Lab Validation Report

Fortinet Advanced Threat Protection Framework

Integrated and Automated Detection, Mitigation, and Prevention of Advanced Attacks

By Tony Palmer, Senior Lab Analyst and Jack Poller, Lab Analyst

February 2016

Contents

Introduction 3
Background 3
Fortinet Advanced Threat Protection Framework 4
ESG Lab Validation 5
Detection 5
Mitigation 9
Prevention 12
ESG Lab Validation Highlights 15
Issues to Consider 15
The Bigger Truth 16
Appendix 17

ESG Lab Reports

The goal of ESG Lab reports is to educate IT professionals about data center technology products for companies of all types and sizes. ESG Lab reports are not meant to replace the evaluation process that should be conducted before making purchasing decisions, but rather to provide insight into these emerging technologies. Our objective is to go over some of the more valuable features/functions of products, show how they can be used to solve real customer problems and identify any areas needing improvement. ESG Lab's expert third-party perspective is based on our own hands-on testing as well as on interviews with customers who use these products in production environments. This ESG Lab report was sponsored by Fortinet.

Introduction

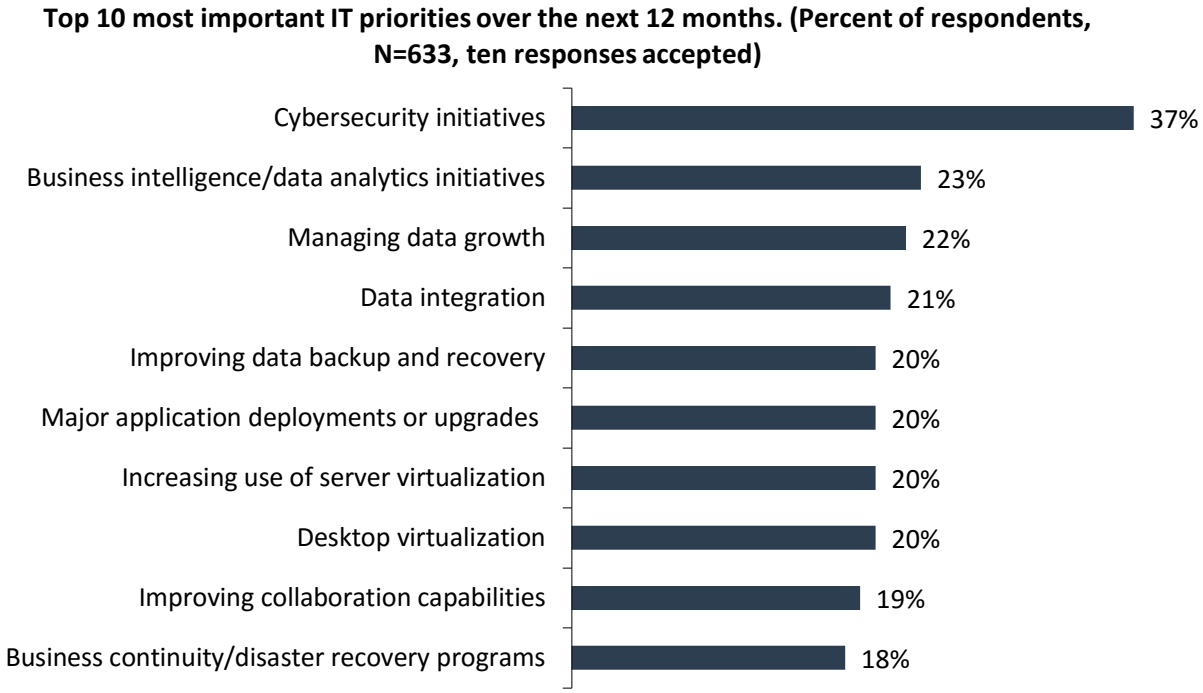
This ESG Lab Validation report documents hands-on testing of Fortinet Advanced Threat Protection (ATP) Framework, which is positioned as an end-to-end modular framework for addressing cybersecurity. Testing was designed to explore how the solution automates identification, prevention, and mitigation of malware, providing protection throughout the ecosystem. Fortinet's holistic approach, integrating coverage of multiple threat vectors and functions into a comprehensive solution, was also examined.

Background

Advanced malware attacks can cause tremendous damage to an organization, from stealing data through compromising identities to shutting down operations. The cyber-criminals perpetrating these attacks are sophisticated—continuously adapting the latest exploits, and creating new and insidious methods of infiltration and attack. Current malware is far more subtle and refined than the malware of the past, and is often camouflaged to prevent identification by traditional security systems.

Due in part to the ever increasing frequency of prominent public malware attacks, most organizations have become aware of the need to improve their IT security infrastructure. According to recently completed ESG research shown in Figure 1, 37% of surveyed organizations cited cybersecurity initiatives as one of their most important spending priorities for 2016, compared with 23% or fewer citations for all other priorities.[1]

Figure 1. Top Ten Most Important IT Priorities for 2016



Source: Enterprise Strategy Group, 2016.

In another survey, ESG asked IT professionals and managers to identify the biggest challenges facing their networking team. Implementing security within the network was cited by 35% of respondents.[2]

Organizations should be evaluating both their ability to detect threats and their ability to respond to those threats. Many of these advanced malware threats are referred to as "stealthy" or "zero-day." Stealthy threats are built to infiltrate systems undetected, sometimes hiding in an inactive state for a period of time before launching their

[1] Source: ESG Research Report, *2016 IT Spending Intentions Survey*, to be published.
[2] Source: ESG Research Report, *Trends in Data Center Networking*, to be published.

