FORTINET ADVANCED THREAT PROTECTION

Broad and Automated Security Coverage for your Expanding Attack Surface

INTRODUCTION

SOPHISTICATED ATTACKS YIELD BIG REWARDS

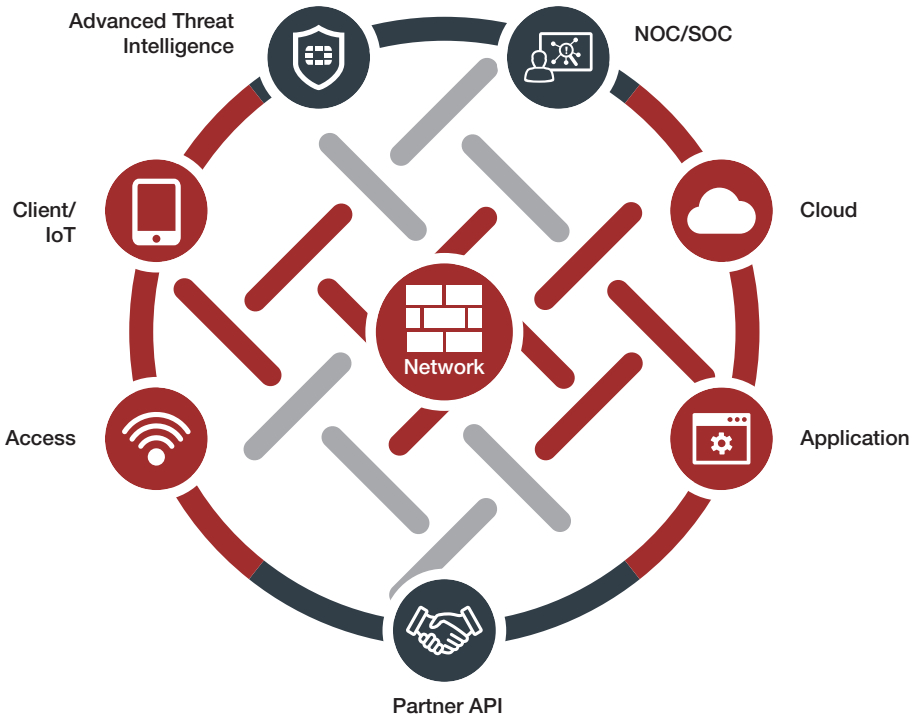
Securing today's enterprise is more challenging than ever. Whereas in the past there was a well-defined perimeter to secure, the rise of the Internet of Things (IoT) following mobility and BYOD, as well as the continued adoption of public following widespread adoption of private cloud services, results in a much more diverse and dynamic attack surface to be protected.

At the same time, the threat landscape continues to evolve in regard to both volume and sophistication as cyber crime has achieved big business status and maturity. Powered by a robust cyber crime ecosystem that includes a growing segment of "malware-as-a-service" providers, our FortiGuard Labs saw more than 700,000 intrusion attempts by the close of 2016, with 120,000 pieces of malware and 25,000 spam messages—every minute of every day. Further, in Verizon's 2016 Data Breach Investigations Report, the malware at the heart of incidents lived for only 58 seconds or less and was seen only at the compromised organization in nearly all cases. Most importantly, regardless of whether the result of a volume-based or targeted attack, a recent Fortinet Threat Landscape publication reported that the average organization has been successfully compromised with more than six active bots communicating out to cyber criminals.

That's why Fortinet is pioneering a new approach to security, our Fortinet Security Fabric, which includes specific components recommended to address today's advanced threats.

THE FORTINET SECURITY FABRIC

With so many potential ways for cyber criminals to gain entry into the dynamic enterprise, it is important to design and implement a security architecture that is broad enough to cover the entire attack surface. Further, it is critical to have security components that are powerful enough to enable all the technologies appropriate at each protection point without slowing networks or employees. And finally, it must be automated and work as a single, cohesive system to keep pace with the changing and fast-moving threat landscape.

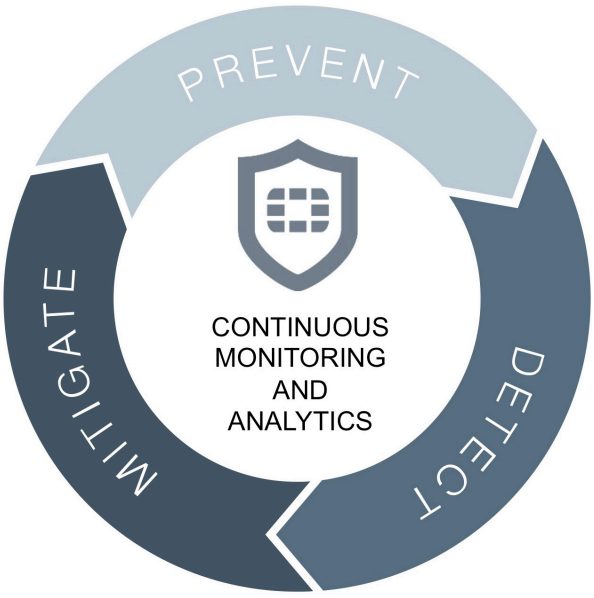


This type of approach is absolutely critical to effective advanced threat protection. While there are always new, innovative technologies to combat new, innovative cyber threats, none represents a "silver bullet" to protect organizations that don't also handle all of "the basics" of security best practices.

