# ADVANTAGES OF A FABRIC VS PLATFORM APPROACH TO ENTERPRISE SECURITY

**One of the challenges many organizations face when considering upgrading or expanding their security infrastructure is simply wading through the sometimes-confusing language and nomenclature being invented by security vendors and manufacturers to describe new technologies and strategies.**

Far too often, security tools are wrapped in marketing language that doesn't always effectively communicate—or sometimes, even intentionally obscures—what a device or tool are able to do. Visit any security trade show and you are going to be overwhelmed by devices claiming to be "cloud enabled" or that offer "advanced threat intelligence." But what do those terms mean? The same is true for entire classes of products. Web application firewalls, for example, sound like a good idea, but there is no industry consensus on what features and functions such a tool should provide. So you have to know what you need and do your homework.

Of course, when an organization is trying to get out ahead of the market and truly innovate, they have no choice but to find new language to describe what they have developed. Often, however, it's not the company that invented the technology that gets the credit, but the one that coins the phrase that gets adopted by the marketplace. An excellent case in point was the term "next-generation firewall" (NGFW). Of course, the technology behind this category of device had been around for a long time. For example, there was, and still is, very little difference between an NGFW and a UTM (unified threat management) device. But someone coined the term, grabbed a lot of media attention and market share, and to keep up, a whole new class of security technology was off to the races.

The challenge, of course, was that there was no standard for what functions an NGFW solution needed to provide. Pretty soon, there were dozens of them from a variety of vendors, ranging from sophisticated systems of integrated technologies to isolated solutions that happened to be wrapped in a single casing of sheet metal to simply traditional firewalls with a few bells and whistles added and a shiny new next-gen firewall label slapped on the box. Fortunately, third-party testing labs came along, set some standards, and helped sort out the confusion.

The same is now true for two new ideas currently competing for space in the marketplace. They are the security platform and the security fabric. Each claims to be the next generation of network security and, on the surface, both seem to try and solve the problems of expanding network environments, increasingly sophisticated threats, and the need for different security technologies to work together to more effectively protect the network. But in reality, they are very different. Let's take a look at these two different approaches and see what they actually mean.

## THE SECURITY PLATFORM

When possible, it always helps to start with some basic definitions. Fortunately, the word "platform" has been used by the tech industry for a long time. In general, a platform is a single environment, usually hardware, on which different point products can be deployed or different applications can be executed, and where everything can generally be managed through a single interface. A smartphone or a laptop, for example, is a platform.

A security platform is no different. In reality, next-gen firewalls with some added interoperability are almost always what organizations really mean when they claim to have a security platform. They usually combine such things as firewall, IPS, antivirus/anti-malware, application controls, and VPN solutions from a single manufacturer into a single device. They are deployed in a single location and only inspect and secure the traffic that passes through them. The biggest difference is that these devices can communicate with each other to share management and threat information.

Just like NGFWs, security platforms are usually deployed at the edge of the network and control traffic moving north and south past a predefined demarcation point or security zone.

## THE SECURITY FABRIC

A security fabric, on the other hand, is fundamentally different from a platform. Rather than being a product or set of products wrapped in a box, a fabric isn't actually a product at all. Instead, it is an architectural approach to security, enabled by open standards and protocols, which allows you to connect different security devices—including security platforms—into a single, integrated security system that spans across your distributed network.

In addition to integrating the technologies usually included in a platform, a security fabric needs to include multi-cloud security, IoT and endpoint protection, secure access points, email and web security, advanced threat protection, management and analytics tools such as SIEM, third-party security devices and technologies, and even leverage the security and intelligence built directly into network devices.

A fabric-based security framework also allows you to seamlessly connect security solutions deployed across highly dynamic

and distributed environments into a single, integrated security ecosystem, not only at the perimeter but also in the data center, campus, cloud, branch offices, IoT and edge devices, parallel networks (IT, OT, and IoT), and anywhere else the business might have assets or people. The proper placement of appropriate security tools, combined with dynamic network segmentation, allows IT teams to integrate new and previously deployed security resources into a single, coherent security system.

## FABRIC VS. PLATFORM

Many platform security vendors position themselves as having an end-to-end solution. One of the challenges of security platforms, however, is that they start with a specific security element, such as a next-generation firewall, and then bolt on other security tools on an as-needed basis. This leads to some challenges and gaps in security, such as:

- **Cost:** A platform-based approach means that, regardless of which technologies you want to deploy, you have to purchase hardware designed to accommodate all of them, which isn't cheap. It also means that you are either paying for processing power that is lying dormant when a particular function isn't needed, or for processing power that drops to its knees during traffic spikes and surges.
- **Scale:** Networks are increasingly dynamic and distributed, and security technology needs to scale dynamically. Because platform devices are built around a static hardware configuration, they scale by either replacing existing platforms with newer, higher-performing ones or by adding additional platforms, regardless of which function you need in a particular location. And as you enable additional features or consume spikes in traffic loads, platforms tend to dramatically lose performance.
  A security fabric approach, however, can incorporate a variety of technologies, including specially engineered hardware designed for today's escalating traffic demands, virtualized solutions that are available on demand, single, purpose-built devices for those places in the network where you only require certain types of inspection, as well as offloading surges in traffic onto other devices.
- **Visibility:** Because platforms are made up of predefined bundles of technologies deployed in a single location, they often have blind spots. For example, specialized security technologies from other vendors may be seeing and collecting data that can't easily be shared with the platform. Furthermore, the "bolt together" strategy of the platform rarely provides a holistic and integrated management interface. The reality is that most platforms have different dashboards and methods for collecting data that limits the availability of real-time visibility because threat information and policy orchestration still need to be managed by hand.
  A security fabric approach leverages all deployed security devices, even those from third-party vendors, into an integrated whole. Open standards and application programming interfaces (APIs) mean that data can be easily collected, shared, and correlated, and automated policy changes and responses to threats can be synchronized between devices across the distributed network ecosystem.
- **Open/Closed:** Third-party integration is tough with platforms because each product in the umbrella is often built around proprietary protocols and interfaces. This limits visibility, control, orchestration, and response.
  The security fabric, on the other hand, is designed around a series of open APIs, open authentication technology, and standardized telemetry data, which allow organizations to integrate existing security investments.

By blending together next-generation detection and response systems, intelligent network segmentation, and single-pane-of-glass orchestration, a security fabric is able to see and respond to today's most sophisticated threats, while dynamically adapting to evolving network architectures. It enables solutions to actively collect and share threat information to improve visibility and intelligence and enhance situational awareness, and automatically distribute mitigation instructions to broaden and deepen a synchronized attack response from end to end.

The Fortinet Security Fabric is the first architecture designed to address and adapt to the security challenges of today's complex and distributed networks. And we are actively engaged in improving and expanding the power and functionality of the Security Fabric. The recent FortiOS 6.0 release, for example, expands the power of the Security Fabric with unprecedented visibility, including a single, comprehensive view of the network, and deep integration between traditionally isolated security devices, while automating controls even more with the security fabric audit that monitors the best practices of the entire distributed fabric and provides the compliance alerts for a continuous trust assessment.

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



February 12, 2018 12:56 PM
wp-advantages-of-a-fabric-vs-platform-020918-1256pm