FORTINET

WHITE PAPER

How to Create
Sandbox-as-a-Service for MSSPs

How to Create Sandbox-as-a-Service for MSSPs

Table of Contents

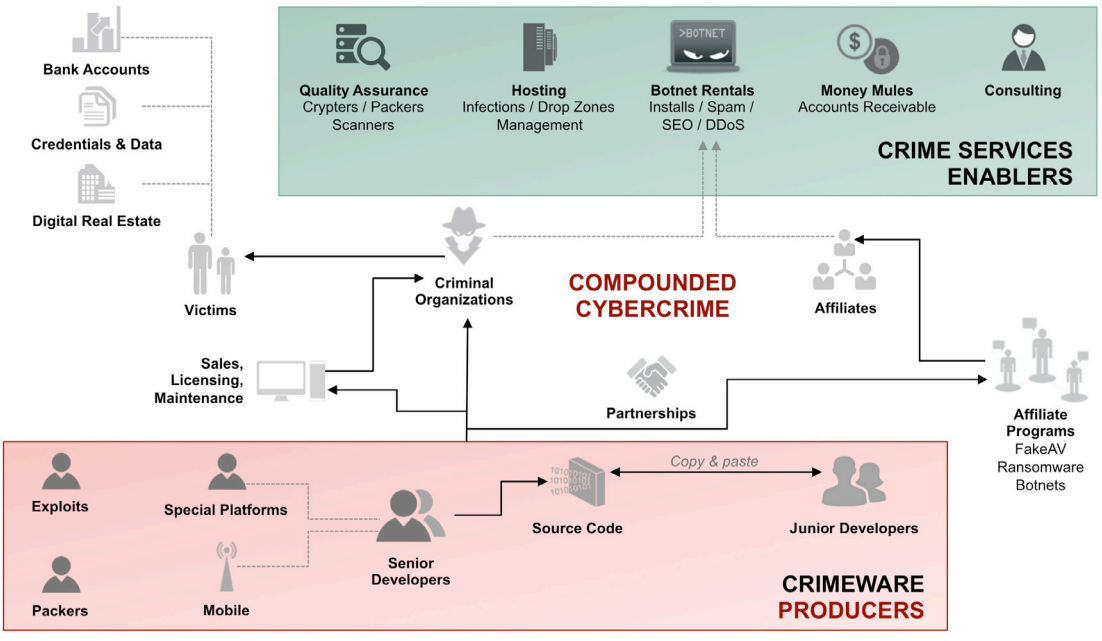
How to Create Sandbox-as-a-Service for MSSPs

Introduction

Advanced Persistent Threats (APTs) and the growing Cybercrime Ecosystem are changing the way companies need to protect their networks. Recent high-profile security breaches indicate that even well-defended businesses are at risk and traditional methods of defending the enterprise are increasingly ineffective.

APTs are sophisticated attacks that seek to gain and maintain access to well-defended targets. They combine multiple targeting methods, breach tools, and techniques to gain access and maintain it for ongoing exploitation. APTs evade traditional detection methods, capitalizing on social engineering tricks, unknown exploits, unpatched vulnerabilities, or missing signatures in signature-based controls. In addition to APTs, the ever-growing Cybercrime Ecosystem consists of mature service enablers such as exploit writers, botnet rentals, and skilled consultants that are readily available to offer experienced assistance to hackers of all skill levels.

The migration of key business applications to the cloud, the explosion of mobile devices on corporate networks, and the increasing competency and organization of hacker networks are causing the threat fabric to increase exponentially. Companies today need adaptive, real-time threat protection to combat this new breed of attacks.



A Rising Trend with Measurable Losses

In 2013, there was a 91% increase in targeted attacks with 23 zero-day threats and a 61% increase in successful breaches.[1] This trend continued in 2014, with several high-profile attacks successfully breaching large, well-defended targets. According to the Verizon 2014 DBIR, last year a total of 511 incidences of cyberespionage were conducted by state-affiliated attackers, with 306 successful breaches[2]—a 60% effectiveness rate.

U.S. businesses alone lose $250 billion annually, with another $114 billion lost due to cybercrime.[3] Former NSA chief Gen. Keith Alexander best described it as the "greatest transfer of wealth in history." It is no wonder that the average time attackers were on a company's network before detection is 229 days. 67% of the victims were notified by an external entity.