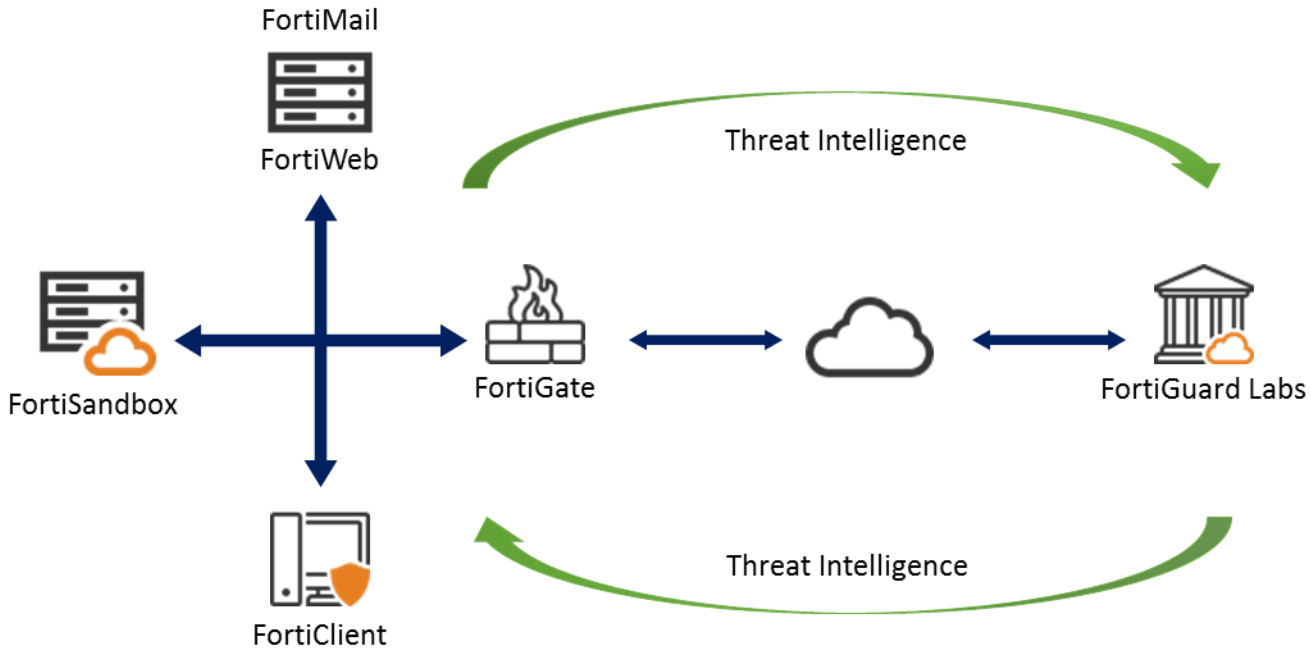
attacks. Zero-day threats attack a previously unknown vulnerability of a network, operating system, or application, making the malware difficult to combat.

Traditionally, security has been implemented with a perimeter firewall combined with client endpoint scanners. The perimeter firewall blocked simple attack techniques, preventing unauthorized users from accessing internal systems, while endpoint antivirus scanned user devices for specific file signatures of previously known or suspect malware. Next generation firewalls and endpoint protection platforms increase the depth of inspection at both the perimeter and computing device, but they still rely on searching for already known or suspect attacks, attack classes, and attack techniques. They are simply not designed to identify the newest, previously unknown threats. Far too often, organizations don't find out about such threats until severe damage has been inflicted.

Fortinet Advanced Threat Protection Framework

Fortinet has designed its ATP Framework with the goal of providing comprehensive visibility into all activity on and off the network, using established and emerging techniques, via a modular approach to integrating its network, application, endpoint, and cloud security products, as shown in Figure 2.

Figure 2. Fortinet Advanced Threat Protection Framework



The Advanced Threat Protection Framework includes:

- **FortiGate**—Next generation firewall combining deep packet inspection and application awareness for network security and threat protection.
- **FortiWeb**—Web application firewall to protect Internet facing applications and data. Bidirectional protection from advanced threats including denial of service, SQL injection, cross-site scripting, buffer overflows, file inclusion, cookie poisoning, and numerous other attacks.
- **FortiMail**—Email security gateway, protecting email users from inbound threats using antispam, anti-phishing, and anti-malware techniques. Outbound email protection includes data leakage prevention (DLP), identity-based encryption (IBE), and message archiving.
- **FortiClient**—Protection for Windows, Mac, iOS, and Android endpoint devices including but not limited to: anti-malware, application firewall, web filter, vulnerability management, two-factor authentication, and remote access.
- **FortiSandbox**—Centralized analysis and detection of potential threats using code emulation and virtual execution in a protected sandbox environment. Examines activity in addition to attributes to identify

undesired behavior. Dynamically generates threat intelligence for incident response and updated protection.

- **FortiGuard**—Fortinet researchers use information from global sources to investigate threats and attacks, and maintain a cloud-based threat research and response knowledgebase. Fortinet products automatically verify potential threats against the FortiGuard knowledgebase.

FortiGate, FortiWeb, and FortiMail are primarily distributed as both physical and virtual appliances, while FortiClient is software that runs on endpoint devices, to meet the needs of organizations of all sizes. Managed and cloud services are also available. Each ATP Framework product can operate as a standalone solution, or can be integrated with other products for expanded protection through interoperability. In the fully integrated framework, network and endpoint threat prevention products feed potential threat data to FortiSandbox for analysis, which in turn feeds intelligence back to those products as well as to FortiGuard and the broader Fortinet portfolio.

Fortinet describes the way its products work together to provide a coordinated defense in three phases: prevention, detection, and mitigation.

- **Prevention**—Prevent attack by/from many known or highly suspect threats.
- **Detection**—Identify previously unknown threats and share intelligence to speed response.
- **Mitigation**—Investigate and analyze new findings; create a fix and turn the unknown into the known for future prevention.

ESG Lab Validation

ESG Lab performed hands-on evaluation and testing of the Fortinet Advanced Threat Protection Framework at Fortinet facilities, in Sunnyvale, California. Testing was designed to explore how the overall solution integrates perimeter security, email and application threat defenses, and endpoint protection with FortiSandbox to automate identification of previously unknown threats, facilitate response, and provide protection throughout the Fortinet ecosystem. With that in mind, we examined the detection component first.

Detection

The primary Fortinet ATP Framework approach to advanced threat detection is to identify unknown threats and trends using FortiSandbox to uncover behaviors indicative of the tactics, techniques, and procedures (TTPs) used in cyber-attacks. FortiSandbox uses instrumented virtual machines to evaluate the threat potential of executable files as well as compressed archives (zip files) and application data, such as Adobe Flash, Adobe PDF, and JavaScript, among others. However, running each suspect file in a virtual machine can be resource intensive and take time. This can limit the total number of suspect files that can be evaluated, with a significant impact on productivity.

