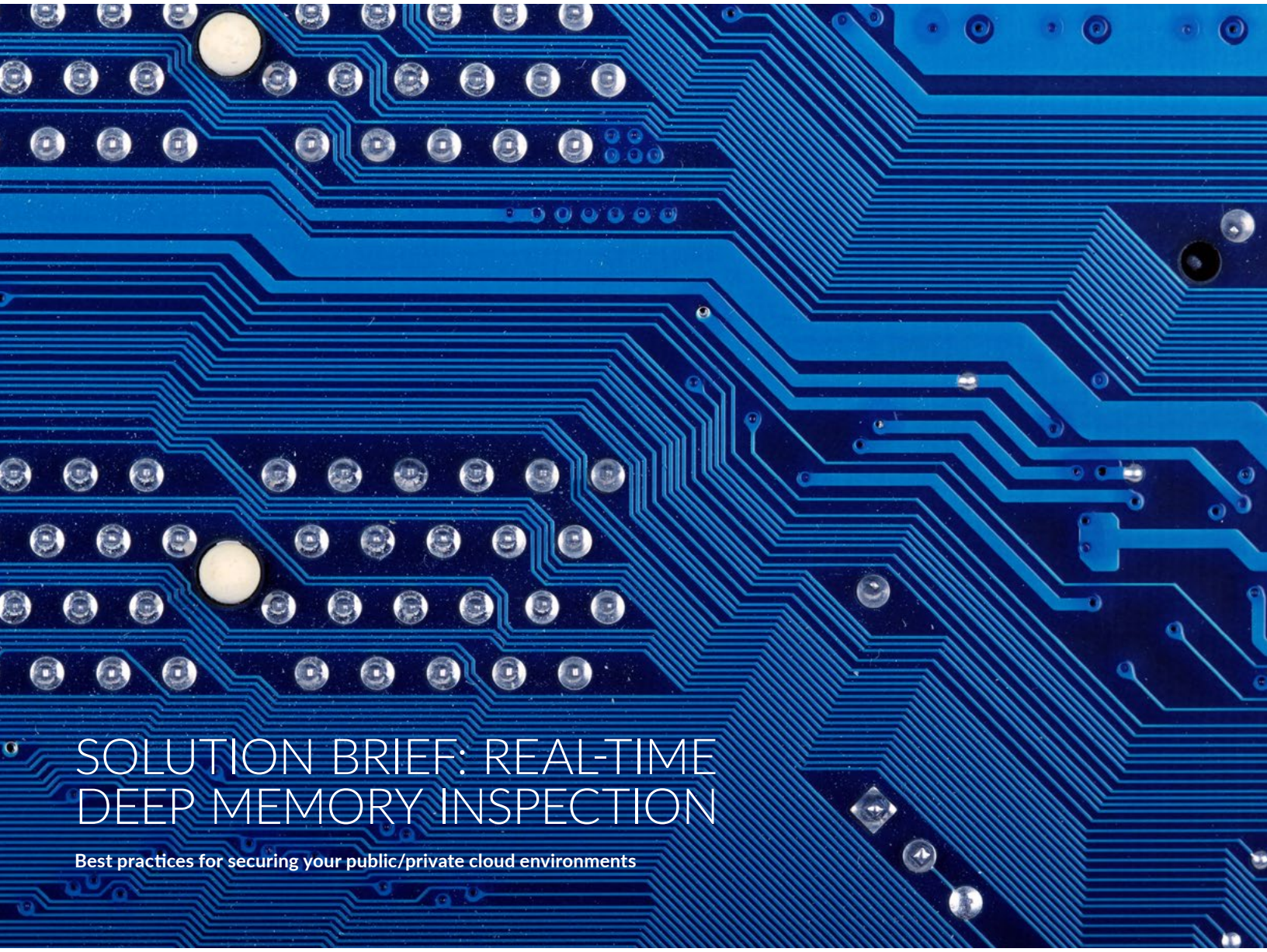

SOLUTION BRIEF: REAL-TIME DEEP MEMORY INSPECTION

Best practices for securing your public/private cloud environments

Abstract

SonicWall Real-Time Deep Memory Inspection (RTDMI™) technology enables SonicWall Capture Advanced Threat Protection (ATP) to catch more malware faster than behavior-based sandboxing methods, with a lower false positive rate.

