Fortinet's Advanced Threat Protection Framework:

A cohesive approach to addressing advanced targeted attacks

Introduction

Looking at the data breach incidents that made the news in 2013 and into 2014 – Target Corporation, Adobe, Tesco, Snecma, LaCie, KT Corp, Yahoo Japan, the New York Times and more – sophisticated threats continue to beat traditional defenses. Surveys confirm this trend: PwC[1] reported that 18% of organizations reported a successful network penetration by outsiders had breached their network, Verizon[2] noted that breaches routinely remained undetected for months and Fortinet's own survey conducted by Forrester found that 44% of organizations cited a recent internal security breach as the driver for their NGFW project. In fact, Gartner recommends that "all organizations should now assume
that they are in a state of continuous compromise".

More and more, we are seeing sophisticated attacks which:

- Step 1. Seek entry to individual organizations (or a small set of similar organizations) via overlooked ports, system vulnerabilities or stolen credentials
- Step 2. Install malware (often tested) to bypass traditional security controls and establish communication back to the cyber criminal
- Step 3. Move laterally and stealthily within the organization in search of data
- Step 4. Exfiltrate (and often stage) that data over a period of time
- Step 5. Persist and morph to remain undetected

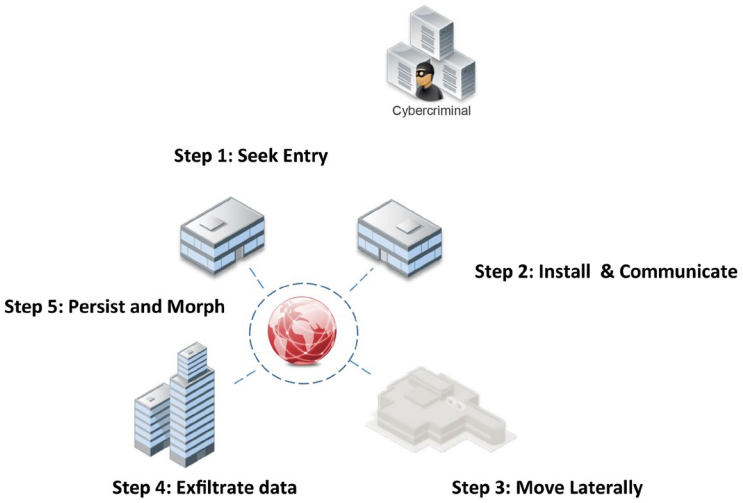

Figure 1. Targeted Attack Lifecycle.

As a result, many new approaches to detecting and mitigating the seemingly inevitable breach have gained growing attention. From anomaly detection on the network to forensics at the endpoint and payload analysis everywhere in between, there is growing recognition that traditional security technologies need to be complemented by newer approaches. However, none of these newer approaches offer a "silver bullet" to individually address the security challenge posed by increasingly targeted and tailored attacks. And even if they did, this current class of sophisticated attacks- along with the new defensive technologies developed in response- is neither the first nor the last battle for control of your network. Rather than relying on any single technology, however new and promising, a robust defense is best founded on an extensible security framework that leverages current capabilities and extends them with new ones.

Fortinet's Advanced Threat Protection Framework

Fortinet recommends a five component Advanced Threat Protection Framework – comprised of established and new technologies and processes – to guide organizations seeking to address this new class of advanced targeted attacks. While the exact technologies appropriate for each organization will vary based on security budget, staffing, skills and risk tolerance, it is critical to ensure that each of the components is covered and works seamlessly together as part of a coordinated defense.

There is no one "best" component or technology that will guarantee protection from this class of threats, despite what some vendors may lead you to believe. Each technology (and component) has inherent strengths and weaknesses, which, even when deployed together but independent from other technologies, may leave exploitable gaps in defenses. Instead, organizations must deploy each technology with an eye towards its role within a complete solution, such that the strengths of one can compensate for the weaknesses of another. As an example, while threat detection is excellent at detecting sophisticated attacks that may bypass other defenses, it can generate an overwhelming number of alerts if relied on too heavily and is thus most effective when deployed in conjunction with highly effective access control and threat prevention technologies.

Figure 2. Fortinet's Advanced Threat Protection Framework.

Access Control

One element of combating advanced persistent threats and advanced targeted attacks seeking entry to your network is access control. Specifically, it is the practice of "reducing the attack surface" or limiting an attacker's ability to penetrate the organization- forcing all users and traffic through established inspection points that have appropriate threat prevention and detection technologies deployed.

