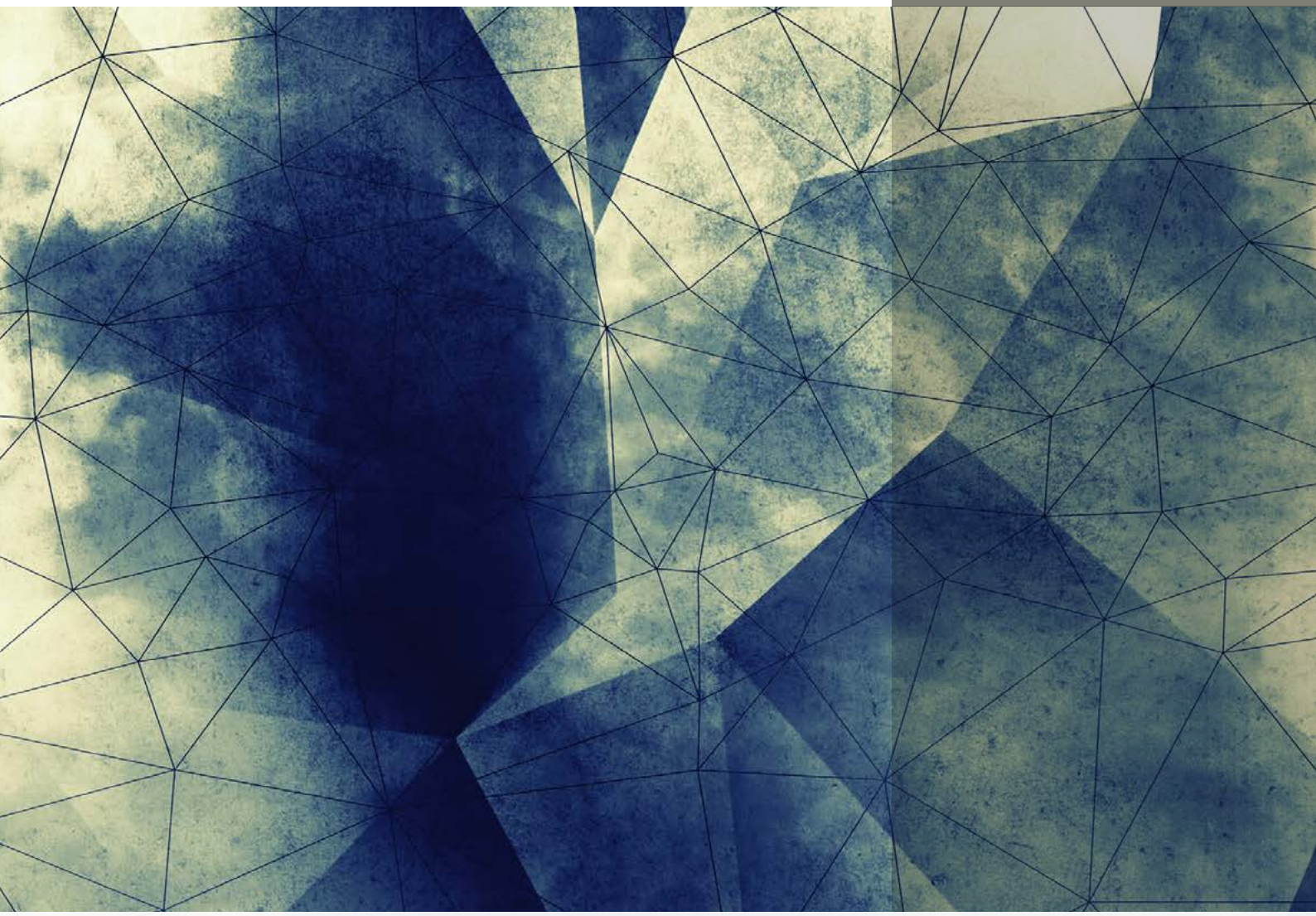
FORTINET

WHITE PAPER



A New Approach to Securing the Enterprise Network

Table of Contents

Executive Summary 2
The Need for a Change 3
The Foundation of a Holistic and Adaptive Security Approach 3
Taking Security Deeper into the Network 4
Cutting the Cord – Without Cutting the Safety Net 6
Solution Management Advantage 6
Enabling the Enterprise Transformation - the Human Element 6
Security Without Compromise 7