Instead, the most effective defense is founded on a cohesive and extensible architecture that encompasses all the important basics, along with the latest emerging technologies, as they demonstrate their effectiveness, working together to stop attacks at multiple points of the organization and multiple phases of their life cycle. As such, the security components recommended as the basis for advanced threat protection span three primary phases:

- Prevention—blocking, as much as possible, typically known threats, often based on global intelligence
- Detection—continuing inspection, usually for unknown threats based on local analysis and intelligence
- Mitigation—responding with new detection to minimize incidents and their impact, primarily by sharing intelligence throughout the security architecture

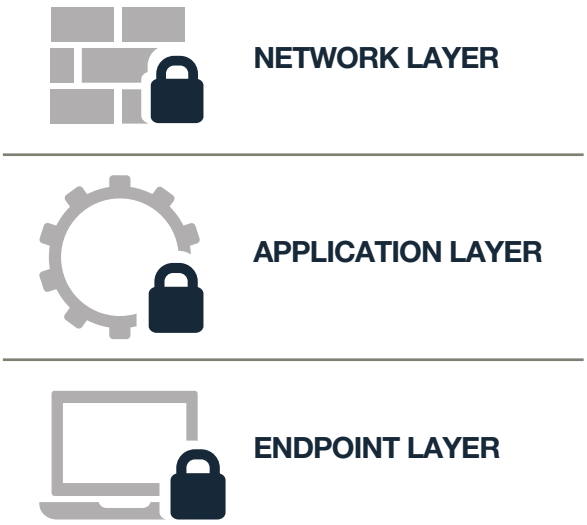
Further, this approach must incorporate current security capabilities, emerging technologies, and customer-specific learning mechanisms to create and distribute actionable security intelligence from newly detected threats in real time. And it must coordinate among security components from multiple vendors, such that the entire infrastructure can act as a single entity to protect the organization.



BROAD COVERAGE ACROSS THE ATTACK SURFACE

Effectively protecting the enterprise starts with ensuring coverage across the entire attack surface—all physical protection points and attack vectors. Specifically, both prevention and detection components must be able to inspect traffic, objects, and user activity from the endpoint (including IoT) and access layer to the network edge and core, all the way out to the public cloud. Further, it must cover the top attack vectors including the:

- Network Layer—encompassing 3 of the top 5 vectors for cyber crime as reported by Verizon
- Application Layer—both email, which was the #1 and #3 vector for cyber crime as reported by Verizon, and web infrastructure, which was the top technique leading to compromise in many industries
- Endpoint Layer—the only place to protect against off-network attacks



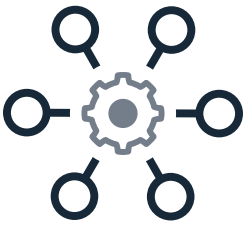
Fortinet recommends our FortiGate next-generation firewall as the foundation of the Security Fabric, spanning the network from branch office and campus, the data center edge and core, and all the way out to workloads in public clouds. From there, coverage can be extended to endpoints with our FortiClient Advanced Endpoint Protection software or Fabric-ready partners like Carbon Black, Ziften, and others. It can also be deepened with enterprise-class protection for email and web infrastructure with FortiMail and FortiWeb. In this manner, the top attack vectors and potential entry points can be covered with global threat intelligence.
To address the fast-moving and more targeted threats, we recommend adding the local intelligence of our FortiSandbox with additional options from Fabric-ready partners like Attivo Networks and their deception infrastructure.

And in many cases, it's possible to "harden" the attack surface, forcing all users (including unauthorized ones) through fewer points of entry or potential threat vectors. Techniques including vulnerability management, virtual private networking, two-factor authentication, and more to limit and control access are also available with our full FortiClient stack.

POWERFUL PROCESSING TO ENABLE THE SECURITY YOU NEED

Note that many of the security technologies required to prevent or detect advanced threats require deeper or more time-consuming analysis, yet they simply cannot be allowed to impede or even slow the business. As a result, it is essential to accelerate, either in hardware, software, or cloud services, these functions so they can be enabled (and not turned off) and improve the organization's security posture. Examples of these more rigorous, yet potentially hindering, security functions include anti-malware inspection on network traffic, sandbox analysis on either the network or endpoint, more advanced behavioral techniques on the endpoints, and similar technologies.

