SonicWall Capture Advanced Threat Protection Service

Discover and stop zero-day and other unknown attacks

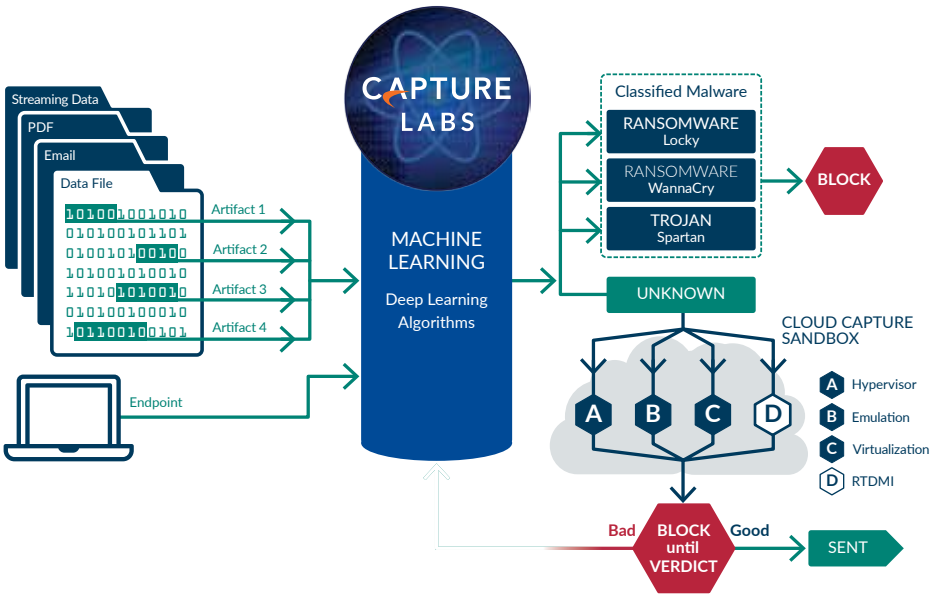
For effective zero-day threat protection, organizations need solutions that include malware-analysis technologies and can detect evasive advanced threats and malware — today and tomorrow.

To protect customers against the increasing dangers of zero-day threats, SonicWall Capture Advanced Threat Protection Service — a cloud-based service available with SonicWall firewalls — detects and and can block advanced threats at the gateway until verdict. This service is the only advanced-threat-detection offering that combines multi-layer sandboxing, including full system emulation and virtualization techniques, to analyze suspicious code behavior. This powerful combination detects more threats than single-engine sandbox solutions, which are compute-environment specific and susceptible to evasion.

The solution scans traffic and extracts suspicious code for analysis, but unlike other gateway solutions, analyzes a broad range of file sizes and types. Global-threat intelligence infrastructure rapidly deploys remediation signatures for newly identified threats to all SonicWall network security appliances, thus preventing further infiltration. Customers benefit from high-security effectiveness, fast response times and reduced total cost of ownership.

Benefits:

- High security effectiveness against unknown threats
- Near real-time signature deployment protects from follow on attacks
- Reduced total cost of ownership
- Block files at the gateway until verdict
- Multiple engines process files in parallel for rapid verdicts
- SonicWall's RTDMI engine blocks unknown mass-market malware utilizing real-time memory-based inspection techniques



A cloud-based, multi-engine solution for stopping unknown and zero-day attacks at the gateway

For best zero-day threat protection, the solution is architected to dynamically add new malware analysis technologies as the threat landscape evolves.

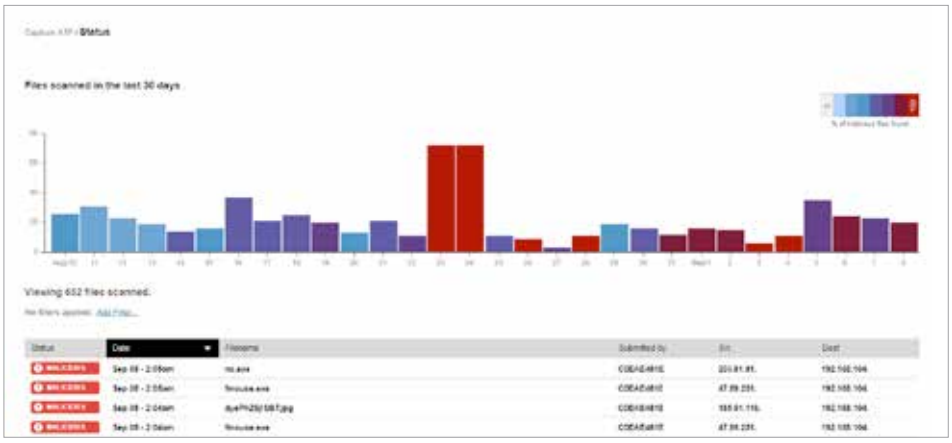
Features

Multi-engine advanced threat analysis — SonicWall Capture ATP Service extends firewall threat protection to detect and prevent zero-day attacks. The firewall inspects traffic, and detects and blocks intrusions and known malware. Suspicious files are sent to the SonicWall Capture ATP Cloud for analysis. The multi-engine sandbox platform, which includes RTDMI, virtualized sandboxing, full system emulation and hypervisor-level analysis technology, executes suspicious code and analyzes behavior, provides comprehensive visibility to malicious activity while resisting evasion tactics and maximizing zero-day threat detection.

