The Fortinet Advanced Threat Protection Framework

A Cohesive Approach to Addressing Advanced Targeted Attacks
The Fortinet Advanced Threat Protection Framework

Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>The Fortinet Advanced Threat Protection Framework</td>
<td>4</td>
</tr>
<tr>
<td>Staying Ahead of the Threat Curve with Fortinet</td>
<td>6</td>
</tr>
</tbody>
</table>
Introduction

Sophisticated Attacks Yield Big Rewards

The past few years have seen many major brands and large companies 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 types of attacks grab the attention of consumers, lawmakers, and the media when they manage to breach very large organizations with dedicated security teams and extensive 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 comprehensive 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

“44% of organizations surveyed cited a recent data breach as the primary driver for their NGFW project.”
– Forrester/Fortinet
Deception, the Most Powerful Tool in a Hacker’s Arsenal

Fueled by the success of profile hacks, we expect to see continued innovation among cybercriminals with an even greater focus 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 means of network protection. 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.

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 network core through to the end user device. This framework incorporates current security capabilities, emerging technologies and a customized learning mechanism that creates actionable security intelligence from newly detected threats. The latter component is arguably most critical to staying ahead of the threat curve.

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 previously unknown threats
- **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 mitigation. These tools are powered by strong research and threat intelligence capabilities 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 a holistic security strategy.

**Element 1 – Prevent**

**Act on Known Threats and Information**

Known threats should be blocked immediately (Element 1 in the Fortinet Advanced Threat Protection Framework) whenever possible through the use of next-generation firewalls, internal network 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.**
Anti-malware technology, for example, can detect and block viruses, botnets, and even predicted variants of malware with the use of technology such as Fortinet’s patented Compact 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 controlling access and implementing VPNs is also an important aspect of Element 1 and part of the first line of defense against targeted attacks.

Traffic that can’t be swiftly dealt with here gets handed off to Element 2.

**Element 2 – Detect**

**Identify Previously Unknown Threats**

There are obvious advantages to addressing threats in Element 1. The more threats that fall into the known category, the better. 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 new 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 so that its full behavior can be directly 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 traditional methods. Detection, of course, is only another element of the ATP framework. The next handoff deals decisively with these new threats.

**Element 3 – Mitigate**

**Respond to Potential Incidents**

Once potential incidents and new threats are identified in Element 2, organizations immediately need to validate the threat and mitigate any damage. Users, devices, and/or content should be quarantined, with automated and manual systems in place to ensure the safety of network resources and organizational data until this occurs.

At the same time, threat detections trigger another critical handoff: moving the discovered information back to the research and development groups. Tactical protections can be put in place. **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.** At this stage, eliminating redundancy and creating synergy between different security technologies is the key to deploying a high-performing security solution, where the unknown becomes known.

Of course, the cycle is not completed until this actionable threat intelligence is available at the different enforcement points and shared globally so that Element 1 is strengthened to act on the new known. This keeps cybercriminals at bay not just for one organization but for all organizations worldwide.

**Executing detection, prevention 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.**
Handoffs – The Missing Link

Perhaps the most critical feature of the threat protection framework – one that is missing in many organizations’ security implementations – is the notion of the handoff rather than any particular technology or element. Advanced threat protection relies on multiple types of security technologies, products, and research, each with different roles. However, each will be less effective if they don’t communicate with each other on a continuous basis, handing off data from one to the next.

As seen in Figure 2, Element 1, the prevention phase, will hand off high-risk items to Element 2, the detection phase, 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 back off to products in Elements 1 and 2, for this constant cycle efficiently improving protection and detection against increasingly sophisticated attacks.

Staying Ahead of the Threat Curve with Fortinet

FortiGuard Labs Synergy and Research

One of Fortinet’s greatest strengths is in the synergy of its proprietary software, high-performance appliances, and, most importantly, the FortiGuard Labs threat research teams. 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 that continually strengthens 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 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: Fortinet’s portfolio of Integrated Security Services are designed from the ground up to maximize protection and optimize performance across Fortinet’s security solutions – both physical and virtual.

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 developed by FortiGuard Labs gets handed off 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 also shares threat intelligence with a larger body of researchers, further extending the reach of their work and of organization-generated threat intelligence discovered under this framework.

Fortinet Solutions Together Deliver Better Protection

A collection of individual security products, however powerful, cannot deliver optimal security if they are acting in isolation. Each piece of the solution needs to work together to deliver optimal protection. Fortinet integrates the intelligence of FortiGuard Labs into FortiGate next-generation firewalls, as well as internal network firewalls, FortiMail secure email gateways, FortiClient endpoint security, FortiSandbox advanced threat detection, and other security products in its ecosystem to continually optimize and improve each organization’s level of security.

For more information about Fortinet and their ecosystem of advanced threat protection products, visit www.fortinet.com/sandbox.