Executive Summary

Much has been said and written about the challenges that enterprises face today in light of the increased level of threat activity and the level of sophistication of the threats themselves. With disclosure of yet another high profile data breach happening with alarming regularity, what can an enterprise do to protect itself? Is technology unable to respond to these new threats?

Perhaps what we are seeing are the consequences of information technologies being deployed without sufficient regard to security rather than an inherent weakness in the technologies themselves. If that's the case, then this should be considered as a clarion call to rethink how to secure the enterprise.

There is not just one way to apply security to a network and different organizations will take different approaches depending upon need and budget. For some organizations such as banking and retail, regulatory compliance such as PCI-DSS is a key driver. While PCI-DSS compliance is certainly a key consideration for these verticals, security should not stop at meeting what are relatively generic requirements. Other organizations will take it a step further by performing a risk assessment and assign security spend according to probabilities. This approach goes further than just compliance but the potential risks that an enterprise faces change on a near daily basis making the accuracy of an annual risk assessment questionable. Finally there is the "point product" approach, deploying key products from different vendors, under the assumption that each product is considered to be the best in its category. Although the best of breed approach has been considered the most comprehensive, a very practical issue is the increase in complexity and cost of managing such a collection of sophisticated and complex products.

The purpose of this paper is to introduce a new concept to implementing network security, a concept that is based on three defining principles:

- **HOLISTIC – AN END-TO-END** approach from the datacenter to end point and beyond, able to react to threats through integrated prevention, detection and remediation capabilities
- **COLLABORATIVE – SOLUTION ELEMENTS WORKING TOGETHER** combined with the ability of the network to gather and share real-time threat intelligence
- **TRANSFORMATIVE - CHANGING** the enterprise network from a collection of boxes to a platform combining technology with human expertise

A second issue facing enterprises is the erosion of a clearly defined network perimeter. Changes in technology and how business uses technology has resulted in a borderless attack surface, increasing the likelyhood of a successful attack and subsequent data breach.

Fortinet believes that it's time to change how network security is regarded and more importantly how it's actually implemented. The role of the network in an enterprise's business strategy is more important today than ever before. Not securing this critical asset against a sophisticated and ever-changing threat landscape is a risk most organizations cannot afford to take.

The Need for a Change

Why has network security become so important so quickly? During the past 20 years or so, enterprises have made transformational changes or created entirely new business models, business models that weren't even imaginable before through the use of technology. Technology turned business on its head – the finished product was no longer the most important piece of the puzzle. It has been replaced by information – mountains of data that can be analyzed over and over again by the enterprise to drive business forward. Datacenters and websites have been transformed from cost centers into critical business assets. But a robust and secure network is required to make all of this work. If customer data is the pinnacle of the pyramid, as shown below, then the underlying network is its foundation (Fig. 1). The question is whether the foundation has too many cracks, putting that data at risk.

With business expansion as the primary driver of network growth, the first requirement for the network was to support the business. Security, although always present to some degree, was often an afterthought comprised of some base level capabilities "bolted" onto the network. Over time however, this security model has shown to be inadequate.

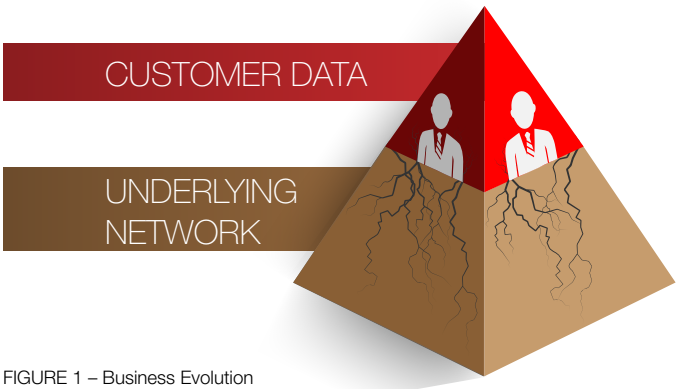


FIGURE 1 – Business Evolution

Insufficient security, too many exploitable gaps, and human creativity in crafting effective malware malware has come together in a perfect storm that has overwhelmed the enterprise.

