HOW TO CHOOSE YOUR NEXT SANDBOXING SOLUTION

FEATURING INSIGHT FROM GARTNER'S MARKET GUIDE FOR NETWORK SANDBOXING

With several sandboxing solutions available in the market today, how do you go about choosing the one that's right for your organization? On March 2, 2015, Gartner published the "*Market Guide for Network Sandboxing"* geared at providing guidance to organizations looking to prevent the most sophisticated unknown malware from compromising their systems and networks.

In this paper, we will present the key points of the Gartner research, and then discuss how we feel Check Point solutions are meeting those requirements today.

In Gartner Predicts 2015: Infrastructure Protection, Gartner states that "By 2018, 85% of new deals for network sandboxing functionality will be packaged with network firewall and content security platforms"[1]

We believe the reason behind this statement is clear—there is an inherent desire to minimize the number of separate security products an organization must deploy, consolidate the security alerts into fewer and more consistent screens, and integrate and correlate the alerts into one meaningful dashboard. Because of this, network firewall gateways with their out-of-the-box visibility to network traffic are the ideal platform to offer the best sandboxing security services to organizations.

Checkpoint has been recognized in the top right quadrant of the Gartner Magic Quadrant for Enterprise Network Firewalls for the past 18 years[2] and continues to be a leader in the threat prevention market by offering the best sandboxing technology available that follows Gartner's guidelines.

MARKET SEGMENTATION

According to Gartner, the market for network sandboxing consists of 3 categories[3]. And in this section we will discuss how the Check Point sandbox solution, Threat Emulation, can support deployment models across all three of Gartner's categories for network sandboxing. The first two categories Gartner describes are:

1. **Sandboxing as a feature of firewalls, IPS and UTM solutions and**
2. **Sandboxing as a feature of secure web gateways or secure email gateways**

Check Point's sandbox solution, Threat Emulation, is integrated with Check Point gateways running **Firewall/IPS/UTM**, as well as the **Check Point Secure Web Gateways**:

Using dedicated Threat Emulation appliances (aka Private Cloud) or the Threat Emulation cloud service, Check Point Security Gateways sends files and objects from across the network to the Threat Emulation sandbox. This option allows customers to add sandboxing capability for protection from advanced and zero-day threats to their existing network security and management infrastructure. For customers using our Cloud sandboxing option, no additional hardware is required beyond the existing firewall gateways, making deployment very easy, quick, and cost effective.

Both our cloud-based and on premise Threat Emulation sandbox options include full threat prevention capabilities deployable inline, on a SPAN port, and as an email relay (MTA). Threat Emulation supports scanning web, email, and file-share traffic, and a single dedicated appliance on premise can manage both email and web traffic.

Coupled with our market-leading management, Check Point Threat Emulation offers built-in SSL inspection and identity awareness. In addition to the sandbox function, Threat Emulation can be purchased with Anti-Bot for detection of infected hosts, as well as Antivirus and Check Point Threat Extraction for delivering clean files immediately.

3. A stand-alone sandboxing solution

Check Point Threat Emulation can be deployed as a **stand-alone** solution in three different modes:

- With only Threat Emulation blades activated, send files for cloud emulation
- With only Threat Emulation blades activated, send files for local emulation on dedicated appliances
- Hardware free implementation—We also offer configuration, set up, management, and sandboxing services fully hosted in the cloud. Customers only need to point their email and/or web traffic to our Capsule Cloud, and benefit immediately from the same protection available in the deployment scenarios described above.

With this range of deployment options, we believe Check Point Threat Emulation, spans all three of Gartner's categories for network sandboxing. This solution provides customers with the flexibility to either inspect files in the cloud or on premise using our Threat Emulation Appliances.

SANDBOXING BACKGROUND

According to Gartner, network-based sandboxing relies on 'sensors' that monitor network traffic and then submit suspicious objects to the 'sandbox' for payload analysis[4]. Suspicious files are flagged while minimizing false positives. Only in the last few years has sandboxing been deployable in the broader market utilizing current security skillsets and offering the capabilities described by Gartner, below. But this basic functionality still has limitations.

