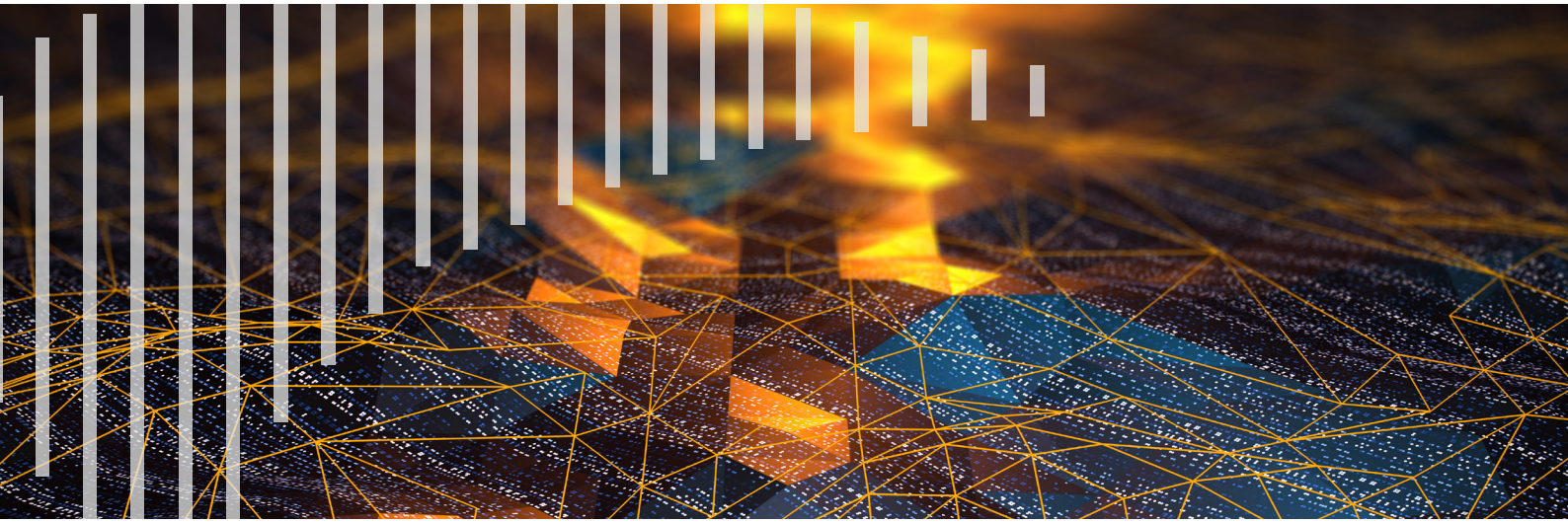
SONICWALL



SOLUTION BRIEF

An Advanced Approach to On-Prem Sandboxing

Balancing accuracy, cost and compliance while retaining sensitive data in-house

Abstract

Large organizations and agencies need to counter advanced malware with advanced security techniques, such as sandboxes. However, many also require their sensitive data stays on premises, so cannot leverage cloud-based offerings. This brief examines an advanced on-prem sandboxing approach that is fast, highly accurate and cost-effective.

Why You Must Have Sandboxing

Traditional network security technology detects known threats via definitions and signatures but can't detect new and refreshed advanced threats like custom malware and zero-day exploits. To allow malicious behavior to remain hidden, modern malware writers implement advanced techniques, including custom encryption, obfuscation and packing, as well as acting benign within sandbox environments. These techniques often hide the most sophisticated weaponry, which is only exposed when run dynamically. In most cases, these are impossible to analyze in real-time using static detection techniques.

To better detect unknown threats, security professionals deploy advanced threat detection technologies, such as sandboxes, that analyze the behavior of suspicious files and uncover hidden malware. Network sandbox engines execute files, log the resulting activity, and then, after execution, look for and attempt to correlate malicious behavior.

With many attack types only revealing their weaponry within memory, a memory-based approach is required to detect and stop attacks before they reach endpoints.

Challenges with Sandboxing

Cloud-based sandboxing creates the lowest barrier to entry when it comes to detecting new and updated attack variants. Even if security efficacy is perfect, there are two challenges with this model. First, this model relies on points of presence (PoPs) where security appliances/services and threat hunters can send files for analysis. Latency is introduced into the equation when the Internet speeds are slow or the distance between the service and the sender becomes great. Secondly, many regulation-intense organizations and government agencies that deal with sensitive data are not allowed to let data to leave their organization (or, in some cases, country or region) and therefore cannot send suspicious files to cloud-based sandboxes for analysis.

To counter these objections, these organizations and agencies will leverage an on-premise network sandbox within the confines of their datacenter. Unfortunately, this sandboxing model tends to be very expensive and just like most cloud-based sandboxes, their evasion tactics are well documented[1]. Additionally, in both models the correlation and scoring of sandbox activities and behaviors can be prone to false positives.

A Balanced Approach

What organizations need to remain compliant with regulations and privacy standards is a budget-friendly on-prem threat analysis platform that malicious code can't detect and evade that renders a quick verdict.

A balanced solution should inspect suspicious files within the data center, using fast and accurate memory-based analysis to provide a strong layer of defense against advanced and targeted threats. At the same time, it should be easy to administer and lower total cost of ownership in order to meet budgetary requirements.