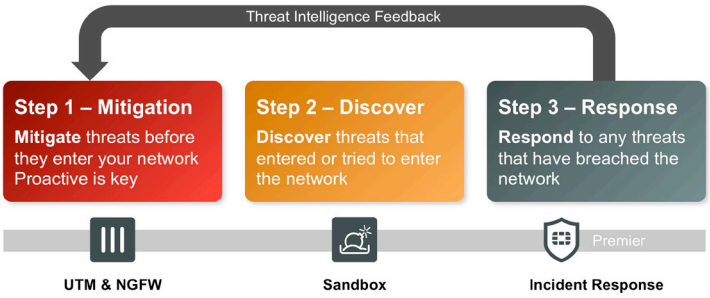
Once a target is compromised by an attack, the company's critical infrastructures can be crippled, in addition to money or intellectual property being stolen.

The Emergence of Managed Security Services

The increasing complexity and persistence of attacks combined with the threat condition and the high stakes at-hand have created a cybersecurity arms race, requiring companies to stay one step ahead. Renewed boardroom pressure to keep enterprises secure is driving the investment in advanced security technologies and Managed Security Services (MSS). Businesses of all sizes are turning to Managed Security Service Providers (MSSPs) to anticipate and mitigate risks with advanced security technologies, incidence response, and professional security services.

Fortinet applies a three-step approach to providing intuitive and effective security solutions for MSSPs:

1. **Mitigation** – Identify and protect against known threats before they enter the network. Partners typically achieve this by leveraging Fortinet's Unified Threat Management (UTM) and Next-Generation Firewall (NGFW) products in combination with FortiGuard security services and threat intelligence.
2. **Discover** – Once technology is in place for protection against known threats, the next step is to discover the unknown threats that have already entered or tried to enter the network. FortiSandbox enables this step in the process.
3. **Response** – In cases where malware has been able to circumvent the first two levels of protection, a different system must be able to quickly respond to threats and effectively neutralize them. FortiGuard's Premier Incident Response service can help with malware analysis and custom signature creation to contain these sorts of breaches.



Many companies offer solutions that address the first step of mitigating known threats. Recent studies have shown, however, that almost 95% of today's malware can evade current firewalls and traditional antivirus engines. This trend has increasingly led companies to deeper-level solutions in the second ("discover") and third ("response") steps to keep up with the ever-evolving threat landscape. Their intuitive effectiveness comes from the fact that these higher levels of security establish a threat intelligence feedback loop to enhance the mitigation step of protecting against known viruses.

What is a Sandbox?

A sandbox is defined as an isolated and controlled environment used to observe the behavior of a file. When a suspicious file is sent to the sandbox, a virtual OS is spun up for observation. The attachment is then opened and executed in the virtual instance. The sandbox analyzes the behavior of the file and determines if it is potentially detrimental to the target (in this case, the IT infrastructure of a business). Once that assessment occurs, a decision on how to handle the file in question can be made.

While sandboxing is not new technology, its use in cooperation with firewalls and email security running dynamic threat intelligence and APT countermeasures is a more recent development. Today, sandboxing has become "service-enabled"—using virtualization and being directly integrated into perimeter enforcement.

Sandboxing is recognized as an excellent approach for protecting key infrastructure from APTs, but to date, the associated costs have limited its wide adoption. Sandboxing has traditionally been an expensive and resource-intensive protection method—primarily the domain of enterprises with large IT security budgets.

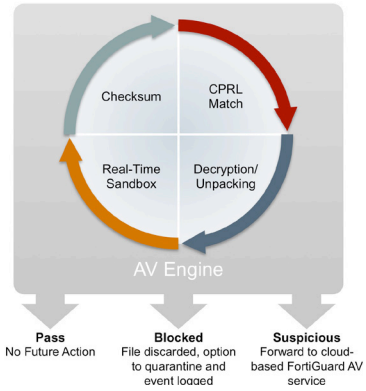
In selecting a vendor's sandboxing solution, some questions to ask in the qualification process would be:

1. How does this sandbox complement the existing security solutions in place?
2. How well does this sandbox virtualize and support multi-tenancy?
3. How to minimize one's hardware investment while maximizing one's security profile?