The Foundation of a Holistic and Adaptive Security Approach

No network security structure will keep 100% of the malware out of the network 100% of the time. The objectives then are to block as much malware as possible from entering the network, detect any intrusions into the network as quickly as possible, and ensure the most key assets are protected in the event of an attack. So, how to achieve these objectives?

At Fortinet it starts with the philosophy that security must be integrated into the fabric of the network infrastructure. This automatically reduces or even eliminates the gaps between the two layers and starts to close the hacker's window of opportunity. But just placing technology, even if tightly integrated into the network infrastructure, isn't enough to combat today's threat landscape. These technologies – deployed at the core, in branch offices, on desktops – must work together with a common foundation that brings them together as a single solution.

Fortinet places the right technology in the right places throughout the network – FortiGate next generation firewall, FortiWeb Web Application Firewall (WAF), FortiMail Secure Email Gateway (SEG), FortiSandbox network sandbox and FortiClient EndPoint Protection (EPP) client software (Fig. 2). What differentiates the Fortinet approach from legacy approaches is that all of these technologies are underpinned by a common threat intelligence capability from Fortinet's FortiGuard Labs. Each of these products has one or more security services running on them; some are essential to their operation such as anti-spam in the SEG while others are designed to improve their security effectiveness such as antivirus or intrusion prevention in the FortiGate. Compared to a legacy fragmented point solution approach, each individual vendor will have their own threat intelligence. The issue is that each product's security efficacy will vary and exploitable gaps will develop. Since there isn't only one attack vector, malware that may be blocked by a firewall could successfully enter the network via a compromised website or as an attachment or URL in a phishing email. The different security services in the Fortinet approach are kept up to date and synchronized by FortiGuard Labs, eliminating any gaps from developing between products. FortiGuard Labs is at the center of the Fortinet ecosystem, receiving real-time threat intelligence from millions of sensors and other sources from around the world. This information is augmented by the advanced