Real-Time Deep Memory Inspection (RTDMI) — Enhancing SonicWall's multi-engine Capture ATP service is our patent-pending Real-Time Deep Memory Inspection technology. The RTDMI engine proactively detects and blocks mass market, zero-day threats and unknown malware by inspecting directly in memory. Because of the real-time architecture, SonicWall RTDMI technology is precise, minimizes false positives, and identifies and mitigates sophisticated attacks.

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

Blocks until verdict — To prevent potentially malicious files from entering the network, files sent to the cloud service for analysis can be held at the gateway until a verdict is determined.



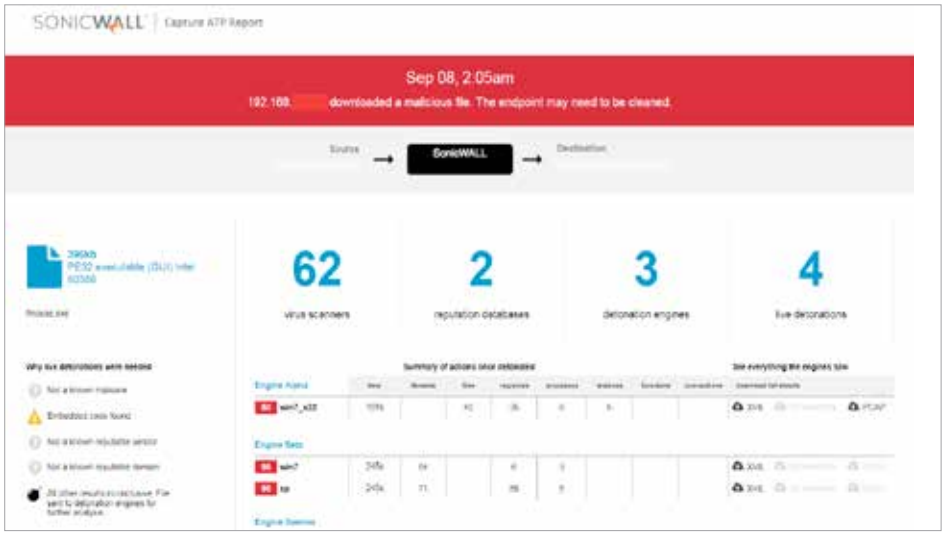
The SonicWall Capture ATP reporting page displays daily at a glance results. Colored bars on the report indicate days where malware was discovered. Administrators have the ability to click on individual daily results and apply filters to quickly see malicious files with results.

Rapid deployment of remediation signatures — When a file is identified as malicious, a signature is immediately available to firewalls with the SonicWall Capture ATP subscription to prevent follow-on attacks. In addition, the malware is submitted to the SonicWall Capture Labs threat research team for further analysis and inclusion with threat information into the Gateway Anti-Virus and IPS signature databases. Additionally, it is sent to URL, IP and domain reputation databases within 48 hours.

Reporting and alerts — The SonicWall Capture ATP Service provides an at-a-glance threat analysis dashboard and reports, which detail the analysis results for files sent to the service, including source, destination and a summary plus details of malware action once detonated. Firewall log alerts provide notification of suspicious files sent to the SonicWall Capture ATP Service, and file analysis verdict.

About Us

SonicWall has been fighting the cyber-criminal industry for over 26 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.



A detailed analysis report is also available for analyzed files to facilitate remediation.

SUPPORTED PLATFORMS

SonicWall Capture ATP Service is supported on the following SonicWall firewalls running SonicOS 6.2.6 and higher:

NS*sp* 12800
NS*sp* 12400

NS*a* 9650
NS*a* 9450
NS*a* 9250
NS*a* 6650
NS*a* 5650
NS*a* 4650
NS*a* 3650
NS*a* 2650

TZ600
TZ500 and TZ500 Wireless
TZ400 and TZ400 Wireless
TZ300 and TZ300 Wireless

NSv 1600
NSv 800
NSv 400
NSv 300
NSv 200
NSv 100
NSv 50
NSv 25
NSv 10

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

DataSheet-CaptureAdvancedThreatProtection-US-KJ-MKTG2923