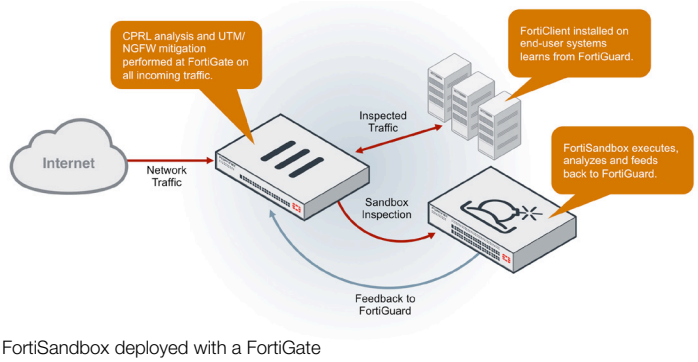
In this white paper, we'll explore Fortinet's creation of MSS that increases overall security effectiveness, complements existing FortiGate or FortiMail base solutions, and enhances a comprehensive security services portfolio. The combination of FortiGate firewall devices running UTM and FortiGuard subscription services used in conjunction with FortiSandbox creates cooperative, layered, and highly adaptable security architecture.

Fortinet's Cooperative Security Strategy and Specialization of Labor

Fortinet uses a combination of UTM, email security, and FortiGuard technologies to reduce issues, which leads to low false positives, less inspection overhead, greater accuracy, and better catch rates. Fortinet's high performance and low false positives come from a dynamic scanning protocol based on a custom Compact Pattern Recognition Language (CPRL) and ASIC hardware acceleration. This combination delivers fast, powerful detection, unique to Fortinet, using a single signature to identify tens of thousands of variations of viral code.



This patented way to identify an attack or evasion emulates malicious code to understand what it is attempting to do and explores all the different code paths for attack vectors. Since CPRL is not as CPU-intensive as spinning up a virtual OS, Fortinet's sandbox solution (FortiSandbox) uses CPRL as the first pass as it scans traffic. CPRL typically catches about 60% of malicious traffic. CPRL tags threat traffic as suspicious, malicious, or unknown. Traffic classified as malicious is eradicated immediately while suspicious and unknown traffic is sent to the sandbox. Attacks or evasion techniques that are uncovered through this process are then reported back to FortiGuard to further enhance the protection ecosystem.



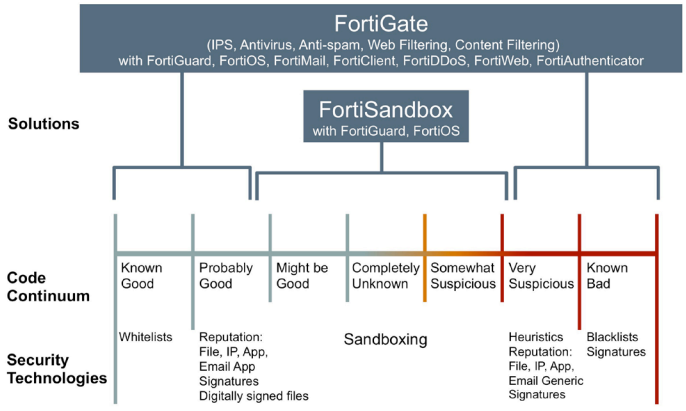
FortiSandbox deployed with a FortiGate

For an MSSP already leveraging Fortinet firewalls and FortiMail in their managed security offerings, launching a Fortinet Sandbox-as-a-Service makes sense from several perspectives. FortiGate firewalls are already FortiSandbox compatible and support proprietary protocols and threat intelligence that improve performance and security effectiveness.

Whether the FortiGate is local or hosted, simply connect the device to the sandbox and the MSSP can start gathering data. The benefits of combining the Advanced Threat Protection of the FortiSandbox with the global FortiGuard network could create additional layers of protection against ever newer, more insidious threat vectors.