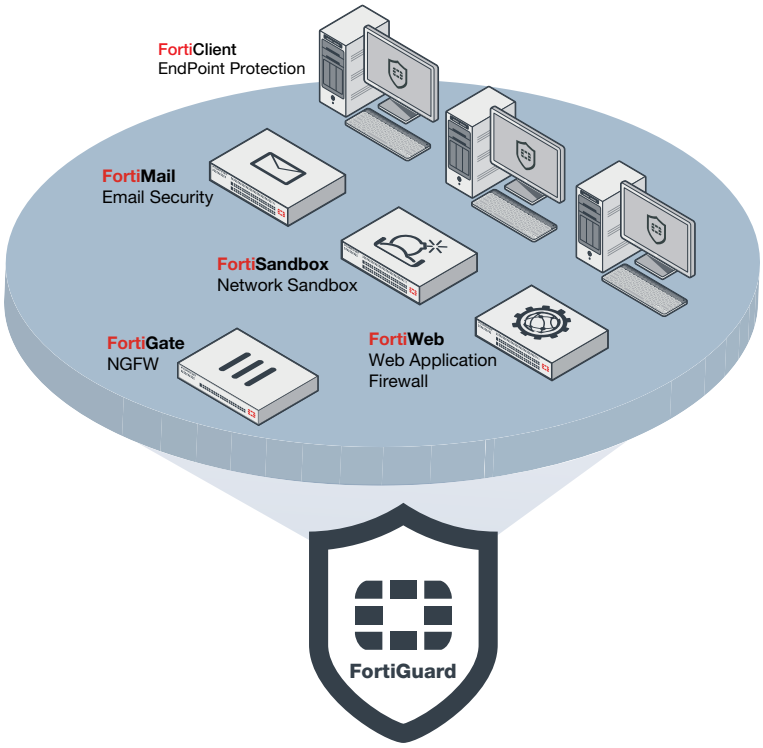


FIGURE 2 – Security Throughout the Network

threat research and discovery of "zero day" vulnerabilities also conducted by that team of cyber experts. The output of FortiGuard Labs is constant updates to the different services running in the Fortinet appliances – updates originating from a single source to eliminate gaps in between the different appliances.

To further eliminate any possible gaps, these products are designed to work together as a single solution, providing the network with the ability to prevent the entry of malware into the network, detect when malware has entered the network and provide key mitigation functions to minimize any damage from the attack and ensure that the solution is updated to protect against future attacks.

Fortinet security integration gets even tighter with its sandboxing technology. Here, a critical aspect to take into consideration is how the sandbox interacts with the other security elements in the network. The blunt force approach is for the sandbox to continuously look for malware samples, putting everything that it finds through its process. The issue with this approach is time. Between the time of the intrusion and when the sandbox detects the malware could be in hours, hours that the malware could have used to spread throughout the network. Fortinet's approach is a tight integration between the sandbox and the other technologies in the network. The technologies that make up the prevention layer act like a pre-filter, blocking a large part of the malware from entering the network. Suspicious samples are then passed onto the sandbox for analysis. If a sample is found to be malicious, the sandbox can communicate to the other elements of the solution so that specific actions can be taken, initiating the first steps of mitigation.

> Through the use of various technologies designed to work collaboratively and supported by real time threat intelligence, the Fortinet solution provides a depth to the network's ability to defend itself from attacks, a depth that a traditional preventive only approach cannot provide.

Taking Security Deeper into the Network

While Hollywood has created a popular image of network attacks always taking place in what they imagine as a data center filled with computers, in real life an attack can happen anywhere in the network. The network should be thought of as a series of concentric circles with the core of the network in the center (Fig. 3). Because of cost considerations, security is typically centralized at the core. As the circles expand

FIGURE 3 – Increasing threat risk

outward, from the core to the branch offices to the individual desktops and beyond, the number of potential attack points increases exponentially. The consequence is that further away from the core of the network, the greater the likelihood of an undetected network intrusion.

To combat this vulnerability, a common practice has been to deploy security throughout the network. Firewalls - deployed at branch offices and remote locations, at the edge of the enterprise campus, at access points to cloud based resources and within the data center itself - effectively segment the network into secure cells (Fig. 4). Where this strategy falls apart is when products from different vendors

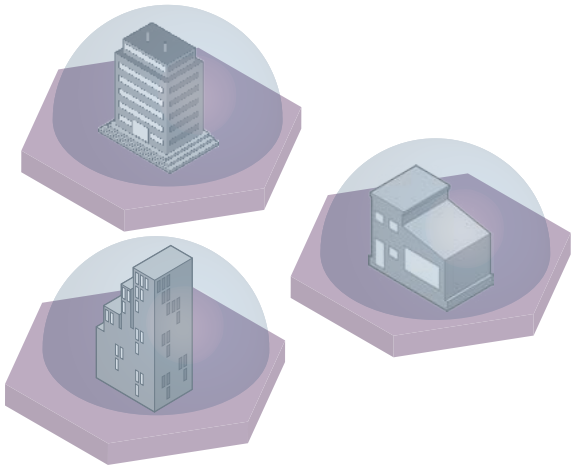


FIGURE 4 – Segmented but not Secure

are mixed together, choosing one vendor for the data center, another for the campus and finally a third for remote sites. While each individual product may work to expectation, each individual product is essentially an island, making the task of managing security policies across the network difficult and time consuming.

