MSSP Advanced Threat Protection Service
Fortinet Empowers MSSP Delivery of Complete ATP Managed Security Service

The Need For ATP Managed Security Service

According to Frost & Sullivan, the global Managed Security Services (MSS) market will grow from $9B in 2013 to $15B by 2015. This business opportunity is driven by two main factors - the growing acceptance of cloud-based, Security-as-a-Service delivery and the need for enterprises and SMBs alike to reduce security related CAPEX and OPEX costs. As the threat landscape continues to evolve and grow in both volume and sophistication, MSSPs need to evolve their MSS offerings to address this growing threat and provide Advanced Threat Protection (ATP) services.

Advanced Persistent Threats are well thought, multi stage processes as outlines in figure 1. Protecting against these APTs requires an equally well thought, multi stage framework that will deploy the largest number of weapons available in the MSSP’s security arsenal to provide a meaningful response for its customers’ concerns.
Fortinet’s Advanced Threat Protection Framework for MSSPs

Fortinet arms MSSPs with a structured Advanced Threat Protection Framework – to provide organizations a comprehensive solution to address this new class of advanced targeted attacks.

There is no one component or technology that will guarantee protection from a sufficiently targeted and sophisticated attack. Each technology has inherent strengths and weaknesses, which, even when deployed together but independently from other technologies, may leave exploitable gaps in the network’s defense architecture. To provide the most effective ATP service, MSSPs must deploy each technology with an eye towards its role within a complete ATP solution, such that the strengths of one can compensate for the weaknesses of another.

FIGURE 2: FORTINET’S ADVANCED THREAT PROTECTION FRAMEWORK
Step 1 - Prevent

The first step in protecting against APTs should be preventing threats from entering the network. This consists of several elements available to MSSPs, as outlined in Figure 2:

- Deployment of AntiVirus and AntiMalware via FortiGate and other purpose-built appliances (such as FortiWeb and FortiMail) as means to prevent known threats from entering the network.
- Deployment of FortiMail secure email gateway to protect against phishing and corrupted attachments.
- 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 traffic and activity indicative of an attack in progress, such as: malformed protocols, suspected instructions or anomalous traffic associated with vulnerability exploit attempts, fast flux activity and more.
- FortiGate and FortiWiFi firewalls to provide secured wireless access and restrict access to only authorized applications, ports/protocols, where threat prevention and other inspection technologies can be deployed.
- FortiGate integration with two-factor authentication methods, such as FortiAuthenticator and FortiToken, to identify users and devices seeking access and only approve the legitimate ones.
- Deployment of FortiClient for desktop and mobile devices for endpoint security in mobile, BYOD environments.

The deployment of prevention technologies and services should continue throughout the APT lifecycle with additional measures such as Data Loss Protection and Trust Zone Segmentation. This is important as the APT’s lifecycle and damage can be reduced and hampered at each phase of its lifecycle.

The deployment of such security services and technologies will prevent many of the threats from entering the network, mostly known threats that can be identified with existing AV and IPS signatures. Some of the codes examined by the services mentioned above will be categorized as suspected codes that need to be handed off for further detection and analysis to determine if they represent a threat. To do so, FortiGate and FortiMail are integrated with the next stage of the ATP framework by submitting unknown suspicious code for further analysis in an isolated and contained environment - the FortiSandbox.

Step 2 - Detect

Step 2 of Fortinet’s ATP framework comes into effect in one of two cases:

1. Suspicious, unknown code has been identified by FortiGate and/or FortiMail. This code is then automatically delivered to the FortiSandbox for detection and analysis.
2. Suspicious code is delivered to the FortiSandbox manually, via the device’s API or by a network sniffing device.

Upon the completion of the code's analysis by the sandbox, the code will be identified as malicious or not, alongside its operational credentials and passed automatically to the third step for mitigation.

In most cases, while suspicious content is examined in a contained environment - that is the FortiSandbox - the content itself is permitted access to the network and the applications it targets. This is done so business continuity can be maintained and to avoid putting workloads and process to halt while the relevant suspicious content is examined by the sandbox. The only exception to this behavior is suspicious code delivered via the email vector as this application is not real-time and emails and their content may be delayed until the sandbox analysis is terminated and the classification of the content is determined as good or malicious.
This behavior drives the need for the sandbox to perform its analysis and discovery as fast as possible, without compromising the quality of the analysis and the results provided. With the FortiSandbox, this is achieved via the integration of an AntiVirus engine, community intelligence cloud query and a code emulation engine that effectively created an array of “pre-filters” that speeds up the discovery process and reduces the amount of suspected code that has to go through the full virtual sandbox analysis, thus providing a fast discovery time and minimum delay between the time a suspicious code has been submitted to the FortiSandbox until the mitigation stage can commence.