FortiSandbox becomes more powerful when used in conjunction with FortiGate as a result of:

- Streamlined redirection of suspicious files with low false positives
- Integration with FortiGuard Threat Intelligence and signature updates
- Simple deployment and "flip of the switch" turn-up
- Updated inline protection
- The ability to send every file download and email attachment to the sandbox for analysis if desired



Combined Sandbox and Email Security

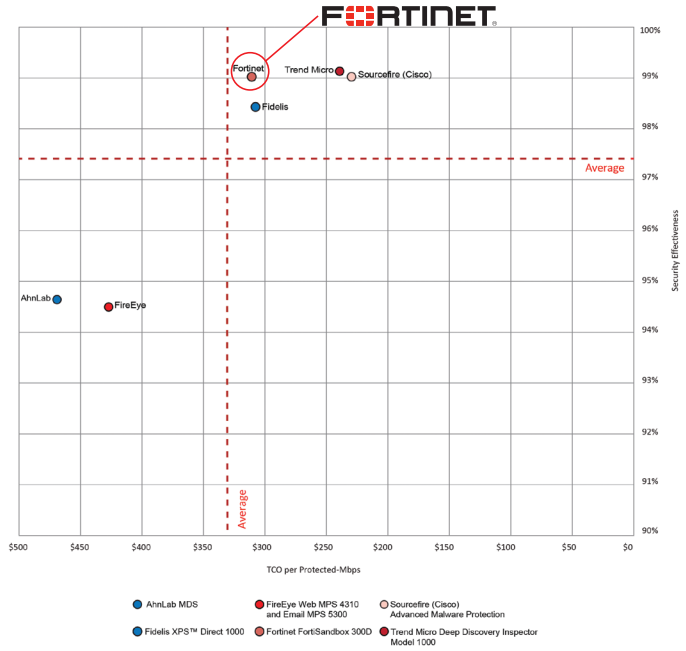
Based on Verizon's 2014 DBIR, email attachments constituted 78% of the attack vectors perpetrated by state-sponsored cybercriminals. Tying email security to sandboxing makes tremendous sense when considering countermeasures to this highly successful and flexible method of attack.

In 2014, FortiSandbox was awarded NSS Labs "Recommended" status, which indicates a product has performed well while also representing a good value, and deserves strong consideration following real-world testing. During these tests, NSS Labs technicians tested industry-leading sandbox solutions from many vendors. These tests were designed to grade each solution based on security effectiveness, performance and stability, management of multiple devices, and Total Cost of Ownership (TCO). FortiSandbox scored a 99% breach detection rate at 1Gb of throughput with 0% False Positives. FortiSandbox also passed all stability and reliability tests and had one of the lowest TCO-per-protected Mbps ($309).

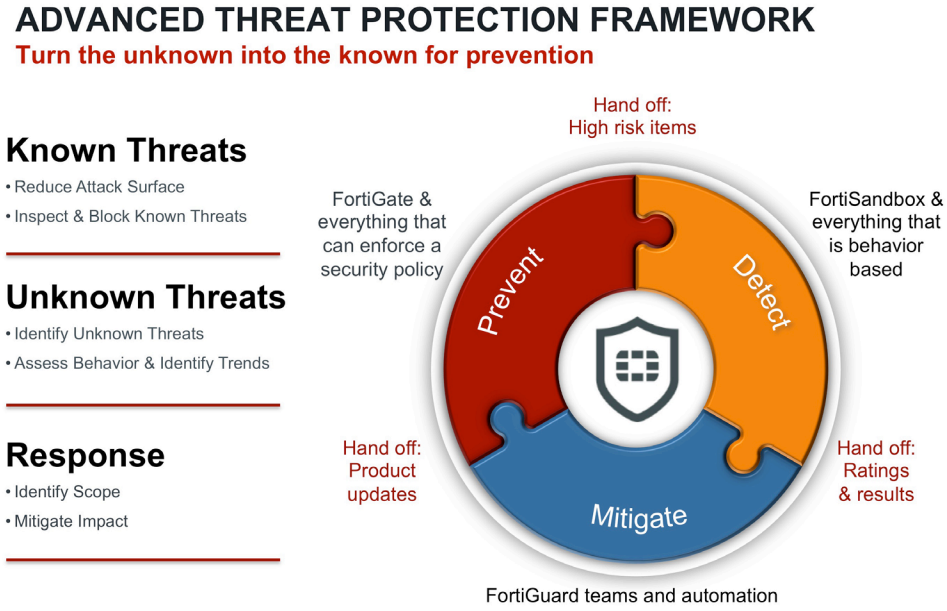
Leveraging Fortinet's FortiMail email security in conjunction with FortiSandbox and FortiGate firewalls creates a highly effective and scalable defense. At present, FortiMail is the second most popular product deployed as a service by Fortinet MSSPs—behind FortiGate firewalls—due primarily to its native multi-tenancy, high catch rates, low false positives, and cost-effective scalability.