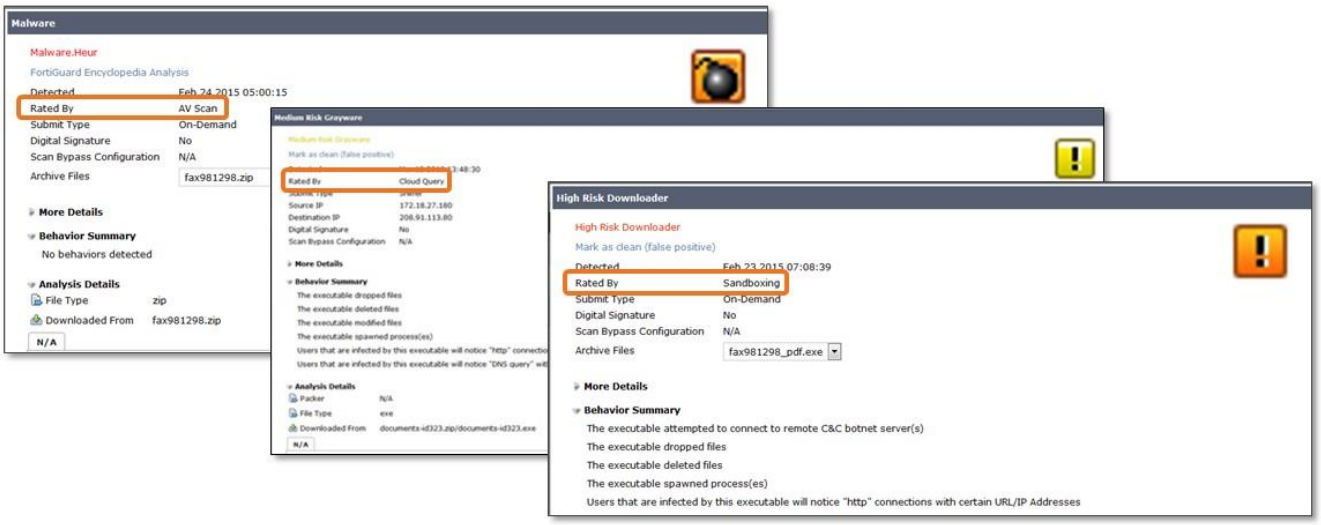
Fortinet applies many diverse methodologies to improve efficiency. Before execution in the sandbox, suspect files are subject to pre-filtering, including screening by an anti-malware engine, queries to Fortinet's FortiGuard cloud-based FortiSandbox Community results, and OS-independent simulation, which is made possible by the Fortinet patented Compact Pattern Recognition Language (CPRL). CPRL is a deep code inspection and pattern recognition system that helps cast a wider net over the attacks and methods of modern advanced persistent threats (APTs) and advanced evasion techniques (AETs) than is possible with traditional signature matching.

ESG Lab Tested

ESG Lab reviewed Fortinet notifications of detected threats. As shown in Figure 3, every threat notification includes a ***Rated By*** tag, indicating the method used for detection, and includes:

- **AV Scan**—The threat was detected when the signature of a file found during a scan of the storage system matched a signature known to FortiClient.
- **Cloud Query**—If the signature of a file is not known to FortiClient, the signature may be matched by FortiGuard, the Fortinet cloud-based advanced threat knowledge base.
- **Sandboxing**—The threat was detected when FortiSandbox evaluated the behavior of the file.

Figure 3. Threat Detection by Digital Signature, Cloud Query, and Sandboxing



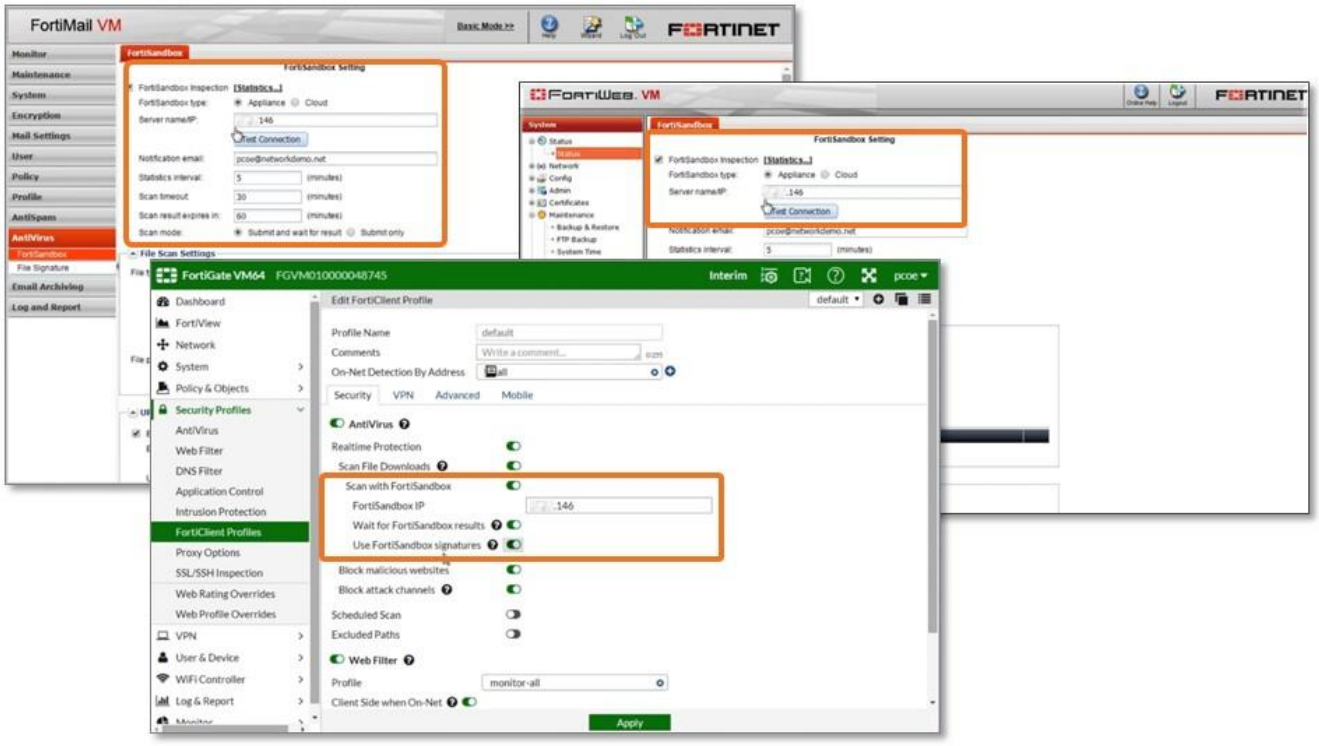
Notifications also come with a risk rating (clean, low risk, medium risk, high risk, or malicious). The ***Results*** tab contained significant details about the code and its rating, including a behavior summary, screen shots of the malware, and the ability to download additional log information.