Step 3 - Mitigate

Once potential incidents and threats are identified via the sandbox analysis during phase 2 of Fortinet’s ATP framework, organizations immediately need to validate the threat and mitigate any damage.

The FortiSandbox, upon detecting a threat, will send an alarm to the MSSP SOC and its customer so that immediate mitigation can take place to ensure the safety of the enterprise resources and data. At the same time, the analysis information is automatically sent back to Fortinet’s threat research & response labs, FortiGuard, for in-depth analysis so that the appropriate fixes that take into account all of the security layers can be done and delivered to the different security enforcement points, such as the Firewall. This may include updated AV and IPS signature, updated IP reputation database, etc. With this actionable threat intelligence available, the Fortinet’s ATP cycle is completed as the unknown threat becomes known and will be prevented from getting into the network in the future.

In addition, Fortinet empowers the MSSP’s incident response capabilities via a mix of technology and service components:

- Consolidated logs and reports to speed investigation and mitigation via the FortiAnalyzer and its integration with the MSSP’s SoC and SIEM.
- Fortinet’s Professional Services to provide security expertise support to the MSSP and its customers to further shorten the response time.

Containment and response lead naturally into continuous monitoring for ongoing assessment and audit to improve security. Here, Fortinet provides the MSSP with the FortiManager management platform, FortiAnalyzer reporting platform and FortiGuard security research and intelligence service for:

- 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.
- APIs for integration with the MSSP’s SoC and SIEM.
FortiSandbox Purpose Built ATP Appliance
FortiSandbox is a purpose built ATP appliance that offers a robust combination of proactive detection and mitigation, actionable threat insight and easy, integrated deployment. At its foundation is a unique, dual-level sandbox which is complemented by Fortinet’s award-winning AntiMalware and integrated FortiGuard threat intelligence.

Suspicious samples are subjected to multi-layer pre-filters prior to execution in the virtual OS for detailed behavioral analysis. The highly effective pre-filters include a screen by Fortinet’s award winning AV engine, queries to cloud-based threat databases and OS-independent simulation with a code emulator, followed by execution in the full virtual runtime environment. Once a malicious code is detected, results are submitted for AntiMalware signature creation as well as updates to other threat databases. FortiSandbox supports inspection of many protocols in one unified solution, thus simplifying network infrastructure and operations. Further, it integrates with FortiGate and FortiMail as a consolidated capability within an existing security framework.

FortiGate and FortiMail Sandbox Integration for Enhanced Security
For an MSSP already leveraging Fortinet firewalls and FortiMail secure email gateway as part of their Managed Security offerings, launching a Fortinet Sandbox-as-a-Service is easy: whether the FortiGate and/or FortiMail is local or hosted, simply connect the device to the Sandbox and the MSSP can start gathering and analyzing data.

Email attachments constitute the majority of the attack vectors perpetrated by cyber criminals. Tying email security to sandboxing is important when considering countermeasures for this highly successful and flexible attack method. Leveraging Fortinet’s FortiMail email security in conjunction with FortiSandbox and FortiGate firewalls creates a highly effective and scalable defense and a compelling value proposition for the MSSP and the customer alike and should be considered as part of a comprehensive, layered security offering.
The Fortinet Advantage

Fortinet provides MSSP with the following advantages in building and delivering a complete ATP managed service:

- Complete delivery of the ATP framework: Prevent - Detect - Mitigate.
- A wide range of physical and virtual-form security appliances for a cost effective delivery of ATP MSS for different size enterprises and SMB customers.
- FortiGate and FortiMail integration with FortiSandbox for stronger layered security.
- Support of CPE-based, Hybrid-based and Cloud-based ATP MSS delivery.
- In-house FortiGuard threat research, expertise, and services.

Conclusion

The ability of MSSPs to provide an ATP managed security service should come in response to a growing demand from their enterprise customers, and can represents an important component of their business growth and success. However, an effective ATP service is more than sandboxing and can only be delivered as part of a complete framework that covers threat prevention, threat detection and mitigation.

Fortinet is the only security vendor delivering such scope and breadth of technologies, products and expertise, empowering MSSPs to implement and deliver a cost effective and flexible ATP service to enterprise and SMB customers. The complete framework’s flexibility, in terms of scalability, virtual and hardware based appliance options and its overall TCO, allows the MSSP to tailor the most appropriate ATP service for each customer’s different needs and budgets, either as a complete ATP service or as a layover service complementing existing MSS delivered by the service provider.