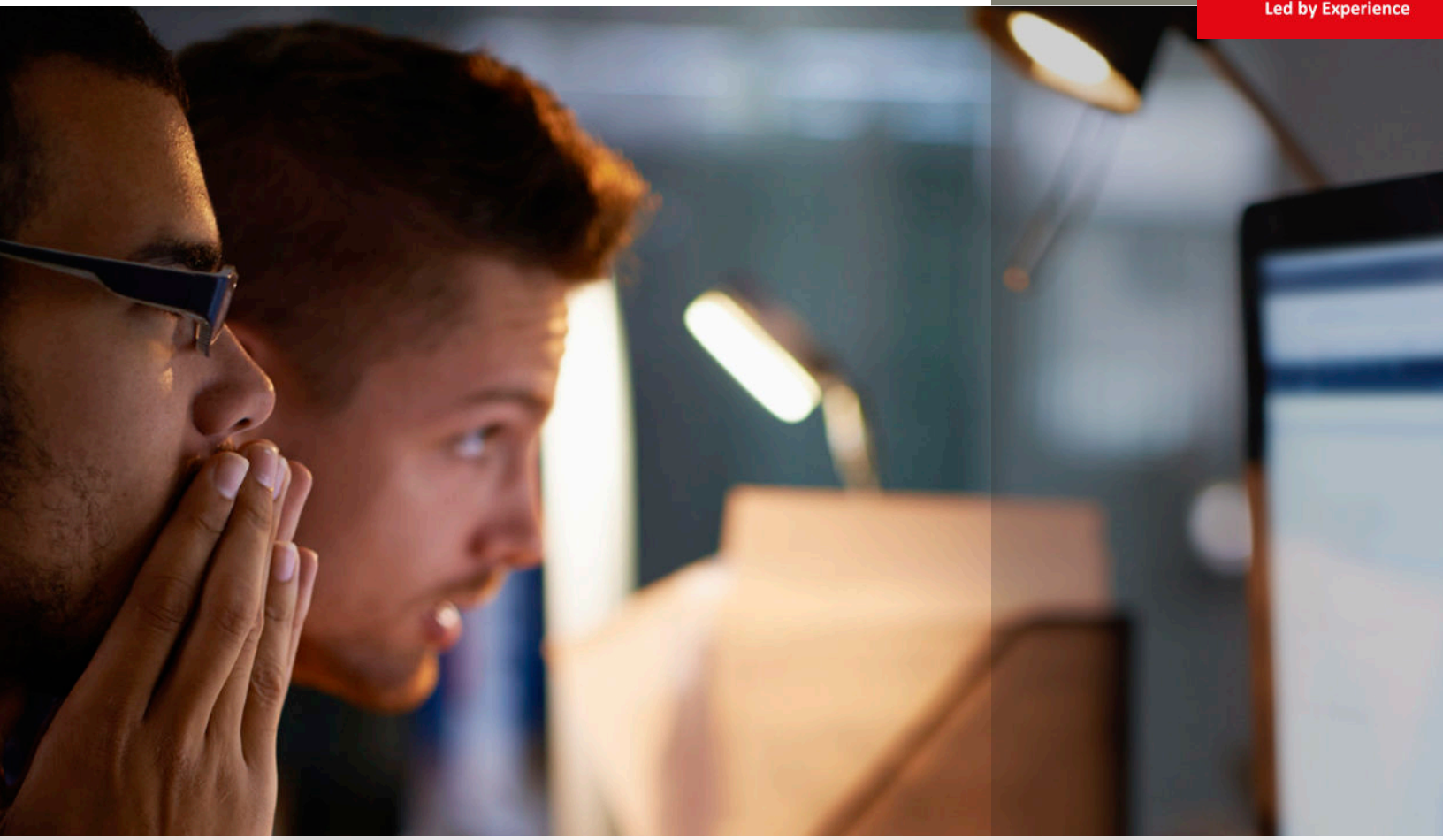
FORTINET

WHITE PAPE

acora
Led by Experience

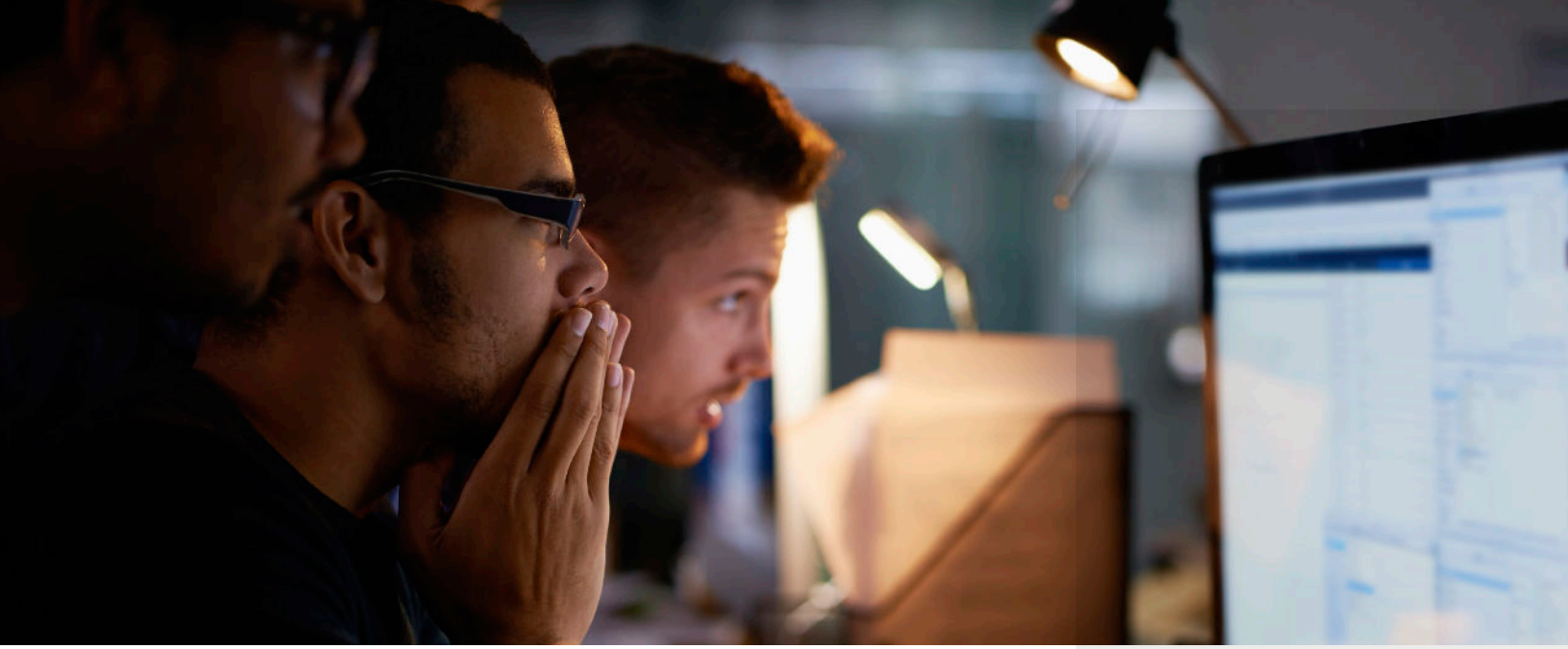


The Fortinet Advanced Threat Protection Framework

An Integrated and Automated Approach to Protecting Against Advanced Targeted Attacks

The Fortinet Advanced Threat Protection Framework

Table of Contents



Introduction

Sophisticated Attacks Yield Big Rewards

The past few years have seen many major brands, large companies and government agencies making headlines, not for some remarkable post-recession economic recovery or innovative product, but for massive data breaches. More than 100 million customers had personal and/or credit card information stolen through just one of these bold and extended attacks.

These kinds of attacks grab the attention of consumers, lawmakers, and the media when they breach very large organizations with dedicated security teams and infrastructure designed to keep hackers at bay. Nobody is immune – smaller organizations are targets as well, either as part of a larger coordinated attack, or through a variety of distributed malware.

The bottom line? It's time for a deeper, more integrated approach to cyber security.

"All organizations should now assume that they are in a state of continuous compromise."

– Gartner

"77% of executives cited protection from/detection of APTs as a high or critical priority in 2015."

– IDG/Fortinet

"55% of organizations experienced 6 or more security incidents over the past 12 months."

– Forrester/Fortinet

Deception, the Most Powerful Tool in a Hacker's Arsenal

Fueled by the ongoing success of high profile hacks, we expect to see continued innovation among cybercriminals focused on deceiving and evading existing security solutions. Malicious hackers have attempted to conceal malware by using different file types and compression schemes with the intent to exploit weaknesses in traditional network protection. Social engineering continues to evolve, and become more targeted, to fool even the most security-aware end users. We also anticipate an increase in sophisticated malware platforms that can be customized for targeted attacks.