In this case, the behaviors resulting in the high-risk rating included:

- The executable attempted to connect to remote C&C botnet server(s).
- The executable dropped files.
- The executable deleted files.
- The executable spawned processes.
- Users infected by this executable will notice “http” connections with certain URL/IP addresses.
- Users infected by this executable will notice “DNS query” with certain domain names.

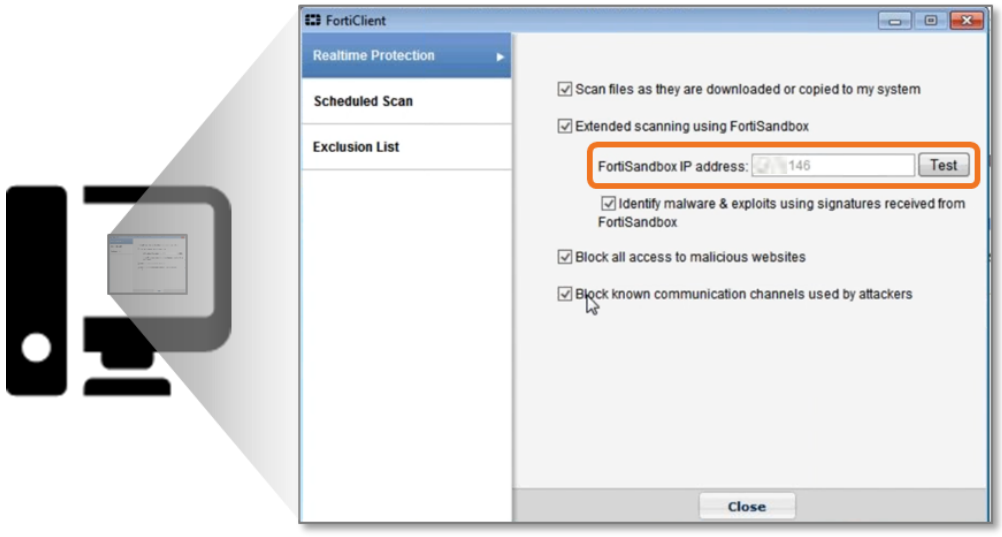
FortiSandbox can extract objects for analysis directly from network traffic or receive them from other Fortinet products already inspecting traffic. ESG Lab reviewed the integration of FortiSandbox with the major components of the Fortinet ATP Framework—FortiGate, FortiWeb, and FortiMail. Configuration of these products to use FortiSandbox was simple, only requiring the administrator to enter the IP address of the FortiSandbox server in the module’s FortiSandbox configuration section. The next and final step was to use the FortiSandbox configuration to click to authorize the connection between FortiSandbox and the ATP module.

Figure 4. Registering Fortinet ATP Framework Components with FortiSandbox



FortiSandbox is also an integrated extension of FortiClient. Administrators can manually configure the FortiClient endpoint protection, or they can configure an endpoint protection profile from within FortiGate. This profile will be applied to a group of endpoints within the environment. ESG Lab manually configured FortiClient running on a Windows 7 workstation. From the FortiClient configuration, we selected the ***Realtime Protection*** tab, and then entered the FortiSandbox server IP address into the configuration. After using FortiSandbox to authorize the client, we clicked ***Test*** to verify the connection, as shown in Figure 5.

Figure 5. Registering FortiClient with FortiSandbox

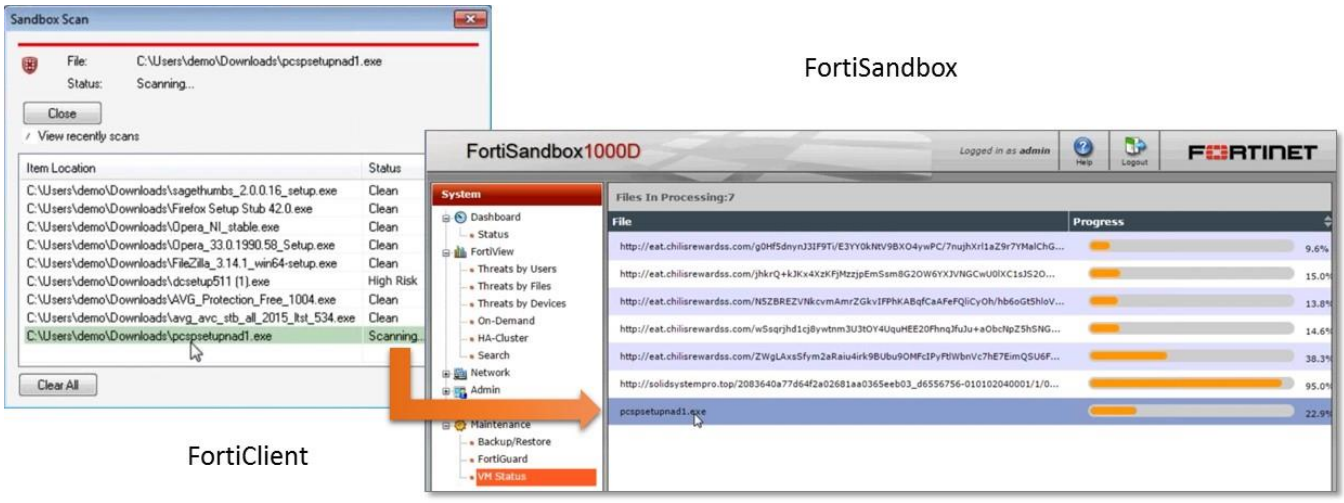


To see how integrated products worked with FortiSandbox, using FortiClient as an example, we used a web browser to download a program from a file downloading site, mimicking everyday behavior found throughout enterprise environments. We saved the file *pssplsetupnad1.exe* to the local disk, as shown in Figure 6.