Fortinet is able to overcome these issues through FortiOS, the common operating system powering every FortiGate. Regardless of where it's deployed in the network, the common functionality of FortiOS distributed throughout the network gives enterprises a win-win environment - a more secure network through internal segmentation and consistent security policies across the whole of the network. FortiOS is also the engine for all of the different security services supported by FortiGate, ensuring that the entire network is protected equally (Fig. 5).

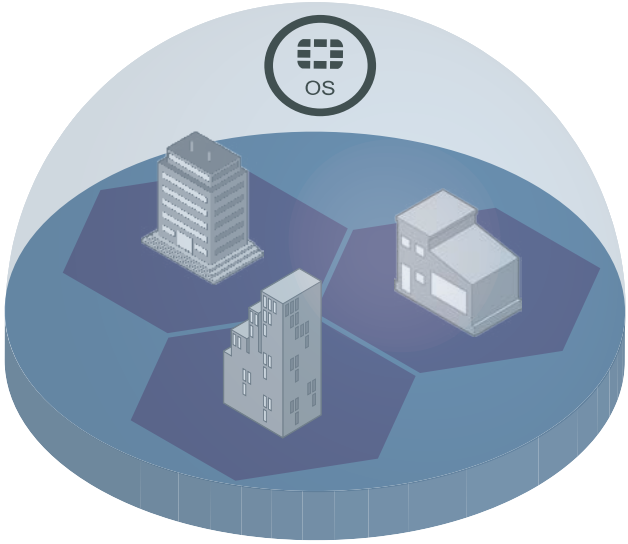


FIGURE 5 – Protection by FortiOs

But this segmentation is still focused on the perimeter of the network and does nothing when a hacker is able to enter the network undetected, particularly when valid but compromised login credentials are used. Sandboxing is a possible solution to this problem but until the hacker implants actual malware into the network, there's nothing that can be done to stop their movement in the network - Until now.

Fortinet believes that it's time to extend the concept to segmentation to inside of the network. While networks have long implemented the concept of segmentation, it was done for networking purposes and would not prevent malware or a hacker from moving freely around the network. The solution to this problem is the Internal Segmentation Firewall (ISFW).

The concept behind the ISFW is the use of an enterprise grade firewall that is deployed inside the network as close to the users and applications as possible. In both the enterprise campus and data center. The close proximity to users and applications is a key factor as to how much the risk of lateral movement can be minimized. Another is the alignment of security policies to user identification. With security policy tied to user identity, it would be easy to create a policy preventing users from accessing parts of the network not relevant to their normal work. For example, a user on the Finance VLAN is trying to access the Engineering Development VLAN. With an ISFW in place, a hacker trying to move from the initial point of intrusion – in this case the Finance Department – to the Engineering Development would be blocked by the firewall and alarms generated to indicate what had happened (Fig. 6).

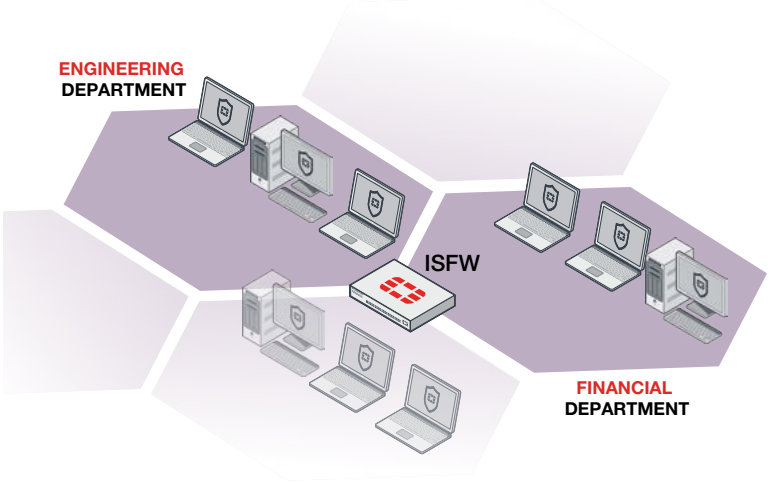


FIGURE 6 – The solution: ISFW

ISFW has triggered an evolution beyond multi-function security to multi-layered security, thus requiring high-speed security appliances. Leveraging its FortiASIC technology, Fortinet has a strong and differentiated advantage here given our ability to provide the deep security at 10, 40 and 100 gigabit line speeds that internal networks run at. Fortinet's ISFW approach delivers continuous visibility and protection of the network from the inside out, shortening the window of exposure and limiting potential damage.

