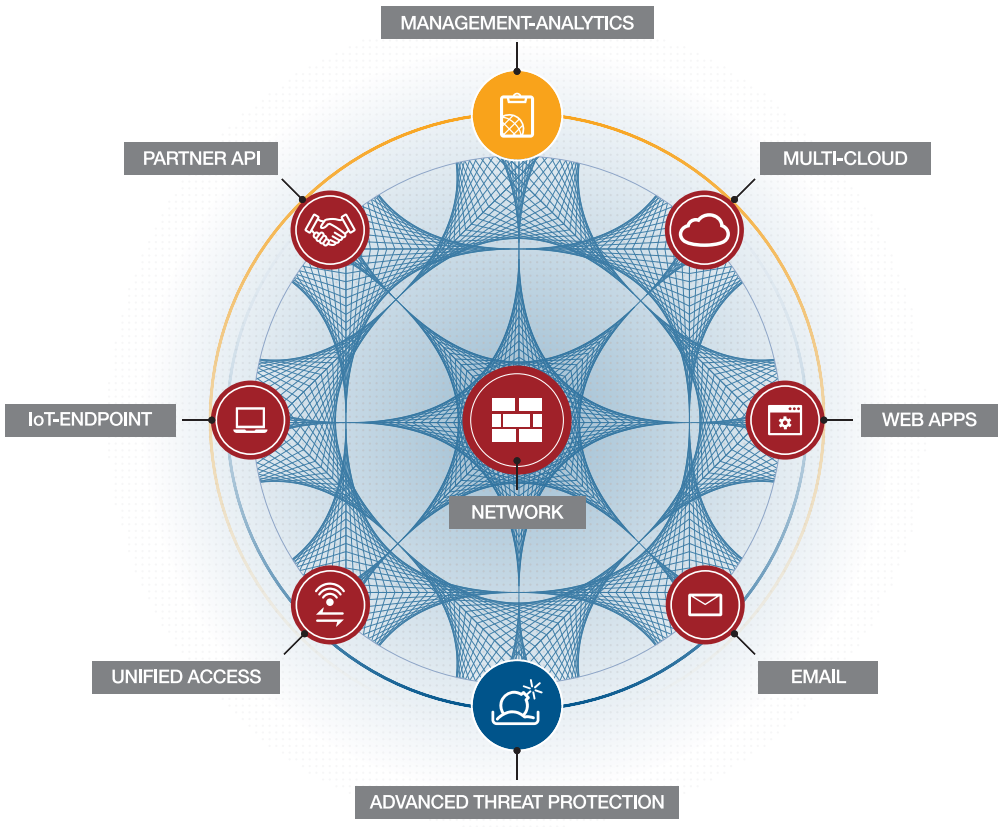
SECURITY TRANSFORMATION REQUIRES A SECURITY FABRIC

The growth and adoption of technology over the past several years has transformed businesses, governments, and even the economy. It affects how people interact socially, manage their finances, make purchases, perform transactions, receive news and entertainment, and even navigate their environment. It has also radically changed their expectations and attitudes as they interact with businesses and services, both as customers and as employees.

To remain competitive, organizations have had to respond by redefining how they participate in the new digital marketplace and meet the shifting demands of tech-savvy users. For most organizations, digital transformation involves the integration of digital technology into all areas of a business, resulting in fundamental changes to how they operate and how they deliver value to their customers.

To accomplish this, companies are having to weave together a variety of devices, technologies, and services into a single, integrated network that can dynamically expand and adapt as market and user demands evolve. This means simultaneously wrestling with issues such as IoT, SDN, OT, and multi-cloud environments, the proliferation of internal and customer-facing applications, unprecedented growth in both the speed and volume of data being generated and consumed, the expansion of workloads beyond the confines of the data center, and the expectations of the next generation of employees to blend their work and personal lives on any mobile device of their choosing combined with instant access to any data at any time from any location.



This digital transformation has simultaneously stretched IT teams to the breaking point while exponentially broadening the attack surface that needs to be protected. For example, multi-cloud environments mean organizations need to worry about an attack surface that may not always be visible to IT, and the convergence of IT and OT environments has now exposed things like manufacturing floors, industrial control systems, and critical infrastructures to new risks. The proliferation of IoT devices across these environments that rely exclusively on the access network for security has compounded these challenges.