Fortinet recommends the following baseline technologies in response to the prevalence of port hopping applications, exploited vulnerabilities and stolen credentials as common methods for cybercriminals to gain access to networks:

- **A layer 2/3 Firewall** to restrict Internet access of the network to only authorized ports/protocols, where threat prevention and other inspection technologies can be depolyed.
- **Vulnerability Management** including a process to regularly, and as needed, identify and update or shield systems from exploit. At a minimum this starts with patch management.
- **Two-factor Authentication** to identify users (or devices) seeking access and only approve those who demonstrate (via multiple methods) that they are who they claim to be.

It is important to highlight that these technologies are less effective when deployed in silos. As a representative example, access via an overlooked port may not have the desired strong authentication or threat prevention technologies established when rolled out separately; allowing relatively easy entrance for a persistent attacker.

A foundational technology in this area is Fortinet's unique approach in leveraging custom ASICs for superior performance. Both its network and content processors are designed and developed in house as purpose-specific components that allow its firewall performance to meet the requirements of high speed networks. They also allow Fortinet appliances to deliver integrated and consolidated security functions, for access control and other security functions.

- Unmatched performance
- Physical and virtual segmentation
- Breadth of integrated technologies

Figure 3. The Fortinet Advantage: Speed and Flexibility.

Threat Prevention

Another established set of technologies that play a role in combating sophisticated attacks is threat prevention. While an increasing number of attacks utilize modified versions of known malware in an attempt to bypass content – oriented inspection threat prevention technologies are still a necessary baseline and the more proactive offerings can in many cases still identify a significant portion of advanced malware.

Threat Prevention technologies to address increasingly blended attacks should encompass:

- **Intrusion Prevention** to inspect traffic for patterns and protocols associated with malicious attacks.
- **Application Control** to block applications that represent a risk to the organization- by type, app or function.
- **Web Filtering** to prevent access or communication with malicious or compromised sites that host or deliver malicious code.
- **Email Filtering** to screen out messages containing malicious code or links to sites hosting code.
- **Antimalware** to stop the delivery of malicious code.

Similar to access control technologies, most of these threat prevention technologies were first developed more than a decade ago; originally based on signatures, then heuristics, then reputations. So it is easy to think of them as all the same. However there remains great variety in the approach and effectiveness of such technologies today as exhibited by real world testing. Fortinet delivers some of the most sophisticated threat prevention engines, leveraging a full programming language for antimalware and deeper inspection such as custom codec definitions for IPS, that go well beyond traditional pattern matching and actually detect a substantial amount of previously unknown and advanced malware.

One important capability in FortiOS 5 is a deep flow advanced malware engine that delivers much more than the traditional flow-based AV including:

- An accelerated architecture that checks an extended detection set (traditionally reserved for proxy inspection) with the speed of in-line flow-based inspection
- Advanced unpacking and emulation technologies, beyond the traditional signatures and heuristics
- The full programming language previously noted, delivering more sophisticated inspection

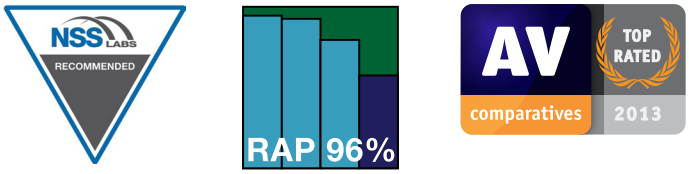

Figure 4. The Fortinet Advantage: Top-Rated Threat Prevention.

These capabilities provide strong threat prevention in complement to the threat detection described in the next section.

Threat Detection

It goes without saying that if access control and threat prevention approaches were sufficient on their own, the data breaches constantly making the news would not be occurring As the threat landscape has evolved so have the technologies introduced to combat these new threats. These technologies examine dynamic behavior (think execution and activity) rather than static attributes (think file hashes, IP addresses or other characteristics) and flag "indicators of compromise."

There is an exciting range of emerging technologies available in the market. Given the fledgling nature of many approaches, for now Fortinet recommends the following:

- **"Sandboxing"** to run objects in a contained environment and assess run-time, multi-stage activity to uncover previously unknown threats.
- **Botnet Detection** to flag communication patterns reflective of Botnet activity and identify previously unknown incidents.
- **Client Reputation** to identify compromised endpoints based on contextual activity that may signal compromise.
- **Network Behavior Analysis** to flag malformed protocols, suspect instructions or anomalous traffic associated with vulnerability exploit attempts, fast flux activity and more indicative of an attack in progress.