Offered by many vendors, traditional OS-level sandboxing is often slow, subject to many successful evasion techniques, incapable of blocking some sophisticated attacks, and can only be evaluated once the malware is already active. By being the first to introduce CPU-level sandboxing, Check Point delivers a solution beyond the traditional OS-level sandboxing. Faster, evasion-resistant CPU-level threat emulation addresses the 'pre-infection' stage by analyzing the malware's impact on the CPU and memory. With the combination of both OS-level and CPU-level sandboxing detection and blocking, we provide the highest level of zero-day protection, an unmatched level of security against even the most sophisticated attacks. In addition, our mobile solution extends this real-time protection to both iOS and Android users.

SANDBOXING CAPABILITIES TO LOOK FOR

The quality of sandboxing solutions varies widely. According to Gartner, some critical capabilities to look for in your next sandboxing solution include:

1. ***"The ability to analyze a broad range of suspicious objects[5]"***
   Check Point Threat Emulation identifies malware across a broad range of the most common document types used in organizations today, including:
   - Adobe Acrobat (PDF)
   - Adobe Flash (SWF)
   - Archive (TAR, ZIP, RAR and Seven-Z)
   - General (EXE, RTF, CSV and SCR)
   - Java (JAR)
   - Microsoft Office Package
     - Microsoft Excel (XLS, XLSX, XLT, XLM, XLTX, XLSM, XLTM, XLSB, XLA, XLAM, XLL and XLW)
     - Microsoft PowerPoint (PPT, PPTX, PPS, PPTM, POTX, POTM, PPAM, PPSX, PPSM, SLDX and SLDM)
     - Microsoft Word (DOC, DOCX, DOT, DOCM, DOTX, DOTM)
   - Word Processing (HWP)

2. ***"Static analysis and other pre-filtering techniques[6]"***
Check Point offers a multi-layered threat prevention strategy, using IPS, Antivirus, Anti-Bot, OS-level Threat Emulation, CPU-level Threat Emulation, Threat Extraction, and Threat Intelligence. Our IPS, Antivirus, and Anti-Bot solutions help filter out known threats, while Threat Emulation and Threat Extraction provide protection against new and unknown threats.

   Check Point leverages multiple pre-emulation engines to minimize the number of objects sent to the sandbox. We utilize advanced machine learning engines for executable files and various signature-based Antivirus engines. Static analysis evaluates and identifies malware without requiring sandbox analysis. In addition, we reduce sandboxing sessions by caching files sent through multiple channels of attack on the gateways, on the Threat Emulation appliance and on the cloud service. As new threats are confirmed as malware, updates are provided to static filtering engines in real-time.

3. ***"Comprehensive operating system and application stack[7]"***
Check Point Threat Emulation provides multiple simultaneous simulation environments for sandboxing: Windows XP, 7, Microsoft Office, Adobe environments, and custom images. In addition to this, our upcoming capability of CPU-level Threat Emulation is OS agnostic and can detect threats based on instruction level behavior on any x86 Operating System.

   Preventing advanced threats on mobile platforms requires a holistic approach that is focused on the unique aspects of these platforms. Covering both iOS and Android, we offer the industry's most advanced Mobile Threat Prevention solution. With the highest advanced threat catch-rate for enterprise-grade mobile security platforms, we secure the entire mobile device.

4. ***"Anti-evasion technologies[8]"***
Traditional OS-level sandbox technology is based upon behavioral analysis within the operating system. Due to this, traditional sandboxing faces a major challenge when it comes to constantly improving evasion techniques. Our CPU-Level sandboxing detects vulnerability exploitations before the attacker has an opportunity to execute any code or evade detection. This extends Check Point Threat Emulation solution beyond even the customized hypervisors supported at the OS-level to provide the most advanced zero-day solution available.

5. ***"The rate at which objects can be analyzed in the sandbox[9]"***
Check Point offers its Threat Emulation sandbox in two forms:
   a. **Threat Emulation Cloud Service:** This cloud service provides a scalable solution without requiring the customer to deploy additional infrastructure. Built to withstand high peak usage, it provides a highly available global service.
   b. **Threat Emulation (TE) appliance:** We provide a wide range of Threat Emulation appliances for on premise sandboxing. Rated by the monthly number of sandboxing sessions, they range from 250K to 2 million sandbox sessions per month. The appliances' design withstands typical peak traffic. If the emulation capacity is exceeded it queues files and objects. With our gateways, customers can send files and objects across their network to the TE appliance for sandboxing. By creating an array of TE appliances load-balanced by our gateways, this solution easily scales to any volume without the need for a third-party load-balancer.