At the same time that critical and proprietary business data is being moved into the cloud or managed through cloud-based applications and services, the growth of Shadow IT has resulted in organizations simply losing track of where data is located or what security measures are in place to protect it. BYOD complicates the issues of data governance even further, as users are able to access critical data from public locations and store it on personal devices that blend their personal and work profiles.

SECURITY TRANSFORMATION

As business and economic forces rapidly drive the evolution of the network, IT security teams have been struggling to keep up. A significant part of the problem is that digital transformation isn't happening as a single, integrated activity. Instead, it tends to happen organically through separate projects that move the needle a little at a time. The tendency is to secure each new network segment as it is developed, using the traditional security tools that are most readily available. Eventually, this results in a complex and largely accidental security infrastructure built around siloed solutions from separate vendors.

Unfortunately, complexity is usually the enemy of security. As different environments require different solution form factors, it can be difficult to standardize on a single vendor, as there can be wide variations between a physical, virtual, or cloud-based version of the same product, if they are even available. As a result, enterprises have now deployed an average of over 30 different security solutions across their distributed networks. Isolated security solutions with separate management interfaces and no meaningful way to gather or share threat information with other devices on the network can obstruct visibility and limit control.

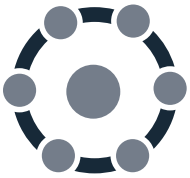
The best response to increasingly complicated networked environments is simplicity. That requires a security transformation that can keep pace with the digital one. Security transformation involves the integration of security into all areas of digital technology, resulting in a consistent and holistic security architecture that enables an effective security life cycle that spans across the entire distributed ecosystem of networks. This includes identifying the attack surface, protecting against known threats, detecting unknown threats, rapidly responding to cyber events in a coordinated fashion, and providing continuous trust assessments.

An effective security transformation strategy needs to include collaborative intelligence and system integration so local and global threat intelligence can be shared between devices and responses can be coordinated between solutions; the orchestration of unified security policies and enforcement; intelligent segmentation across physical and virtual environments for deep visibility into traffic moving laterally across the network, even across multi-cloud environments, and to quickly identify and quarantine infected devices; and automation to sift through growing network noise, correlate threat information, and respond in real time to any threat found anywhere along the extended attack surface.

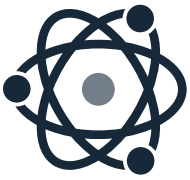
THE FORTINET SECURITY FABRIC

The Fortinet Security Fabric is an architectural approach that unifies the security technologies deployed across the digital network, including multi-cloud, endpoints, email and web applications, and network access points, into a single security system integrated through a combination of open standards and a common operating system. These solutions are then enhanced through the integration of advanced threat protection technologies and a unified correlation, management, orchestration, and analysis system.

This fabric-based approach to security is built around three keystones:



Broad. Visibility and protection need to extend across the entire digital attack surface. With data and workloads crossing between a variety of device form factors and network ecosystems, IT teams need a holistic view into devices, traffic, applications, and events and the ability to stop a threat anywhere along its attack chain. This approach needs to encompass and unify physical networks, IoT, mobile devices and users, and increasingly complex multi-cloud environments for both IaaS and SaaS solutions.



Integrated. The integration of devices using open standards, common operating systems, and unified management platforms enables the sharing and correlation of real-time threat intelligence. This common framework also supports the coordinated detection of advanced threats through sophisticated, centralized analytics that are difficult or impossible to achieve using traditionally isolated security deployments.

Automated. Like today's digital business, cyber crime happens at digital speeds. The time between a network breach and the compromise of data or systems will soon be measured in microseconds. Security systems need to automatically provide continuous trust assessment and then provide an immediate, coordinated response to detected threats. And because today's network environments are highly elastic, security needs to also be able to dynamically adapt as network requirements and configurations change.