Figure 6. Downloading an Unknown File

We then executed the file to install the program. FortiClient automatically scanned the file and generated a file signature. Because the file signature was unknown to FortiClient, it automatically sent the file to FortiSandbox to be evaluated for threats. The FortiClient sandbox scan status, shown on the left of Figure 7, showed that a number of downloads had previously been scanned and generally the results were clean—although one was rated high risk. The status display also showed that FortiSandbox was in the process of evaluating the current file *C:\users\demo\Downloads\pcspsetupnad1.exe*.

Figure 7. Automatically Scanning the File with FortiSandbox



ESG Lab also reviewed the evaluation status on FortiSandbox. Sandbox evaluations are performed in virtual machines, as can be seen on the right-hand side of Figure 7. There were seven simultaneous threat evaluations running in virtual machines. At the end of the evaluation, FortiSandbox reported that the file was clean, showing no bad behaviors. FortiSandbox updated all integrated components so that subsequent downloads would not require a repeat evaluation.

Why This Matters

The threat landscape has grown more dangerous for critical infrastructure organizations over the last two years. Nearly one-third (31%) of surveyed organizations believe that the threat landscape—cyber-adversaries, cyber-attacks, exploits, malware, etc.—is much worse today than it was two years ago, while another 36% say that the threat landscape has grown somewhat worse in the past two years.[3] Despite 91% of these organizations rating their cyber security policies either good or excellent, the overwhelming majority of these organizations (68%) report experiencing some type of security incident in the same time period.

It is clear that a consolidated approach that integrates multiple threat detection and assessment techniques, where in-place security can hand files off to a sandbox for additional analysis, can provide an important extra layer of defense and close gaps easily exploited by new and previously unknown advanced threats.

ESG Lab confirmed that integrating FortiSandbox into the Fortinet Advanced Threat Protection Framework was straightforward, requiring just a few steps. Once integrated, the ATP Framework can provide fast, accurate detection and analysis of previously unknown threats leveraging the analysis of file activities and attributes by FortiSandbox.

Based on hands-on testing, ESG Lab concluded that Fortinet's integrated approach can offer a consolidated, multi-layered detection of previously unknown threats from multiple sources using FortiSandbox to enhance the protection offered by Fortinet's traffic inspection, endpoint protection, web application, email, and firewall security appliances.

Mitigation

The Fortinet unified approach to protection is designed to mitigate the previously unknown threats and attacks identified by FortiSandbox. In the context of cybersecurity, mitigation is defined as reducing the likelihood of unwanted occurrences and/or lessening their impacts and consequences by the application of measures to reduce the likelihood of an unwanted occurrence and/or lessen their consequences. All Fortinet components that integrate with FortiSandbox submit items for analysis and use the data provided by FortiSandbox to speed response and mitigate newly identified threats.

ESG Lab Tested

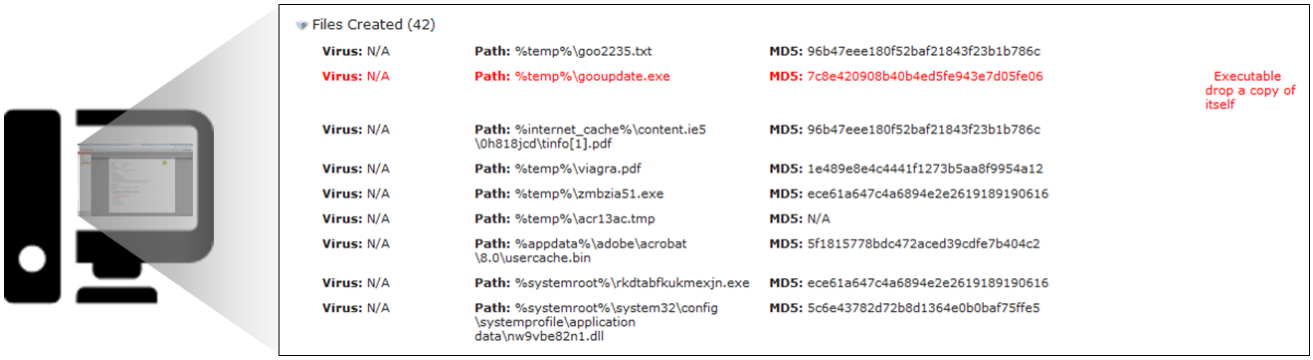
Administrators are provided with the ability to drill down into the details of the behaviors exhibited by the malware in order to rapidly validate risk ratings. The details are contained in an expandable dynamic list. By clicking on the triangle icon on the left, ESG Lab expanded the details for suspicious behaviors and botnet info, as seen in Figure 8.

[3] Source: ESG Research Report, *Cyber Supply Chain Security Revisited*, September 2015.

Figure 8. Malware Suspicious Behavior and Botnet Info Details

In this case, FortiSandbox reported five suspicious behaviors, detailing that the malware behaved as a rootkit, created a copy of itself, and deleted itself after execution, making remediation more difficult. As these behaviors are potentially very damaging, they were highlighted in red.