For MSSPs offering email security, FortiSandbox used in combination with FortiMail offers a compelling value proposition for providers and customers alike, and should be considered part of a comprehensive layered security strategy.

MSSPs encounter better detection rates when combining the functionality of FortiGate and FortiMail. Introducing FortiMail into the sandbox architecture provides automatic detection and mitigation of malicious attachments, phishing and spam—something that other vendors cannot do as effectively. If a customer already has FortiGate firewalls, these devices automatically become sensors at all ingress and egress points, thereby eliminating the cost of purchasing new sensors for every location.



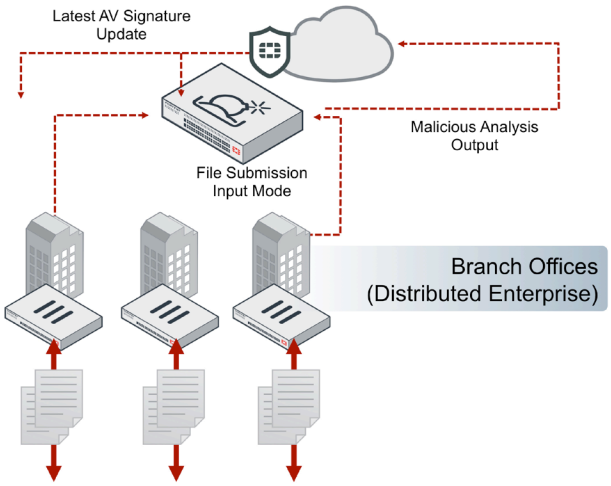
NSS Breach Detection Systems (BDS) Security Value Map™



Deployment Methods and Detection Modes

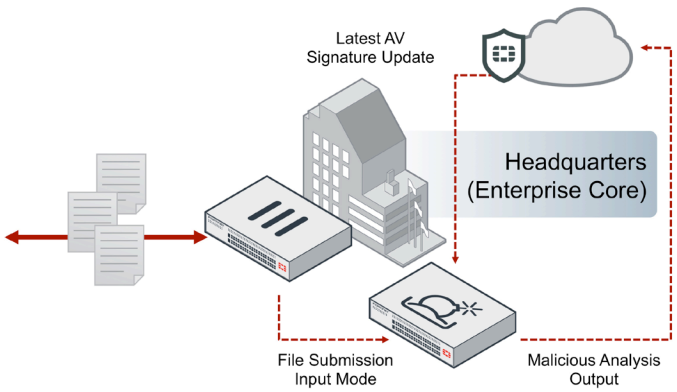
FortiSandbox is the most flexible threat analysis solution available today. It offers deployment options that are suitable to the unique setup and requirement needs of different customers.

In-line Distributed Enterprise deployments are attractive for MSSPs with multi-location customers, where FortiGates are deployed in the branch offices and submit suspicious files to a hosted FortiSandbox. This setup yields the benefits of lowest TCO. It protects against threats in remote locations while allowing the MSSP to employ economies of scale to reduce the cost of the service. (For planning purposes, 500 would be the absolute maximum number of deployments; 100 would be a more optimal target, as determined by files-per-hour/devices on a single sandbox instance.)



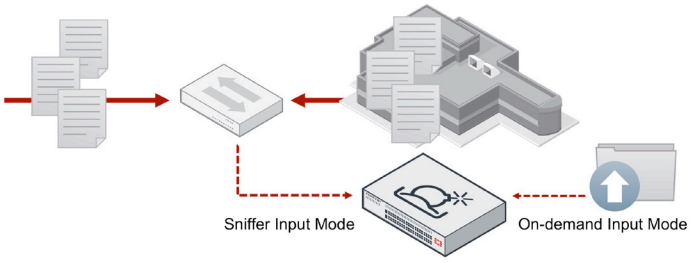
Distributed Deployment

FortiGate can be configured as an **In-line Core Deployment** to submit suspicious files only or all files to the FortiSandbox for inspection. This seamless integration reduces network complexity and expands the applications and protocols supported including those that are SSL encrypted, such as HTTPS.