To deliver these functionalities, the Fortinet Security Fabric is built around a number of key elements:

- *Network Security*. As networks continue to evolve beyond their traditional boundaries, sophisticated cyber attacks are being launched at the expanded attack surface, looking for soft spots and weaknesses. Fortinet's family of high-performance firewalls, built around a consolidated and integrated set of advanced security solutions, is the essential first line of defense of any organization.
- *Multi-Cloud Security*. The majority of organizations have adopted a multi-cloud strategy, including multiple IaaS providers and over a dozen different SaaS solutions. The expansion of data and workloads into a distributed cloud environment makes consolidated security prevention and detection difficult. Fortinet's integrated virtual and physical cloud solutions, powered by the Fortinet Security Fabric, extend seamless security across your distributed cloud deployment, including being the first to provide advanced security solutions for all five of today's top cloud service providers.
- *Web Application Security*. Unprotected or vulnerable web applications are common entry points into your network. The FortiWeb web application firewall uses the latest detection and protection technologies and advanced intelligence to protect web applications from sophisticated attacks.
- *Email Security*. Email continues to be the primary entry point for malware to infect your network. Email spammers and phishers use infected attachments, malicious links, and sophisticated scams to trick users into clicking on or executing malware. In fact, email was the primary vector for ransomware in 2017. The FortiMail secure email gateway inspects incoming and outgoing email, blocks malicious messages and attachments, and prevents sensitive information from being leaked.
- *Secure Unified Access*. Most wireless access points provide connectivity, but little in the way of real security. But as more and more devices require wireless network access, securing business communications, personally identifiable information (PII), mobile devices, and a variety of users demands much more than simple access control. Fortinet's secure access solutions deliver with high-performance access combined with comprehensive security and application control for secure Wi-Fi that is fully integrated with your network security protocols and policies.

- *Endpoint Security*. Networks need to support a highly mobile workforce and a growing array of personal endpoint devices connected to the network. Not surprisingly, these devices are another common entry point for threats. The challenge is that endpoint solutions often don't share threat intelligence with the rest of the network, which can impede determining if a device is infected and slow down threat response if they begin behaving badly. FortiClient allows IT teams to integrate a layer of automated endpoint security into the Security Fabric for faster and more comprehensive network protection.
- *Advanced Threat Protection*. Today's advanced threats are designed to evade detection through multistage attacks, complex attack vectors, and by observing and mimicking legitimate applications and traffic. FortiGuard Threat Intelligence helps companies combat these advanced threats by automatically delivering real-time intelligence about newly detected threats directly to their security solutions, while Fortinet sandboxing solutions detect unknown threats and then isolate and inspect any suspicious files detected by devices on the Security Fabric.
- *Management and Analytics*. In a large and highly elastic network, visibility and control are more important than ever. IT teams need to be able to see and understand threats and events regardless of where they occur across the distributed network. But this can be a huge challenge for enterprises that have deployed isolated security products. Fortinet solutions for logging and reporting, SIEM, and centralized security management collect and correlate data from your Fortinet and Fabric-Ready security products, providing the critical visibility and granular control necessary to efficiently manage security processes and orchestrate automated responses.

A SOLUTION DESIGNED FOR TODAY'S DIGITAL ENTERPRISE

Digital transformation is the biggest challenge that IT security teams have ever had to face. As the evolution of computing and networking continues to drive changes across critical business infrastructures, architectures, and practices, organizations require an innovative security transformation approach that enables them to embrace those changes.

Once traditionally isolated security solutions are combined into a unified Security Fabric framework, organizations can see deep into the distributed network to detect advanced threats, dynamically adapt to the evolving network architecture and threat landscape, and leverage the continuous trust assessment that today's digital enterprises require, from core to cloud.

Click here for more information on what the Fortinet Security Fabric can do for your organization.

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
06560 Valbonne
France
Tel: +33.4.8987.0500

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

LATIN AMERICA HEADQUARTERS
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel: +1.954.368.9990

171575-A-0-EN June 1, 2018 1:20 PM

Mac:Users:susiehwang:Desktop:Egnyte:Egnyte:Shared:Creative Services:Team:Susie-Hwang:Egnyte:Shared:CREATIVE SERVICES:Team:Susie-Hwang:WP-Fortinet-Security-Fabric:wp-fortinet-security-fabric Folder:wp-fortinet-security-fabric