Fortinet has taken an integrated approach to delivering these advanced technologies. Fortinet has taken an integrated approach to delivering these advanced detection technologies, either as a FortiOS feature or a centrally managed extension, with intelligence from all flowing through FortiGuard Labs.

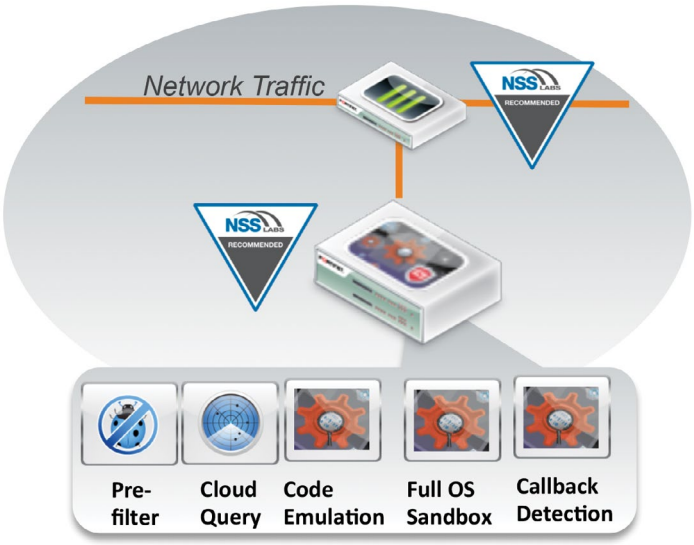

Figure 5. The Fortinet Advantage: Integrated Detection and Prevention.

The four detection technologies noted in this section are critically important to enabling incident response and improving protection. Longer-term Fortinet expects that tthey will ultimately move into the threat prevention category – another reason for selecting a vendor who integrates capability across categories.

Incident Response

Once the detection of potential incidents takes place, actions to validate and contain them becomes paramount. In this area, service and technology components (including those deployed for detection and prevention, as well as incident response) need to work closely together to speed response and corrective action.

Fortinet recommends that organizations utilize a mix of technology and service components:

- **Consolidated logs and reports** to speed investigation and mitigation.
- **Professional Services** to provide supporting security expertise to further shorten the window of response.
- **User or Device Quarantine** to temporarily segregate suspect users or devices when something suspicious or malicious is detected.
- **Threat Prevention Updates** to continually improve in-place protections based on new intelligence, including that received from customer-specific threat detection.

Fortinet delivers actionable visibility in these technology areas – with severity ratings, drill down and policy manipulation capabilities seamlessly within its logs and reports- as well as automated response based on device or user reputation to speed response.

But technical controls and automated inspection can only take organizations so far in addressing sophisticated cyberthreats specifically engineered to mimic legitimate or benign code. Validation and response by security experts is often necessary – to convert detection of previously unknown attacks into initial remediation and ultimately to deliver proactive protection from future attacks. FortiGuard Labs offers a diverse set of expert services, including dedicated support, security incident response, premium updates.

The Fortinet Advantage:

- 200+ researchers
- Expertise from network edge to endpoint
- 140+ zero-day vulnerabilities discovered

Figure 6. The Fortinet Advantage: Depth and Breadth of Security Expertise.

Continuous Monitoring

With that in mind, containment and response (as well as learning from the other components) leads naturally into Continuous Monitoring for ongoing assessment and audit to improve security. This assessment and audit includes the effectiveness of an organization's security, the state of security among the industry/peers and the continued evolution in the threat landscape.

Here 'Fortinet recommends the following:

- **Real-time Activity Views** through dashboards to continually assess network activity and security posture.
- **Security Reporting** to audit security against a baseline, correlate information across security products and identify areas for security improvement.
- **Threat Intelligence** to constantly assess threats, trends and emerging attack vectors and techniques.

New, real-time visibility into cloud services and other activity help organizations assess their risk on a continual basis, as do a range of new pre-defined reports in critical security areas.

Further, our own capability in this area is extended with the help of more than a dozen partners, demonstrating our leadership and commitment to providing organizations a comprehensive picture of its current and projected risk in their ongoing effort to help security professionals keep pace with cybercriminals and threats.

- Enterprise-class management used by Global 2000
- Actionable visibility and reporting
- 100% NSS Labs rating for management

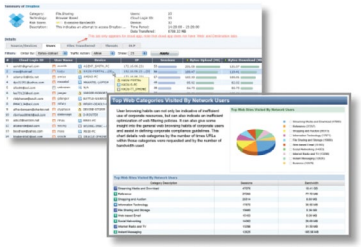

Figure 7. The Fortinet Advantage: Enterprise Class Management and Reporting..

