THE FORTINET SECURITY FABRIC

The collection and distribution of data is the new currency of business. Its growth is completely transforming networks. It is driving the explosion of IoT and other connected devices, the expansion of the network into the cloud, the increase in hyperconnectivity between networks, and the emergence of the new digital economy.

This transformation is also having a dramatic impact on cyber security. Traditional security models were never designed to protect today's increasingly distributed and highly flexible networks. But as networks and data converge, the failure of security to adapt to these changes could be devastating.

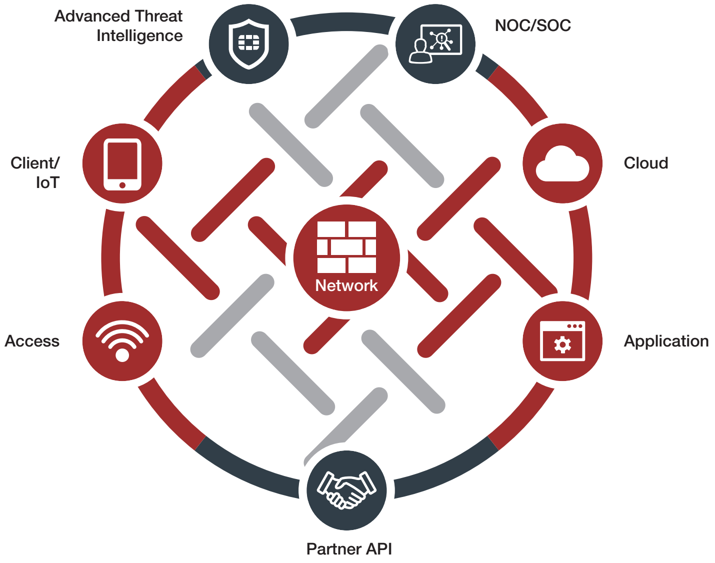
To meet today's advanced networking and security requirements, security can no longer function as a set of discrete security tools operating in isolation. To meet the demands of today's networks, effective security requires:

- Integration—Traditionally isolated security and network tools now need to work together as a single system to enhance visibility and correlate and share threat intelligence across the expanding network.
- Synchronization—Security tools need to work as a unified system to enable single-pane-of-glass management and analysis and to enable a coordinated response to threats through such things as identifying and isolating affected devices, updating rules, enforcing policies, and removing malware.
- Automation—In order for security solutions to adapt to dynamically changing network configurations and respond in real time to detected threats, security measures and countermeasures need to be applied automatically.

The Fortinet Security Fabric enables organizations to connect distributed and isolated security solutions into a unified architecture, allowing them to more easily adapt to and defend the network's rapidly changing attack surface. It integrates security for the endpoint, access layer, network, applications, data center, content, and cloud—whether from Fortinet or from the growing number of Fabric-Ready third-party vendors—into a cooperative, synchronized solution that can be managed, analyzed, and orchestrated through a unified management interface and automatically respond to threats in real time anywhere across the distributed network.

It is able to do this because the Fortinet security solutions being tied together through the Security Fabric have been designed around a common operating system, FortiOS, to simplify management and control. It also supports open application programming interfaces (APIs), open authentication technology, and standardized telemetry data to integrate existing solutions from a growing list of Fabric-Ready partners, along with those from other vendors built around APIs.

This fabric-based approach allows IT teams to see every device on the network, actively collect and share threat information to improve visibility and intelligence and enhance situational awareness, and automatically distribute mitigation to enable a synchronized attack response from end to end.



WHITE PAPER

The Fortinet Security Fabric provides three essential functions necessary to protect and defend today's networks:

1. Broad

Comprehensive visibility across the distributed enterprise ties together data, applications, devices, and workflows. Awareness of each network element and automated correlation of data enable administrators to find and respond to even the most sophisticated threats. Such broad deployment and deep visibility aids in compliance, helps monitor internal traffic and devices, prevents unauthorized access to restricted data and resources, and controls the spread of intruders and malware.

2. Powerful

As the speed of business continues to accelerate, the volume of data needing inspection grows, and threats become increasingly sophisticated, security not only needs to be pervasive but also extremely powerful. Organizations cannot afford to choose between performance and protection.

Fortinet's physical security solutions are built using the fastest, custom-designed security processors in the industry. And for virtualized environments, software versions of these technologies have been highly optimized, allowing them to run several times faster than competitive solutions. This allows organizations to establish comprehensive security without affecting performance. When integrated through the Security Fabric, both physical and virtual security technologies can be woven together to scale policy and enforcement across your entire distributed network, allowing you to more effectively secure your evolving network environment.

3. Automated

Because an attack can compromise a network in minutes, visibility and performance aren't enough. Security solutions not only need to correlate threat intelligence to determine the level of risk but they also need to automatically synchronize a coordinated response in order to stop a threat anywhere it is found. The Fortinet Security Fabric framework allows the network to automatically see and dynamically isolate affected devices, partition network segments, update rules, push out new policies, orchestrate policy enforcement, and remove malware.

The Fortinet Security Fabric allows security devices to dynamically adapt to changing network configurations, see and correlate intelligence collected from across the entire distributed landscape, and automatically establish and enforce policies as the environment being protected adapts to shifting business needs at the speeds today's businesses require, anywhere along the attack surface, from remote devices to the cloud.

FORTINET®

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

70906-0-A-EN **April 17, 2017**