6. ***"A combination of virtualization-based and emulation-based sandboxing analysis[10]"***
We focus our sandbox approach on the providing the best methods of threat detection while preserving both performance and efficiency. With virtualization-based approaches, we provide exceptional performance compared to solely emulation-based approaches. With the combination of our CPU-Level technology and the actions we perform within virtualization, we provide the best of both of the approaches.

7. ***"Contextual information about the malware or targeted attack[11]"***
Our Threat Emulation solution works hand in hand with ThreatCloud™, our threat intelligence database. ThreatCloud™ leverages threat feeds from all of our customers and many threat intelligence partners. Every time Threat Emulation marks a file as malicious, it adds this information to the ThreatCloud™ database. In addition, through Check Point's management and

SmartEvent, customers gain complete visibility into their network. Customized reports of events pointing at the sources, destinations, services, and type of attacks help determine whether attacks are targeted or not.

8. ***"Integration with forensics tools[12]"***

Our Endpoint Forensics solution provides detailed insight for detections found on the network and the endpoint. Coupled with complete forensic information, it provides a complete analysis highlighting how the attack entered the organization, damage occurred, command and control communications, lateral movement, and more. This information allows it to automatically identify all hosts with the same infection. Additionally, we offer a tie-in between Threat Emulation and Bit 9's Carbon Black, enabling 2-way transfer of zero-day malware information at the endpoint.

SUMMARY

Gartner recommends that "if your organization is budget-constrained or looking for a quick path to add sandboxing, first evaluate adding sandboxing as a feature from one of your current security vendors.[13]" And "If budget permits, or when targeted malware is identified as a high risk, evaluate stand-alone sandboxing solutions.[14]" At Check Point, we offer both.

For customers looking for the best stand-alone solution we provide three alternate implementations based on a dedicated and comprehensive solution. These solutions range from a zero-hardware approach to an on-premise Threat Emulation appliance. Bundled with a full stack of threat prevention technologies, they also include our unique CPU-Level sandboxing and innovative Threat Extraction capabilities. The solutions integrate with Check Point's leading intelligence—ThreatCloud™, and the only open marketplace for cyber-intelligence—IntelliStore™. Our solution covers the Incident Response process, including SmartEvent—our visualization and investigation platform, Endpoint Forensics, and the ability to detect and block infected hosts with Anti-Bot.

For the budget-conscious customers, we provide a state-of-the-art advanced threat protection solution that seamlessly integrates with existing security, secure web gateways, and management to send files and objects either to the Threat Emulation cloud service or to an on-premise Threat Emulation appliance.

Check Point Threat Emulation meets all the criteria provided by Gartner for an effective sandboxing solution. We provide the only sandboxing solution that combines the power of CPU-level and OS-level protection to detect and block malware, and to prevent infections from undiscovered exploits, zero-day, and targeted attacks.

Check Point's Threat Emulation is only one part of our comprehensive end-to-end portfolio spanning next-generation threat protection, mobile security, next-generation firewalls, security management, and much more.

Evaluate Threat Emulation today—http://www.checkpoint.com/try-our-products/

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

[4] "Market Guide for Network Sandboxing," page 1, Gartner, 2 March 2015
[5] "Market Guide for Network Sandboxing," page 4, Gartner, 2 March 2015
[6] "Market Guide for Network Sandboxing," page 4, Gartner, 2 March 2015
[7] "Market Guide for Network Sandboxing," page 4, Gartner, 2 March 2015
[8] "Market Guide for Network Sandboxing," page 4, Gartner, 2 March 2015
[9] "Market Guide for Network Sandboxing," page 4, Gartner, 2 March 2015
[10] "Market Guide for Network Sandboxing," page 4, Gartner, 2 March 2015
[11] "Market Guide for Network Sandboxing," page 4, Gartner, 2 March 2015
[12] "Market Guide for Network Sandboxing," page 4, Gartner, 2 March 2015
[13] "Market Guide for Network Sandboxing," page 5, Gartner, 2 March 2015
[14] "Market Guide for Network Sandboxing," page 5, Gartner, 2 March 2015