Core Deployment

There are three detection modes for importing files to FortiSandbox. In **sniffer mode**, the FortiSandbox sniffs traffic on a specified interface, reassembles files, and analyzes them. In **device mode**, FortiGate or FortiMail is configured to send suspicious files or all files to FortiSandbox for analysis. **On-demand** allows for upload of executable files or archived executable files directly to FortiSandbox for analysis.



FortiSandbox Detection Modes

FortiSandbox executes code in a contained virtual environment and the output is analyzed to determine the characteristics of the file. Inspection is run post-execution and all aspects of the file are examined. FortiSandbox checks files for the following malicious characteristics:

- Known virus downloads
- Registry modifications
- Outbound connections to malicious IP addresses
- Infection of processes
- File system modifications

FortiSandbox can process multiple files simultaneously because it has a VM pool to dispatch files into for sandboxing. The time to process a file is hardware dependent; it can take anywhere from 30 seconds up to three minutes to process a file.

FortiSandbox for MSSPs

An MSSP can determine which logs sent to the sandbox belong to which customer site by leveraging external Security Information and Event Management (SIEM), such as HP Arcsight, AccelOps, LogRhythm, or QRadar to segment customer logs. More often than not, when the MSSP is loading a new customer into the sandbox, it can also load the customer information into their external SIEM via the FortiGate serial number to enable customer and log separation.

For adding a device to the sandbox, it is best to standardize device naming and authorization conventions. The standard naming convention should include information such as Customer Name, Site Identifier, Equipment and Model, SLA, and any comments about the device. The MSSP may even be

able to integrate these feeds into other systems to automate billing, etc. Otherwise there will be additional data integration needed in order to accomplish these tasks.

There are a few different methods for MSSPs to consider in terms of sizing and pricing FortiSandbox solutions for customers. Different strategies will appeal to different companies depending on margin requirements, capital considerations, and back office capabilities.

The primary methods of deployment for sandboxing managed security services are resale and OPEX models. In the resale model, the MSSP sells the hardware, support, and subscriptions to the customer and manages it for them. In the OPEX, or sandbox-as-a-service model, the customer consumes and pays for the service on a monthly basis.

Selling FortiSandbox to a customer, installing it on-site, and managing it is the simplest method of deployment and offers benefits such as short-term ROI and solution match. But as the desire for cloud-based delivery and consumption models solutions continues to grow, MSSPs that can deliver sandbox-as-a service gain a competitive edge in an increasingly competitive market.

Large enterprises are increasingly adopting cloud-based security services like SIEM and sandboxing to complement their security profile. With sandbox-as-a-service, the MSSP owns the technology and delivers it to the customer for a monthly subscription fee. While this solution extends the return on investment timeframe, it increases overall margins and complements a managed firewall and email security offering. Leveraging virtual machines allows MSSPs to make the solution affordable even for SMBs and mid-enterprise customers.

MSSPs must design a solution that's easy for salespeople to communicate and for customers to understand. Reducing complexity simplifies the qualification process and improves sales efficiencies. Sizing solutions can be done for customer segments or verticals, but should come in options that apply to the breadth of the provider's customer base.

Targeting a cost-per-location allows MSSPs to appropriately account for compute resources, management infrastructure investment, and operational overhead. For example, a customer with over 50 locations may trigger economies of scale that allows the MSSP to reduce the cost-per-location for larger customers.

Simplified Service Models

Beyond standardized per-location sizing, offering a basic menu of service options (e.g., simplified, basic, and advanced) allows providers to reach both small business and enterprise segments without having overly complex choices.

Sandbox On-demand: Service includes a scalable platform for customers to manually upload suspicious files for inspection that could include a report on the file or provide that report for an additional fee.

- SMB Option – 10 files/day per Firewall
- Mid-Enterprise – 50 files/day per Firewall
- Enterprise – 100 files/day per Firewall

Sandbox-as-a-Service (Files sent to the Sandbox): Service includes notification of malicious file email sent to customer administrator and MSSP help desk.

- SMB Option – 300 files/day per Firewall
- Mid-Enterprise – 600 files/day per Firewall
- Enterprise – 1500 files/day per Firewall
- Summary Reporting

Sandbox-as-a-Service Premium: Service includes notification email and multiple incident response support requests. Incidence response would include initial mitigation along with investigative and remediation activities conducted by the MSSP.