Figure 9. Files Created by Malware

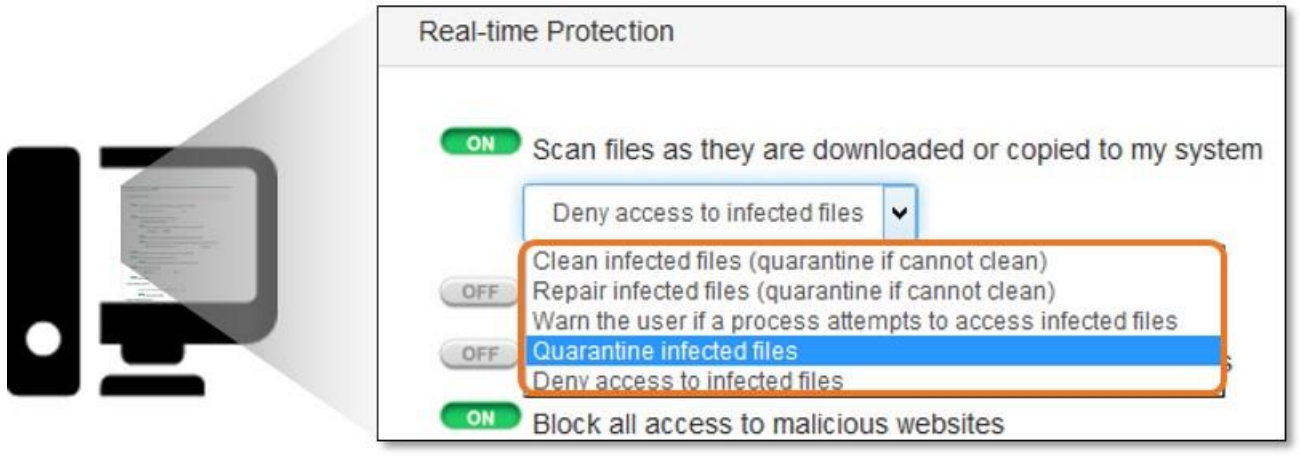


The expansion of the ***Files Created*** section, shown in Figure 9, provides information on each of the 42 files created, with the path and the MD5 checksum for each file. Potentially dangerous activity, such as creating a copy of itself, is highlighted in red.

The ***Results*** tab also provided the administrator with the ability to download a copy of the original file from FortiSandbox, along with a tracer log detailing each action of the analyzed file, a screenshot, and all of the captured packets from the malware-initiated network traffic.

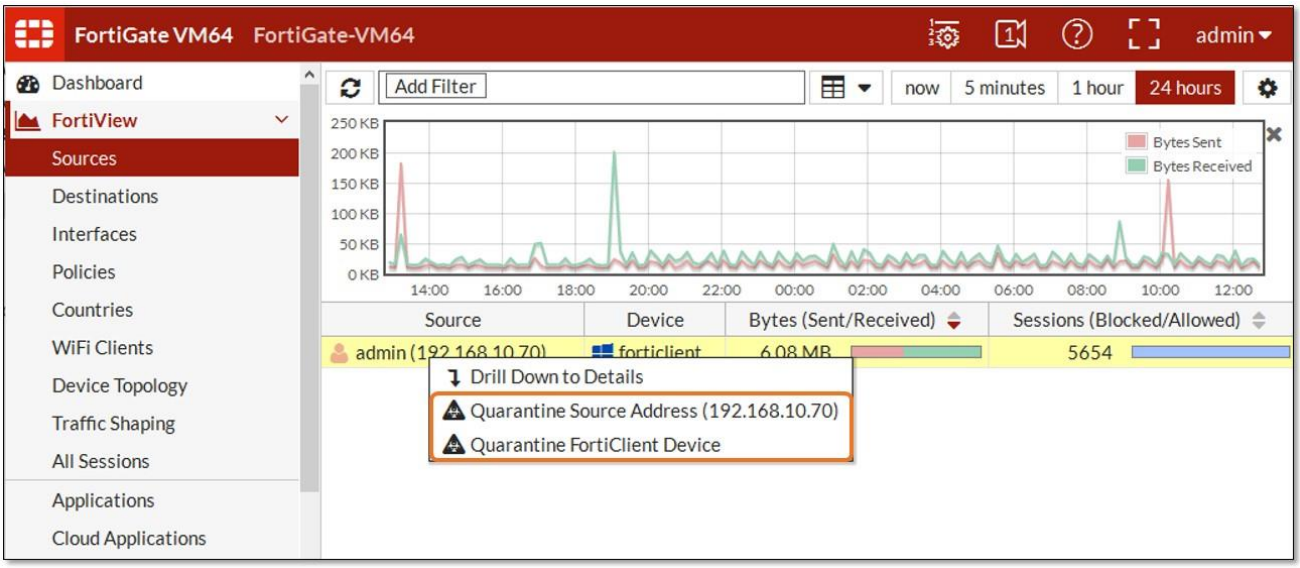
Once positive identification is made, mitigation can be automatic, based on policies that can be set at each control point. Figure 10 shows the configuration options in FortiClient.

Figure 10. FortiClient Mitigation Options



Mitigation can be applied at any control point in the ecosystem. FortiGate, FortiWeb, and FortiMail offer quarantine options; Figure 11 shows how FortiGate can quarantine both an infected device and the source of the infection. FortiWeb has similar options.

Figure 11. Quarantining an Infected Client with FortiGate



Why This Matters

ESG research has found that 31% of organizations surveyed identify new malware threats as the consideration having the most significant influence on their endpoint security strategy moving forward.[4] In addition, nearly half (47%) of cybersecurity professionals working at critical infrastructure organizations claim that security incidents required significant IT time and personnel for remediation.[5] The ability to automate and assist as much of the mitigation of these attacks as possible and minimize or eliminate manual processes is critical.

ESG Lab confirmed that Fortinet's unified approach to security can deliver fast, accurate detection and analysis of potential threats. FortiSandbox can improve efficiency by implementing a consolidated approach, providing coverage for a wide variety of protocols and file types as well as universal sandbox functionality for potential threats from any source.

