

Loose Chips Sink Ships

Stop Side-Channel Attacks with SonicWall's Real-Time Deep Memory Inspection



Real-Time Deep Memory Inspection™ (RTDMI) is a patented technology that examines suspicious files in memory to render a fast and accurate verdict.

Threat Bulletin: Side-channel attacks

Takeaway: Side-channel attacks exploit unavoidable information produced as a by-product of the computing process

As computers compute, they create breadcrumbs that provide information about their activities. These can take the form of power usage fluctuations, hard drive electrical emissions, keyboard sound patterns, or many other things. And as infrastructures have grown more complex, the body of unintentional information they generate has increased astronomically.

Hackers can use this information to fool a processor into giving up a lot of secrets. For instance, a vulnerability called Meltdown exploits a pattern of memory access to read all memory without authorization. These types of attacks are called side-channel attacks.

Side-channel attacks can be devastating. They are hard to detect because they usually don't leave any trace or alter a targeted system. They are hard to stop because the weaknesses that allow side-channel attacks are inherent to

the hardware platforms they target. Patches exist to work around the hardware vulnerabilities but applying them can require updates to BIOS/firmware and software, which is hard to do across large user bases.

SONICWALL CAPTURE ATP WITH RTDMI IDENTIFIES AND STOPS MORE THAN 1,600 NEW MALWARE VARIANTS EVERY BUSINESS DAY

How SonicWall RTDMI Catches What Others Can't

Takeaway: RTDMI mitigates millions of new forms of malware that attempt to slip by traditional network defenses via evasion tactics.

SonicWall RTDMI™ uses proprietary memory inspection, CPU instruction tracking and machine learning capabilities to become increasingly better at recognizing and mitigating cyberattacks never seen by anyone in the cybersecurity industry — including threats that do not exhibit any malicious behavior and hide their weaponry via encryption.

These attacks are missed by traditional sandboxes because they are designed to look for malicious behavior. RTDMI doesn't give the code a chance to behave suspiciously: it detects it in the memory in real-time, before it can execute its next attack phase. In many cases, the entire process takes less than 100 nanoseconds.

RTDMI accomplishes this by allowing the compressed malicious code to unpack itself in a secure environment, where it can then "see" every CPU instruction within the code before it can execute. At that point, the code can be stopped.

- Detects Meltdown, Spectre, Foreshadow, TMP-Fail and more
- Exposes threats in MS Office files and PDFs
- Blocks malware on unexpected ports

589,313

Number of new malware variants identified by SonicWall in 2020. Of those,

268,362

were detected by SonicWall Real-Time Deep Memory Inspection.

'PERFECT' THREAT DEFENSE

Capture ATP + RTDMI™

SonicWall Capture ATP with patented Real-Time Deep Memory Inspection™ faced 35 days of rigorous testing by ICSA Labs during the first quarter of 2021. The result? **A 'perfect' score.**

Threats Detected	580
Threats Missed	0
False Positives	0

Capture ATP detected 580 of 580 new and unknown malicious samples — and with no false positives.

THE TESTS

- 35 Days of Testing
- 1,471 Total Tests
- 580 New & Little-Known Samples
- 891 Innocuous Applications

THE RESULTS

- 100% Detection of Previously Unknown Threats
- Zero False Positives
- Fifth Consecutive ICSA Labs Certification

SonicWall Capture ATP + RTDMI Stops Threats before They Execute

Takeaway: RTDMI was built to help SonicWall researchers analyze more than 100,000 threats a day. It proved so accurate and effective that we added it to the SonicWall Cloud Capture platform.

Modern malware writers implement advanced techniques, including custom encryption, obfuscation and packing, and the code they produce can appear to be benign within sandbox environments. These techniques allow malicious behavior to remain hidden, and an attack is only exposed when run dynamically. Static detection techniques usually

can't analyze this type of malware in real-time, so the threat can't be stopped until it has reached a more advanced stage of its attack. RTDMI prevents these sophisticated attacks no matter whether the targeted system is in the public cloud, private cloud, or on-premise.

SonicWall Capture Labs threat research team process more than 100,000 samples a day. RTDMI was originally built to help them use machine learning to discover and identify new malware. The results were so accurate that the original tool was incorporated into Capture ATP at no additional cost to customers, and is now part of many SonicWall offerings, from firewall to email to wireless access points.

SonicWall Earns Another Perfect Score from ICSA Labs for Q2

[Download the full ICSA Labs report.](#)

THE "PERFECT" THREAT DEFENSE

ISCA Labs conducted Advanced Threat Defense testing that compared SonicWall Capture ATP + RTDMI against all other leading sandbox providers, subjecting the solutions to 1,471 tests that included 580 new or novel samples and 891 innocuous applications.

Capture ATP + RTDMI detected 100% of previously unknown threats and produced 0 false positives. That's a perfect score.

Learn how SonicWall Capture ATP service with RTDMI can deliver unparalleled real-time threat detection and protection:

sonicwall.com/capture-advanced-threat-protection

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 or follow us on [Twitter](#), [LinkedIn](#), [Facebook](#) and [Instagram](#).



SonicWall, Inc.

1033 McCarthy Boulevard | Milpitas, CA 95035

Refer to our website for additional information.

www.sonicwall.com

SONICWALL®

© 2021 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-RTDMI-COG-4955