If providers don't have the in-house expertise for incident response specifically around malware analysis and custom signatures, they can leverage FortiGuard's Premier Incident Response service, which allows access to 200+ security analysts to respond to customer incidents with SLAs in place.

Sizing and Scaling

The sizing of a sandbox infrastructure depends upon the volume of files per location that will not only be processed by the FortiGate, but also sent up to the FortiSandbox. A good rule of thumb is that the average branch office with 50 people or fewer (a typical 90D Deployment) will process approximately 24 suspicious files per hour. Since around 60% of these files will be classified and dealt with by the CPRL/AV duo, that leaves approximately 10 files per hour that the system would need to send to the sandbox. If a customer has 10 locations, then they would be sending 100 files per hour.

Using VMs would allow the MSSP to scale up to address demand. In the case of larger environments (a deployment with approximately 500 sites), it might make more sense to dedicate a sandbox appliance to that particular customer. In either case, the economics of offering sandbox-as-a-service still prove effective.

From a VM-sizing perspective, one can construct and scale a service infrastructure to mimic hardware specifications. Base licenses (FSA-VM-Base) and virtual machine licenses (FSA-VM-10) are purchased to support customer files. Each VM can scan one file every three to five minutes; files are processed first-in, first-out in the order they're received. An FSA-VM-Base license combined with 10 VMs (FSA-VM-10) is equivalent to one FSA1000D hardware appliance. An FSA-VM-Base license combined with 25 VMs (FSA-VM-10) is equivalent to one FSA3000D hardware appliance.

Nonrecurring set-up charges can be assessed per firewall to cover operational expenses. Some customers will submit fewer files, while others will submit more; the MSSP can extrapolate a monthly recurring charge per customer that ensures a profitable product. What's more, this service leads into far more profitable professional services engagements that occur as a result of malicious files being detected.

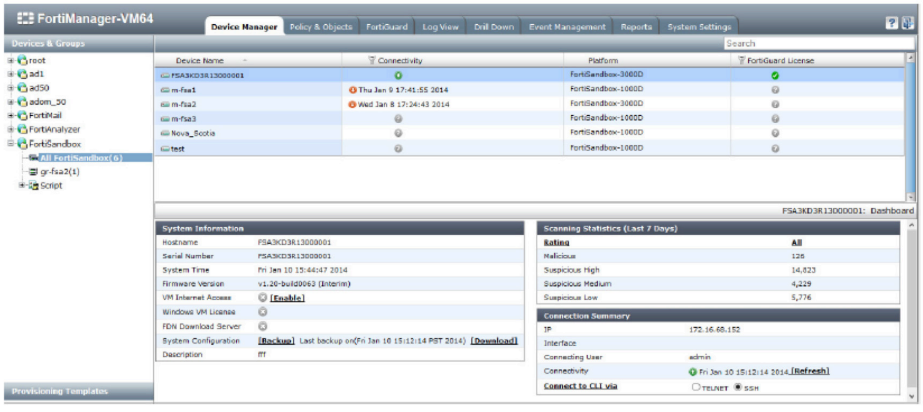
Once the sandbox VM is set up in the MSSP's data center, naming conventions, billing codes and internal methods and procedures have been written, the MSSP offering would now look something like this:

- FortiGate for Network Traffic Analysis – Currently a piece of the MSSP offer
- Blocks known threats using IPS, Application Control, web filtering, botnet detection and more – Currently a piece of the MSSP offer
- Flags suspicious (or high-risk) objects for more inspection – New feature/additional MRC
- Receives updated threat intelligence for inline prevention – New feature/additional MRC
- FortiSandbox for Payload Analysis – New feature/additional MRC
- Runs objects in a contained environment, analyzing activity – New feature/additional MRC
- Provides a malicious or low, medium, or high risk rating – New feature/additional MRC
- Uncovers threat lifecycle information and allows information sharing with FortiGuard experts for protection updates – New feature/additional MRC
- Provides summary reporting
- Offers incidence response
- New features offer opportunities for additional revenue as well as increased customer "stickiness" for MSSPs, as they provide greater value by increasing protection of the company's critical network and infrastructure

Centralized Management

For managing multiple sandboxes simultaneously, FortiManager centralized management offers considerable deployment and operational efficiencies. FortiSandbox v1.2 can be centrally managed by a FortiManager running v5.0.6 or later. The provider simply needs to configure central management on the FortiSandbox, and then add the device to FortiManager to take advantage of this capability.