Cutting the Cord – Without Cutting the Safety Net

Wireless technology has moved from a convenience feature to a "must have" in today's modern enterprise, whether for internal use or to provide a better customer experience. But the challenge is to offer a unified access environment without compromising security. The traditional branch office wireless network is an overlay – that is the wireless network is independent of the underlying network infrastructure. While the wireless network offers security in the form of access control, Wi-Fi Protected Access (WPA and WPA2) for example, this is not the same as network security. What is needed here is a common security framework for all users, regardless of the access method.

In Fortinet's Secure Access Architecture, the wireless network is an extension of the FortiGate itself. In addition to the access control and security features found in typical wireless networks - WPA - all network users are subjected to the same authentication and policy measures. Authentication can be done locally by the FortiGate or via external systems such as RADIUS or Active Directory. Two Factor Authentication (2FA) can also be implemented to minimize the risk from valid, but compromised login credentials. Users, once identified and authenticated, can only access those network resources defined in their policy. Since their network access is via the FortiGate, the chance of malware entering the network is severely minimized.

End-to-end security, End-to-end control

Along the various elements of the deployed solution collaborating with one another, another key element of adopting a proactive approach towards security is centralized security management & analysis. With so much going on in the network, comprehensive tools are needed to help correctly configure the different elements of the solution and cut through the clutter and provide a clear view of the network. The Fortinet solution includes a single pane of glass network management approach, FortiManager, so that configuring individual products, defining policy based provisioning, update management and end to end network monitoring is a straightforward process. FortiManager's Graphical User Interface, (GUI), is designed so that within a few clicks, the network administrator can drill down to the level of detail needed to understand alarms and other events taking place in the network. Once the network is installed and configured, the next objective is to understand what is going in the network, to turn a collection of alarms and events into clear view of the network's station. FortiManager seamlessly integrates with FortiAnalyzer to provide in-depth discovery, analysis, prioritization and reporting of network security events.

Enabling the Enterprise Transformation - the Human Element

Implementing and maintaining network security is not a "one and done" effort. Enterprises should constantly be testing their security solutions and taking advantage of professional services available from their technology partners. Not all enterprises have the full range of knowledge and skills in-house across all security technologies to ensure that those are configured and deployed correctly. Vulnerability testing and assessments, configuration reviews and training are all steps that can be taken to ensure that the technologies deployed in the network are done so correctly and are not "back doors" waiting to be exploited. Incident response is another service that the enterprise can take advantage of, leveraging the skills and knowledge of the technology providers to supplement those of their internal staff. Fortinet works closely with its customers to provide such services and introduce new ones to address the changing market. Fortinet also offers a range of premium support services that focus on several specific areas to enhance the value the organization receives – Proactive, Continuous Improvement and Collaboration. These services, such as dedicated Technical Account Manager (TAM), enhanced Service Level Agreements and upgrade and lab pre-staging to ensure that the Fortinet solution meets the needs of the enterprise, throughout its lifecycle.

Security Without Compromise

Considering the relationship between today's enterprise and the technology that drives it, focusing on securing the IT infrastructure should be considered fundamental. But too many enterprises still regard security as a questionable expense rather than a strategic investment. An enterprise waiting for a data breach to happen before examining its current security posture is akin to locking a house after it has been already broken into.

Fortinet has two key objectives - to be at the forefront of the effort to change the mindset towards enterprise security and to be the organization's trusted partner in guiding them through this transformation.