Fortinet FortiGate appliances include our proprietary security processors for network traffic (our NP chips), content inspection (CP chips), and a combined system on a chip (SoC) to ensure that all necessary FortiGate security features can be enabled on properly sized appliances to stop threats seeking entry, from the smallest remote office to the largest data center and all points in between. These features include the full next-generation firewall stack of intrusion prevention, application control, web filtering, anti-malware, SSL inspection, integrated sandboxing, and more. Further, our FortiGate virtual appliances have been optimized for cloud-scale performance in the world's largest IaaS and PaaS environments to extend advanced threat protection out to the public cloud.



AUTOMATED TO ACT AS A SINGLE SYSTEM

Covering the breadth of the organization with security components powerful enough to enable the necessary security functions are simply the building blocks to improve security. If these components operate independently from each other, there will be gaps between them through which cyber criminals can slip through and silos that will slow response and mitigation when that happens. Remember, in the absence of ties between the products, it falls to the security team to manually bridge gaps and coordinate responses—an inherently time-consuming and less-effective exercise.

Accordingly, an organization's strongest defense will only be achieved when security can be automated across all of the deployed components. This automation can include:

1. prevention products sharing objects with detection products for the deeper analysis
2. detection products distributing threat intelligence based on that analysis for updated prevention
3. response elements immediately accessing detection and prevention products for faster mitigation

And this automation must occur across offerings from different vendors, as it is rare to find components for each protection point and attack vector that meet every organization's requirements and budget.

That's why Fortinet has developed six primary APIs, including two specifically for local intelligence sharing from our FortiSandbox for a coordinated defense. These APIs are documented and open for use by Fabric-ready partners with precertified integrations and indeed any third-party security product that will leverage them.

INDEPENDENTLY TESTED

The ultimate measure of the security infrastructure that you have in place is its effectiveness in preventing, detecting, and quickly responding to mitigate attacks in real-world deployment. And while most security offerings will have dashboards showing what's been detected, they are not going to show what's been missed. That's where independent, real-world testing can surely help. There are a number of credible, independent test houses that regularly test a range of security vendor offerings at various protection points and attack vectors. These include NSS Labs, Virus Bulletin, ICSA Labs, and AV-Comparatives.

Fortinet security products have undergone the most independent testing, and earned the most top ratings, of any vendors' offerings in the industry. Among them, Fortinet is the only vendor to earn:

- NSS Labs Recommendation for NGFW, DCIPS, WAF, AEP, and BDS;
- ICSA Labs ATD Certification (both standard and email) from the inception; and
- Virus Bulletin VBSpam+ rating for the full year of 2016

As our co-founder and CTO Michael Xie asserted years ago and remains committed to today, "Fortinet is a strong believer in third-party testing. We are always willing to put our products on the line against our colleagues and competitors in the security sphere... because to us, regardless of where we finish, we take the results and use them to create a better product."

STAYING AHEAD OF THE THREAT CURVE WITH FORTINET FORTIGUARD LABS SYNERGY AND RESEARCH

One of the greatest Fortinet strengths is the synergy of its proprietary software, high-performance appliances, and FortiGuard Labs threat research teams. Most importantly, FortiGuard Labs research groups serve as the intelligence hub that ensures all three elements work seamlessly. They study previously unknown threats, develop comprehensive remediation strategies that are built from the ground up with high performance and efficient protection in mind, and deliver security intelligence to continually strengthen prevention and detection over time. As a result, organizations benefit from:

Comprehensive Security: FortiGuard Labs leverages real-time intelligence across 12 distinct disciplines within the threat landscape to deliver comprehensive security updates across the full range of Fortinet solutions and core technologies for synergistic protection.

Protection Ahead of the Threats: As a new threat emerges, certain detection and prevention products communicate directly for immediate, automated response. Additionally, FortiGuard Labs 24x7x365 global operations pushes up-to-date security intelligence in real time to Fortinet solutions, delivering instant protection against new and emerging threats. And many of the same automated threat analysis tools and techniques have been packaged up within FortiSandbox to bring this same real-time detection and intelligence distribution to the individual customer environment.

Collaboration in the Industry: In addition to its proactive research, global honeypot infrastructure, and 3,000,000+ network security appliances also acting as sensors, FortiGuard Labs has established more than 200 threat information-sharing agreements with other recognized vendor research groups, ISACs, and industry groups like the Cyber Threat Alliance, with a mature process for the automated ingestion, deduplication, and validation to turn raw data into high-value threat intelligence.

For more information about Fortinet and the products that comprise the Advanced Threat Protection Solution, please visit www.fortinet.com/atp.

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

68218-0-A-EN April 11, 2017