Once malware has breached a network, it will, either automatically or under control of cybercriminals, morph, adapt, and move about undetected for as long as possible, mining data ranging from customer records and intellectual property to device profiles and employee credentials. **If security controls cannot detect the malware or its communication during this period, then it's only a matter of time before collected data is staged and exfiltrated, that is, sent back to the cybercriminal and your organization is breached.**

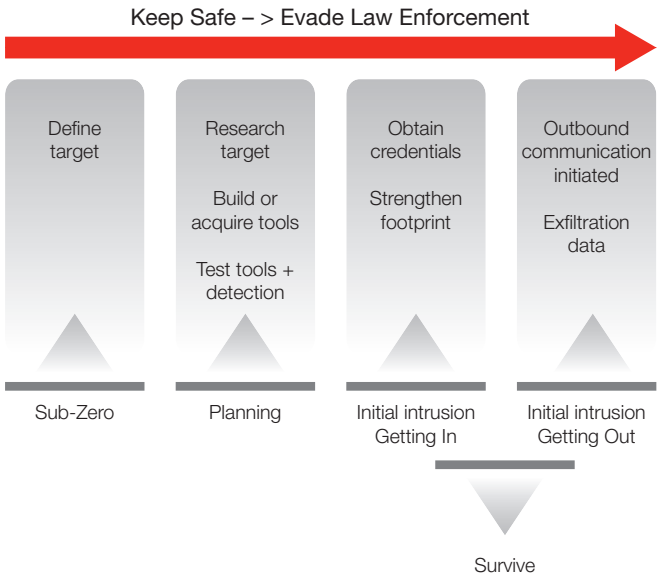


FIGURE 1: THE ANATOMY OF AN ADVANCED THREAT

Advanced Threats Require Advanced Threat Protection

There is no "silver bullet" to protect organizations against the types of advanced targeted attacks outlined above. Rapid innovation on the malware front, frequent zero-day attacks, and emerging evasion techniques can all render any single approach ineffective at preventing tailored intrusion.

Instead, the most effective defense is founded on a cohesive and extensible protection framework that extends from the cloud to the data center and all the way through to the end user device. This framework incorporates current security capabilities, emerging technologies and a customized learning mechanism that creates and distributes 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.

A Simple Framework for Complex Threats

The Fortinet Advanced Threat Protection Framework consists of three elements:

- **Prevent –** Act on known threats and information
- **Detect –** Identify unknown threats and distribute intelligence networkwide
- **Mitigate –** Respond to potential incidents

This framework is conceptually simple; it covers a broad set of both advanced and traditional tools for network, application and endpoint security, threat detection, and incident response. These tools are powered by strong research and threat intelligence competencies that transform information from a variety of sources into actionable protection. Although elements of the framework (and even technologies within them) can operate in a vacuum, organizations will achieve much stronger protection if they are used together as part of an integrated and automated security solution.

Element 1 – Prevent

Act on Known Threats and Information

Of course, as many known threats as possible should be blocked immediately through the use of next-generation firewalls, internal segmentation firewalls, secure email gateways, endpoint security, and similar solutions that leverage highly accurate, security technologies. Examples include anti-malware, web filtering, intrusion prevention, and more. **This is the most**

efficient means of screening out a variety of threats with minimal impact on network performance and end user productivity.
Anti-malware technology, for example, can detect and block viruses, botnets, and even predicted variants of malware with the use of technology such as the Fortinet patented Content Pattern Recognition Language (CPRL) with minimum processing time.

Attacks can also be thwarted by reducing the attack surface. The fewer points of entry or potential threat vectors available to cybercriminals the better, meaning that carefully controlled access (user identity, two factor authentication, VPNs) is also an important aspect of Element 1, and part of the first line of defense against targeted attacks.

High risk traffic that appears legitimate based on quick inspection gets handed off to Element 2.

Element 2 – Detect

Identify Previously Unknown Threats

There are obvious advantages to addressing threats in Element 1. However, unknown "zero-day" threats and sophisticated attacks designed to hide themselves from traditional measures are being used every day to penetrate high-stakes targets. **Element 2 of the framework uses advanced threat detection technologies to examine the behavior of network traffic, users, and content more closely in order to identify novel attacks.**

There are a number of emerging approaches that can automatically detect previously unknown threats and create actionable threat intelligence. Sandboxing, in particular, allows potentially malicious software to be handed off to a sheltered environment where its full behavior can be observed, without affecting production networks. Additionally, botnet detection flags patterns of communication that suggest command & control activity while client reputation capabilities flag potentially compromised endpoints based on contextual profile.

Though incredibly powerful, this type of threat detection is resource intensive and thus reserved for threats that could not be identified by more efficient methods. Further, detection spurs the final element of the ATP framework – dealing decisively with these new threats including communicating actionable threat intelligence across the network.