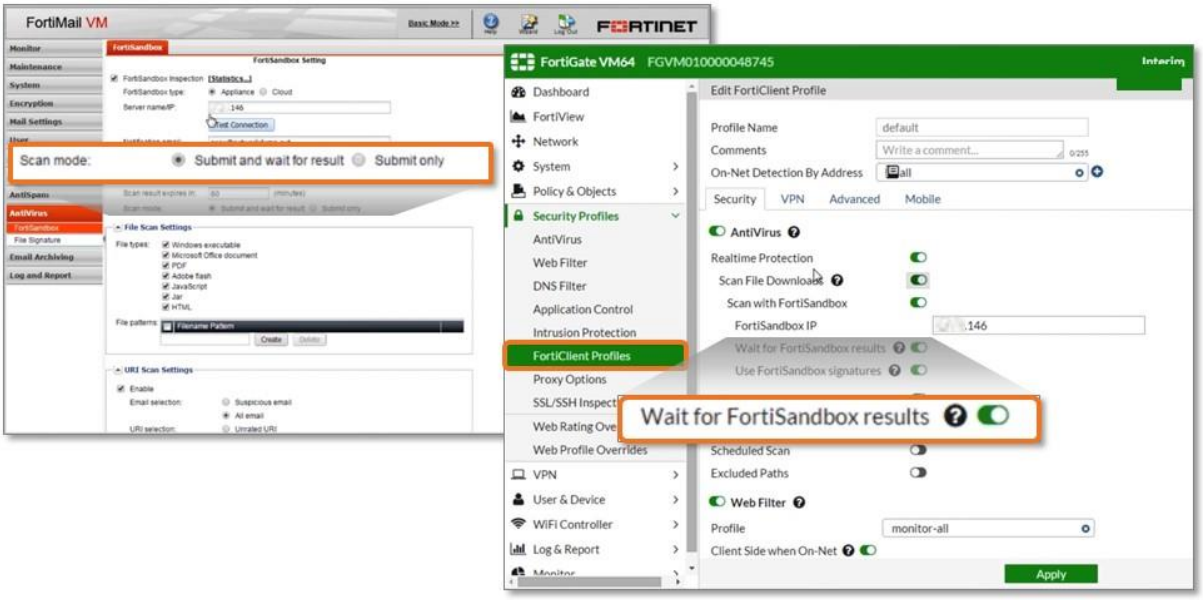
Based on hands-on testing, ESG Lab validated that Fortinet's integrated security ecosystem can provide consolidated mitigation and remediation while enabling administrators to implement automated response to threats and attacks and assisted response to incidents requiring intervention. Integration with Fortinet FortiSandbox enabled this automation across threat vectors based on information shared with Fortinet's control points, which leverage that data to isolate and clean infected systems.

Prevention

The least problematic attack is the one prevented from occurring in the first place. Fortinet's ATP Framework automates and consolidates analysis of suspicious files across all control points from multiple potential vectors using techniques including direct traffic inspection and integrations with FortiGate, FortiClient, FortiWeb, and FortiMail security appliances, with the objective of preventing as many attacks as possible to reduce the load on FortiSandbox and minimize the need for manual, labor-intensive response to preventable attacks.

In addition to using the traditional threat prevention technologies in these products—examples include application control, intrusion prevention, web filtering, antivirus, and antispam—to block known threats and attacks, FortiSandbox analysis plays an important role in preventing even the most advanced threats.

Figure 12. Configuring FortiClient and FortiMail to Wait for FortiSandbox Results

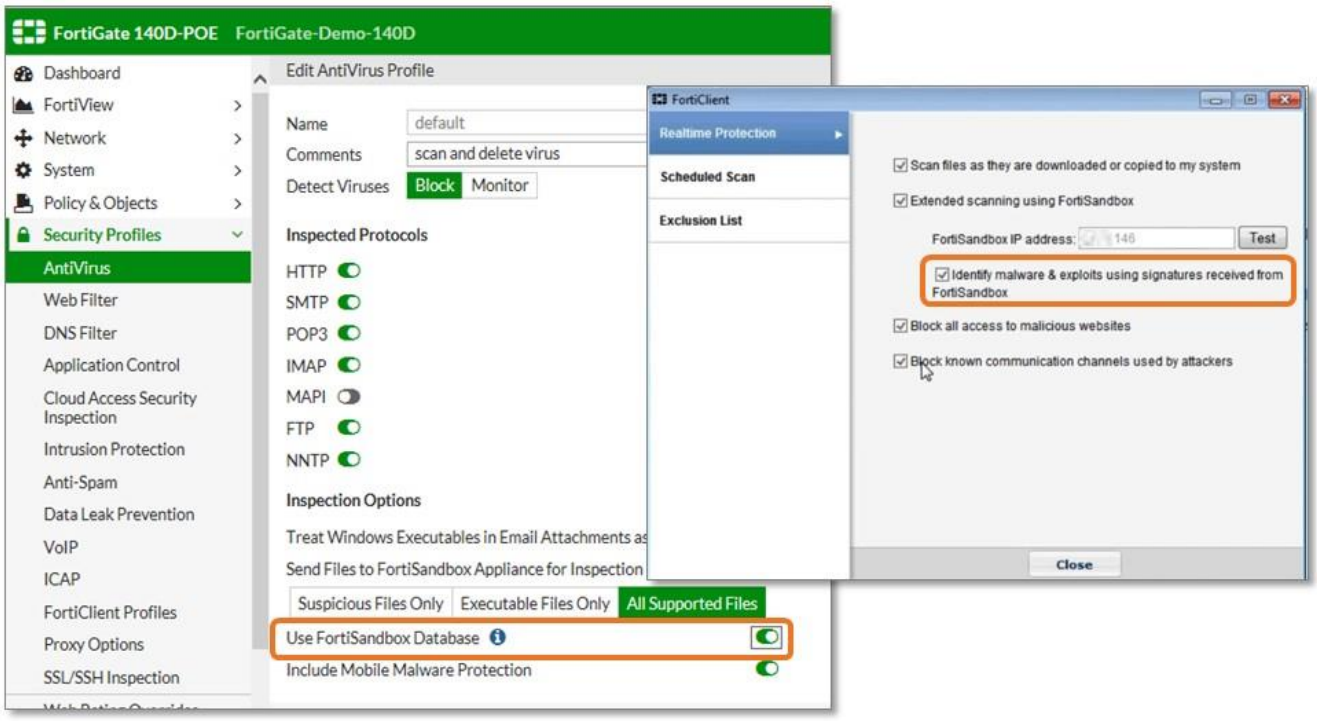


[4] Source: ESG Research Report, *The Endpoint Security Paradox*, January 2015.
[5] Source: ESG Research Report, *Cyber Supply Chain Security Revisited*, September 2015.

First, FortiMail and optionally FortiClient automatically hold unknown files and wait for FortiSandbox analysis before allowing delivery or installation, avoiding the need for mitigating response as seen in Figure 12.