Providers can add a FortiSandbox to FortiManager using the add device wizard. Simply select to discover the device or select to add model device. FortiSandbox devices added to FortiManager are located in a default FortiSandbox ADOM. ADOMs must be enabled in order to add FortiSandbox devices.



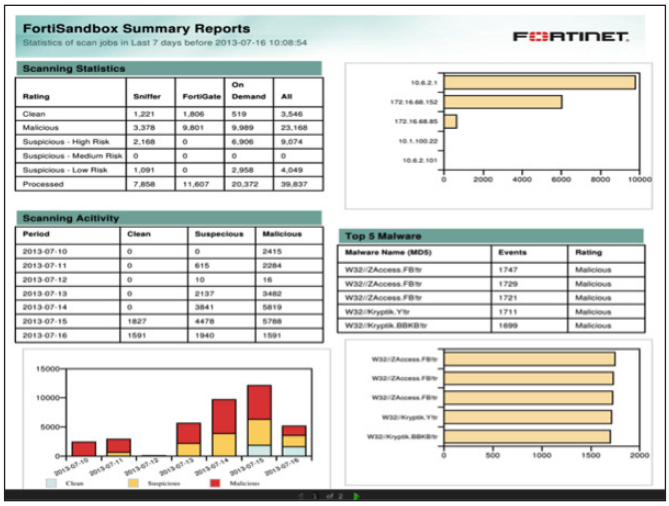
The top portion of the content pane shows the device list. When you select one of the devices in the table, the bottom portion of the content pane displays the selected device dashboard. The menu navigation of the device settings is in a menu format and referred to as the dashboard toolbar.

FortiManager

Summary Reporting

The FortiSandbox summary report contains statistics of scan jobs for the previous seven days. The global summary report provides information for all files received by FortiSandbox, including device(s), sniffer, and on-demand. The summary report contains the following sections:

- Scanning Statistics (table and bar graph)
- Scanning Activity (table and bar graph)
- Top Malware Files (table)
- Top Targeted Hosts
- Top Infections URLs
- Top Callback Domains



Summary Report

Detailed Reporting

The FortiSandbox detail report contains a list of all malicious and suspicious events for the previous seven days. The global detailed report provides information for files received by FortiSandbox including device(s), sniffer, and on-demand. When VDOMs are enabled on FortiGate, detailed report data is broken down by VDOM. The detailed report contains the following sections:

- Report Summary
- The total number of events for the past seven days
- Device Events Summary

This report lists event summary information including: rating, malware name, source, detection time, destination, and download path.

Sandbox-as-a-Service – Going Forward

Advances in multi-tenancy, VM deployment, and automated orchestration will continue to drive down the cost of delivering sandbox-as-a-service for the MSSP, but the value of the combination of this service with perimeter and cloud firewalls will continue to be sought after as threats continue to adapt. By leveraging economies of scale, MSSPs can make sandboxing an affordable service for all customer segments.

Offering a sandbox-as-a-service will increase revenue and profit margins for providers while delivering timely protection against the latest, most aggressive forms of cyberattacks. When combined with other security enforcement tools, it creates a unique offering that differentiates the provider from its competition. Sandbox-as-a-service improves the quality and effectiveness of services and positions the MSSP to benefit from the market shift towards cloud-based security.

For more details about sandbox-as-a-service or any other Fortinet product, contact the MSSP team at **MSSP@Fortinet.com** or your local Fortinet Sales Engineer.

1. Erin Palmer, "Report: Targeted Cyber-Attacks Increased by 91% in 2013," Business Administration Information, April 25, 2014, http://www.businessadministrationinformation.com/news/report-targeted-cyber-attacks-increased-by-91-in-2013
2. Verizon Enterprise Solutions, "2014 Data Breach Investigations Report," p. 38, http://www.verizonenterprise.com/DBIR/2014/
3. Peter Maass and Megha Rajagopalan, "Does Cybercrime Really Cost $1 Trillion?," Pro Publica, August 1, 2012, http://www.propublica.org/article/does-cybercrime-really-cost-1-trillion

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
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