06560, Alpes-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

Sep 20, 2016