The Fortinet Products Powering the Advanced Threat Protection Framework

The foundational building block of Fortinet's Advanced Threat Protection Framework is its FortiOS network security platform that runs on its flagship FortiGate physical or virtual appliances. On its own, FortiOS delivers a strong baseline of capability across all five components of access control, threat prevention, threat detection, incident response and continuous monitoring. However, any organizations choose to extend that capability with integrated add-ons including:

- FortiSandbox to detect the most sophisticated threats
- FortiAuthenticator to scale strong authentication for larger organizations
- FortiAnalyzer for richer and deeper reporting
- FortiManager for consolidated monitoring and management of larger deployments
- FortiGuard services as well as partner integrations in the areas of anomaly detection, threat intelligence and security management for faster response and a bigger picture

Figure 8. The Products Powering Fortinet's Advanced Threat Protection Framework.

Conclusion

As security technologies continue to evolve – from signatures to heuristics to reputation to behavior analysis and beyond – they do so in response to the changing nature of Internet threats and cybercrime. Cutting through the noise made by vendors promising quick solutions to the APT – problem, Fortinet encourages all organizations to assess their tolerance for risk and determine which security technologies are right for them.

However deploying a robust set of established and emerging security technologies that can work together is required if organizations hope to reduce their security risk. In particular, addressing the five component areas that make up Fortinet's Advanced Threat Protection Framework – with highly effective and real-world proven technologies that work in a coordinated fashion- is critical to reducing the risk of today's advanced targeted attacks.

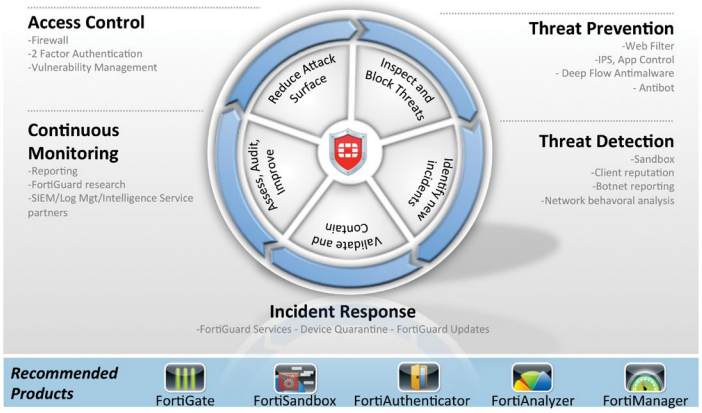

Figure 9. Fortinet's Advanced Threat Protection Framework.

Beyond its breadth of integrated technologies across these five areas, what really sets Fortinet apart is the intersection of:

1. Deep security expertise embodied in its 200+ security researchers around the world who not only uncover new threats and vulnerabilities but also continue to deliver unique prevention technologies as part of a single FortiOS network security platform. These technologies include a patent-pending Compact Pattern Recognition Language (CPRL) that delivers sophisticated threat prevention (far above and beyond traditional signature, heuristic or reputation engines) to match the sophistication of threats, Fortinet's industry leading sandbox for advanced threat detection (based on the automated malware analysis technology used in our labs for more than half a decade and much more.
2. Unique ASIC technology that delivers exponentially greater processing power at an affordable cost in order to, among other things, make more (and more advanced) threat prevention techniques like CPRL possible at line speed on a single appliance.
3. 3rd party validation and a company commitment to exceed exacting standards for real-world performance and effectiveness, that starts from the very top.

The Fortinet Advantage

- Top performance (Ixia, NSS Labs) firewall appliances to control access
- Top-rated (NSS Labs, Virus Bulletin, AV Comparatives), real-world threat prevention
- Top-rated (NSS Labs), real-world threat detection – 99% effectiveness for breach detection
- Leading security expertise (140+ zero-day discovers) across all elements of the strategic framework mitigation and facilitate a coordinated defense across them
- A broad range of partners to contribute to the continuous monitoring and improvement of the security system as a whole.

For more information on Fortinet's technologies, products and approach, please visit our Advanced Threat Protection Solution page.

1. PwC. 2014 State of Information Security Breaches Survey. March 2014
2. Verizon. Data Breach Investigations Report 2014. March 2014.

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
Fax: +1.408.235.7737
www.fortinet.com/sales

EMEA SALES OFFICE
120 rue Albert Caquot
06560, Sophia Antipolis,
France
Tel: +33.4.8987.0510
Fax: +33.4.8987.0501

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730
Fax: +65.6223.6784

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

Copyright © 2014 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other resultsmay vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations,and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.