Exposing threats hidden in memory

Network sandbox engines execute files, log the resulting activity, and then, after execution, look for and attempt to correlate malicious behavior. The correlation and scoring of these activities and behaviors are prone to both false positives and negatives. They are also prone to cause delays, unsatisfactory end user experience and subsequent IT ticket requests.

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.

When SonicWall released Capture ATP, it was the industry's first multi-engine sandbox that could block files at the gateway until a verdict. The multi-engine design answered the need to detect and stop evasive malware. Capture ATP was designed to process unknown files in isolated parallel environments to see what suspicious code intends to do, from the application, to the OS and down to the software that resides on the hardware.

Recently, SonicWall announced a new engine for Capture ATP called Real-Time Deep Memory Inspection (RTDMI) to improve the technology's security effectiveness. Invented and developed by SonicWall's Capture Labs threat researchers, patent-pending RTDMI engine already had been running in the background of Capture ATP service for months beforehand, dynamically self-learning and self-enhancing.

How RTDMI works

SonicWall RTDMI technology detects and blocks malware that does not 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 in a secure sandbox environment. It sees what code sequences are found within and compares it to what it has already seen. Identifying malicious code in memory is more precise than trying to differentiate between malware system behavior and clean program system behavior, which is an approach used by some other analysis techniques.

Besides being highly accurate, RTDMI 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.

Ability to identify individual CPU level instructions

Upon detailed analysis, SonicWall Capture Labs researchers discovered that RTDMI engine had the ability to stop new forms of malware trying to exploit the Meltdown vulnerability. RTDMI engine's CPU level instruction detection granularity (unlike typical behavior based systems which have only API/system call level granularity) is what allowed RTDMI engine to detect malware variants which contained exploit code targeting Meltdown vulnerability.

Exposing threats in MS Office files and PDFs

With RTDMI running in the background, SonicWall Capture Labs researchers discovered that it had already discovered and stopped hundreds of new forms of document-based malware.. Upon further review, Capture Labs researchers found that it caught malicious code embedded in within PDFs and MS Office files at rates higher in side-by-side tests with third-party network sandboxing technologies.

In these tests, RTDMI found 35 times more malicious PDF documents and nearly two times more malicious MS Office files than the two other engines combined, giving customers a better defense against malicious code contained in these files.

When applied inside Capture ATP, RTDMI engine analyzes documents dynamically using proprietary exploit detection technology along with static forms of inspection. These combined techniques have the capability to detect many malicious document categories, including:

- Malicious Flash-based Office documents
- Dynamic Data Exchange (DDE) based exploits and malware inside Office files
- Malicious Office and PDF files containing executables
- Malicious PDF files containing Office malware
- Shellcode-based malicious Office and PDF files
- Macro-based malicious Office documents
- Malicious multi-layer PDF and Office documents
- Office and PDF-based malware utilizing dynamic proprietary exploit detection technology
- JavaScript-based exploits in PDF documents
- PDF documents containing "JavaScript infectors"
- "Phishing style" malicious PDF documents leading to both phishing and malware hosting websites

What this means

"This is a revolution in engineering, execution and innovation," says General Michael Hayden, Principal at the Chertoff Group, a global advisory firm focused on security and risk management. "To introduce this technology in the relatively early stages of these advanced attacks is a huge win for the security industry, as well as the public and private sectors."

By adding RTDMI engine to Capture ATP, SonicWall customers should see a significant improvement in detection rates when analyzing files on a larger scale. This technology is being added to Capture ATP with no increase in cost to the customer.

Conclusion

By forcing malware to reveal its weaponry into memory, the RTDMI engine proactively detects and blocks mass-market, zero-day threats and unknown malware with a very low false positive rate where weaponry is exposed for less than 100 nanoseconds.

Learn more about SonicWall Capture ATP.

About Us

SonicWall has been fighting the cyber-criminal industry for over 25 years, defending small, medium size businesses and enterprises worldwide. Our combination of products and partners has enabled a real-time cyber defense solution tuned to the specific needs of the more than 500,000 businesses in over 150 countries, so you can do more business with less fear.

If you have any questions regarding your potential use of this material, contact:

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, CA 95035

Refer to our website for additional information.
www.sonicwall.com