Solution: SonicWall Capture Security *appliance*

SonicWall Capture Security appliance (CS*a*) is an on-premises file analysis and malware detection solution featuring our patent-pending Real-Time Deep Memory Inspection (RTDMI™) technology. RTDMI adds protection against malware that eludes other detection methods while delivering far more than half of all verdicts in under five seconds.

As a result, CS*a* catches more malware and faster than network sandboxing methods. CS*a* also offers a lower false positive rate to improve security and the end user experience. It analyzes malware hidden in a broad range of file types, file sizes and operating environments to best provide comprehensive zero-day threat detection.

Furthermore, CS*a* can detect and stop potential side-channel attacks through real-time memory-based inspection techniques. By forcing malware to reveal its weaponry into memory, CS*a* proactively blocks mass-market, zero-day threats and unknown malware.

How it Works

CS*a* detects and blocks malware that does not even exhibit any malicious behavior or that hides its weaponry via encryption. To discover packed malware code that has been compressed to avoid detection, the RTDMI engine allows the malware to reveal itself by unpacking its compressed code in memory. It sees what code sequences are found within and compares it to what it has already seen along with several other dynamic inspection techniques. Identifying malicious code in memory is more precise than trying to differentiate between malicious system behavior and clean program system behavior, which is an approach used by most other analysis techniques.

Besides being highly accurate, CS*a* also improves sample analysis time. Since it can detect malicious code or data in memory in real-time during execution, no malicious system behavior is necessary for detection. The presence of malicious code can be identified prior to any malicious behavior taking place, thereby rendering a quicker verdict.

And unlike typical behavior-based systems that only reach down to the level of APIs and system calls, RTDMI's granular CPU-level instruction detection can stop new forms of malware that attempt to exploit Meltdown, Spectre, or other side-channel vulnerabilities.

Broad file type analysis

CS*a* with RTDMI is also proficient in stopping new forms of document-based malware, including malicious code embedded within PDFs and MS Office files at rates higher in side-by-side tests with third-party network sandboxing technologies. These capabilities alone provide a better defense against phishing emails containing these files, which can introduce significant latency in some sandboxing models.

The appliance analyzes documents dynamically via proprietary exploit detection technology along with static forms of inspection with the ability to detect many malicious document categories, including:

- Malicious Flash-based MS Office documents
- Dynamic Data Exchange (DDE) based exploits and malware inside Office files
- MS Office and PDF files containing malicious executables
- PDF documents containing MS Office malware
- Malevolent shellcode-based files
- Macro-based malicious files
- Malicious multi-layer files
- PDF documents with "JavaScript infectors"
- JavaScript-based exploits in PDF documents
- Files leading to phishing and malware hosting websites
- "Phishing style" malicious PDF documents leading to both phishing and malware hosting websites

CS*a* supports analysis for a broad range of file types, including executable programs (PE), DLL, PDFs, MS Office documents, archives, JAR, and APK plus multiple operating systems including Windows, Android, and multi-browser environments. Administrators can customize protection by selecting or excluding files to be sent to the cloud for analysis, including by file type, file size, sender, recipient and protocol. In addition, administrators can manually submit files to the appliance for analysis.

Easy Administration and Reporting

Easy-to-understand reports clearly show why something was blocked, detailing the analysis results for files sent to the service including session information, OS information, OS activity, network activity and a copy of the original file (based on privacy settings). Log alerts provide notification of suspicious files sent to the CS*a*, as well as file analysis and verdict results.

Deployment Options

CS*a* can be deployed in your main datacenter and can be referenced by IP address or FQDN which makes it an excellent resource for your SonicWall HQ firewalls, email security appliances, and even branch firewalls as well. Furthermore, with the REST API, administrators and threat hunters can manually upload files to CS*a* for quick results.

Conclusion

To combat evasive and targeted malware, sandbox analysis is required to discover and stop unknown threats. With many attack types only revealing their weaponry within memory, a memory-based approach is required to detect and stop attacks before they reach endpoints. Furthermore, cloud-based sandboxing engines can introduce latency and are not compliant with many organizations' data sovereignty requirements.

Capture Security appliance enables you to inspect suspicious files within your data center. Using fast and accurate memory-based analysis provides a strong layer of defense against advanced and targeted threats.

Learn more. Contact your SonicWall representative or visit www.sonicwall.com.

About SonicWall

SonicWall delivers Boundless Cybersecurity for the hyper-distributed era and a work reality where everyone is remote, mobile and unsecure. By knowing the unknown, providing real-time visibility and enabling breakthrough economics, SonicWall closes the cybersecurity business gap for enterprises, governments and SMBs worldwide. For more information, visit www.sonicwall.com.

[1] Mitre.org; Virtualization/Sandbox Evasion, https://attack.mitre.org/techniques/T1497/ 26 September 2019

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Refer to our website for additional information.
www.sonicwall.com

© 2020 SonicWall Inc. ALL RIGHTS RESERVED.

SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners. The information in this document is provided in connection with SonicWall Inc. and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of SonicWall products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON- INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. SonicWall Inc. and/or its affiliates do not make any commitment to update the information contained in this document.

SolutionBrief-AnAdvancedApproach-US-VG-1641