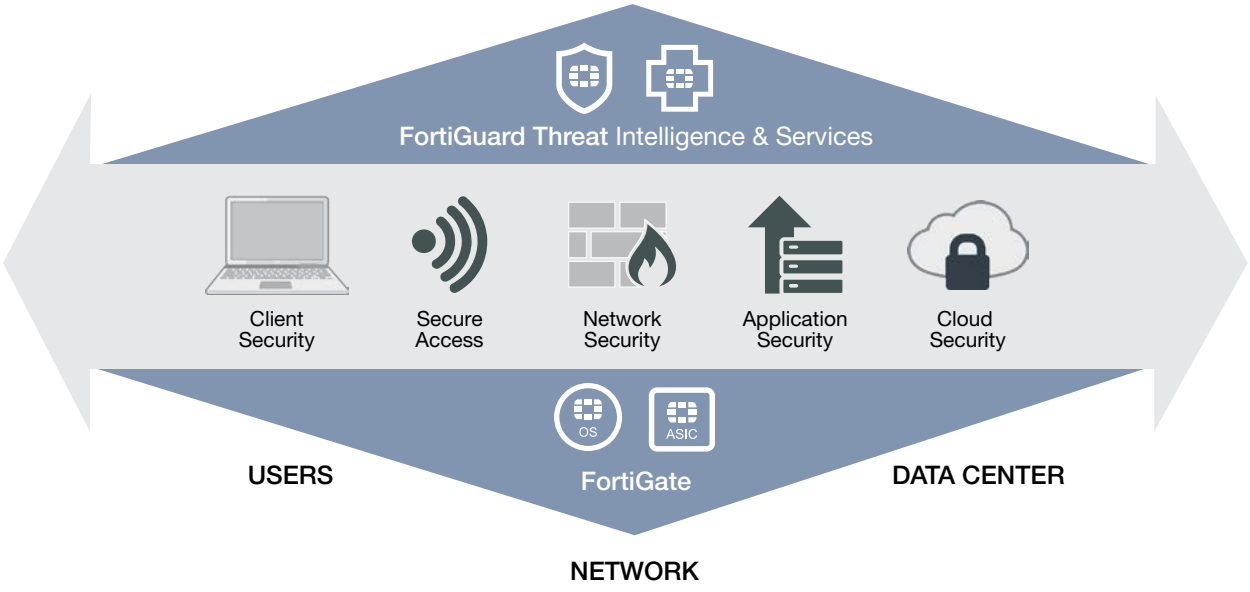
> The network must be seen from a holistic perspective, that the network is a single entity. The right technology must be positioned in the right place to improve the network's ability to detect attacks and defending itself throughout the lifecycle of the threat.

In order to increase threat detection capability, technology must be supported through continuous and relevant threat intelligence, intelligence that the technology can leverage to take specific actions and improve its security efficacy.

Fortinet can enable this new philosophy of network security through the breadth and depth of its product line – products designed for each functional area of the network and products designed to work together. The response is not just a local action as the Fortinet solution is designed to work collaboratively and take automated and proactive actions. Each action that is taken is fed back into the threat intelligence ecosystem to strength the overall solution, automatically and consistently.

Completing the picture is human intelligence and intervention, supporting both the technology and the enterprise's own human resources. Combining their human expertise, Fortinet and the enterprise work together to remove the weak links in the organization, increasing the enterprise overall defense capabilities.

As the threats that enterprises are facing on a daily basis continue to increase in volume and sophistication, enterprises must change how they think about network security. Fortinet is there to work with the enterprise to transform and evolve its approach to network security from reactive to one that is adaptive, holistic and collaborative and combines the best of technology with human capability.



SEAMLESS
Seamless end-to-end, consistent threat posture

INTELLIGENT
Intelligent protection from the inside out, with full visibility across the attack surface

POWERFUL
Power and performance for today – and into the future

www.fortinet.com

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, Sophia Antipolis,
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
Prol. Paseo de la Reforma 115 Int. 702
Col. Lomas de Santa Fe,
C.P. 01219
Del. Alvaro Obregón
México D.F.
Tel: 011-52-(55) 5524-8480