Element 3 – Mitigate

Respond to Potential Incidents

Once new threats and potential incidents are identified in Element 2, organizations need to immediately validate the threat and mitigate any damage. Users, devices, and/or content should be quarantined, by automated and manual systems in place to ensure the safety of network resources and organizational data. They also need to be investigated fully, remediated and returned to a safe operational state. This can be handled manually by response teams, in an automated fashion through intelligence sharing between detection and prevention products, or with "assisted mitigation" – a combination of both people and technology working together for efficiency and accuracy.

At the same time, threat detections trigger another critical handoff: moving the discovered information back to the research and development groups. **Previously unknown threats now can be analyzed in depth, resulting in fixes that take all of the security layers into account, providing the right mix of up-to-date protection for every layer.**

Executing prevention, detection and mitigation in the most efficient way possible (combining Elements 1, 2, and 3) is essential to maintain high levels of network performance and maximize protection.

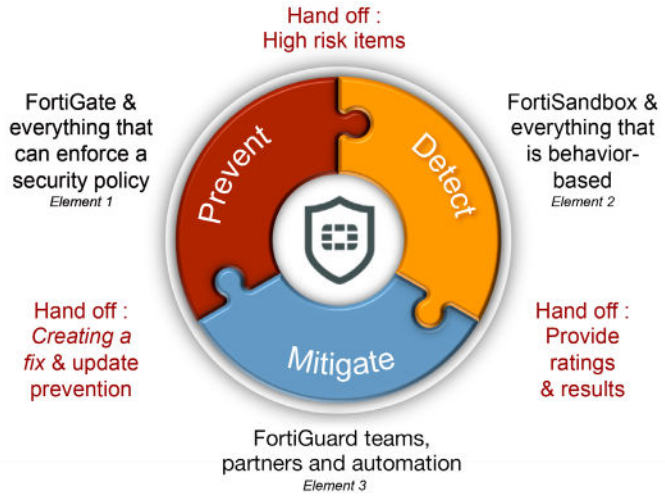


FIGURE 2: THE FORTINET ADVANCED THREAT PROTECTION FRAMEWORK

Handoffs – The Missing Link

The most critical feature of the Fortinet Advanced Threat Protection framework – one that is missing in most organizations' security implementations – is the notion of the handoff, beyond any particular technology or element. Advanced threat protection relies on multiple types of security technologies, products, services and research, each with different roles. To be most effective, they must be aware of and communicate with each other on a continuous basis, handing off data from one to the next.

As seen in Figure 2, the prevention phase, Element 1, will hand off high-risk items to the detection phase, Element 2, with previously unknown threats handed off in Element 3 for further analysis or mitigation. Ultimately, threat intelligence and updated protection from Element 3 is handed off back to products in Elements 1 and 2, for **this efficient cycle of constantly improving protection and detection against increasingly sophisticated attacks.**

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.

Comprehensive Security: FortiGuard Labs leverages real-time intelligence on 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.

High-Performance Solutions: The Fortinet portfolio of Integrated Security Services is designed from the ground up to maximize protection and optimize performance across Fortinet security solutions – physical or virtual and cloud.

The handoff between Element 3 back to 1 and 2, where the advanced threat protection cycle is routinely completed, occurs when the extensive threat intelligence from FortiGuard Labs is delivered to all users of Fortinet solutions via the global Fortinet Distribution Network. Additionally, as part of the Cyber Threat Alliance and other related initiatives, Fortinet shares threat intelligence with a larger body of researchers, further extending the reach of its work.

Fortinet Solutions Together Deliver Better Protection

A collection of individual security products, however powerful, cannot deliver the best security if they are acting in isolation. Each piece of the solution should be aware of the others and work together as a single entity to deliver optimal protection. Further, that entity must combine highly effective global and local intelligence to respond to the latest threats. Fortinet integrates the intelligence of FortiGuard Labs into FortiGate next-generation firewalls, as well as internal segmentation firewalls, FortiMail secure email gateways, FortiWeb web application firewalls, FortClient endpoint security, FortiSandbox advanced threat detection, and other security products in its ecosystem to continually optimize and improve each organization's level of security. More importantly, the named products also share traffic and actionable intelligence directly and via an open API, for immediate and automated response.

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

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
120 rue Albert Caquot
06560, Sophia Antipolis,
France
Tel: +33.4.8987.0510

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

LATIN AMERICA SALES OFFICE
Paseo de la Reforma 412 piso 16
Col. Juarez
C.P. 06600
México D.F.
Tel: 011-52-(55) 5524-8428

May 27, 2016