Then FortiGate and FortiClient can be configured to receive signature updates directly from an integrated FortiSandbox, seen in Figure 13, in order to prevent targeted attacks from gaining entry at multiple points as well as multi-stage attacks whose later components are proactively uncovered by FortiSandbox before they are encountered by end-users.

Figure 13. Configuring FortiGate and FortiClient to receive Signature Updates



Finally, FortiSandbox can optionally share threat data from its analysis with FortiGuard labs, allowing the creation of broader one-to-many protections that can be distributed to the full Fortinet threat prevention portfolio—beyond those integrated directly with a FortiSandbox—strengthening protection for the entire community.

Figure 14. FortiSandbox Intelligence Sharing with FortiGuard

Why This Matters

Security breaches have become increasingly common, with targeted attacks and zero-day malware evading traditional, standalone security solutions. Organizations relying on these types of solutions can potentially find themselves vulnerable to attacks with serious financial and operational consequences. Prevention enables organizations to get out of reactive mode and focus on proactive, strategic activities to strengthen their security posture. Leveraging the advanced detection capabilities of FortiSandbox and the deep global knowledge of threats from FortiGuard Labs can give organizations the context and tools they need to prevent attacks before they happen.

ESG Lab confirmed that Fortinet FortiSandbox can dynamically generate and distributes intelligence that enables other Fortinet threat prevention products to immediately start blocking previously unknown threats. FortiSandbox also offers intelligence transfer with FortiGuard labs to ensure that when a previously unknown threat is detected, it becomes known throughout the Fortinet portfolio for customers anywhere in the world.

Based on hands-on testing, ESG Lab concluded that Fortinet's integrated approach can help prevent attacks before they happen by cross-correlating knowledge across all control points.

ESG Lab Validation Highlights

- ☑ ESG Lab found Fortinet's components and user interface to be easy to configure and use. Fortinet provides clear understanding of an organization's current security posture from top level to detailed forensic views, and the integration of FortiSandbox throughout the environment enhances the ability to detect threats quickly.
- ☑ Fortinet FortiSandbox is able to consolidate analysis of suspicious files from direct traffic inspection as well as integrations with FortiGate, FortiClient, FortiWeb, and FortiMail security appliances while those same products offer control points that leverage FortiSandbox data to help mitigate and often prevent previously unknown attacks through assisted or fully automated actions.
- ☑ ESG Lab confirmed that FortiSandbox provides deep context that can aid response teams and/or Fortinet control points to prevent threats from becoming full-on compromises and data loss incidents. The ability to hold for FortiSandbox analysis and quarantine after, if necessary, can be particularly powerful and efficient.
- ☑ FortiSandbox also provides optional intelligence transfer with FortiGuard labs so when a previously unknown threat is detected, threat intelligence can be shared more broadly throughout the Fortinet portfolio of security products and by customers anywhere in the world.
- ☑ ESG Lab found through hands-on testing that Fortinet's integrated approach simplified analysis of data from multiple diverse sources, enabling efficient use of the data gathered by FortiSandbox to accelerate response processes. This enables organizations to prevent attacks when possible, detect attacks when necessary, and mitigate threats quickly.

Issues to Consider

- ☑ While the operation of Fortinet FortiSandbox and its integration with the ecosystem of Fortinet security products proved to be straightforward, the tests were performed in a lab environment and were not designed to prove efficacy. Due to the many variables in each production environment, planning and testing in users' own environments is recommended.

The Bigger Truth

Security breaches are becoming a very common occurrence. Any computing device in the corporate infrastructure, from smartphones and tablets to laptops, desktops, and application servers, are all susceptible. Attacks affect organizations of any size indiscriminately, and the consequences can be devastating to operations, company reputations, and bank accounts. The costs stemming from successful attacks may include not just resuming operations and addressing security gaps, but legal liability and regulatory fines that can be a tremendous burden as well.

This may be why information security has remained at the top of the IT priority list for the last four years, according to ESG research. When asked to consider their organizations' most important IT priorities for 2016, information security initiatives were the most often cited, identified by 37% of respondents.[6]

ESG Lab found that the Fortinet Advanced Threat Protection Framework is easy to understand and manage. Fortinet's modular approach, with standalone products that can be integrated for interoperability and greater prevention, detection, and mitigation can enhance advanced threat detection or prevention beyond what is possible with other standalone systems. Integrating FortiSandbox to FortiGate Next Generation Firewall, FortiMail Secure Email Gateway, and FortiClient Endpoint Protection was quick and simple in our lab testing. Once configured, analysis of unknown files, regardless of how they were introduced into the environment, was automatic. The FortiSandbox dashboard provided intuitive access to clear information. FortiSandbox made understanding the current security posture clear and easy to parse. Further, ESG Lab was able to quickly gain comprehensive visibility and drill down into a specific threat quickly.

The data gathered and the assisted and/or automated responses of the Fortinet Advanced Threat Protection Framework enables organizations to accelerate response processes, preventing known attacks, detecting unknown threats, and converting those unknown threats into the currently known and prevented.

The Fortinet ATP Framework can offer the features, capabilities, and integration that can address organizations' security requirements, providing security teams with the ability to detect, prevent, and mitigate malware. The ability to operate as standalone products or integrate into the Fortinet comprehensive Advanced Threat Protection Framework can also provide the flexibility to fit into most any environment. Businesses looking for a flexible, efficient solution to improve its security posture would be well-served by giving the Fortinet Advanced Threat Protection Framework serious consideration.

[6] Source: ESG Research Report, *2016 IT Spending Intentions Survey*, to be published.

Appendix

Table 1. ESG Lab Test Bed

Network Security Infrastructure	Version
FortiSandbox 1000D	2.11
FortiGate VM	FortiOS 5.4
FortiMail VM	5.3
FortiWeb	5.4
FortiClient Software	5.4
Virtualization Infrastructure	Guests/Endpoints
VMWare vSphere 5.1	Windows 7 Professional Windows 8.1

Enterprise Strategy Group | **Getting to the bigger truth.**

20 Asylum Street | Milford, MA 01757 | Tel: 508.482.0188 Fax: 508.482.0218 | www.esg-global.com