SonicWall Capture Advanced Threat Protection Service

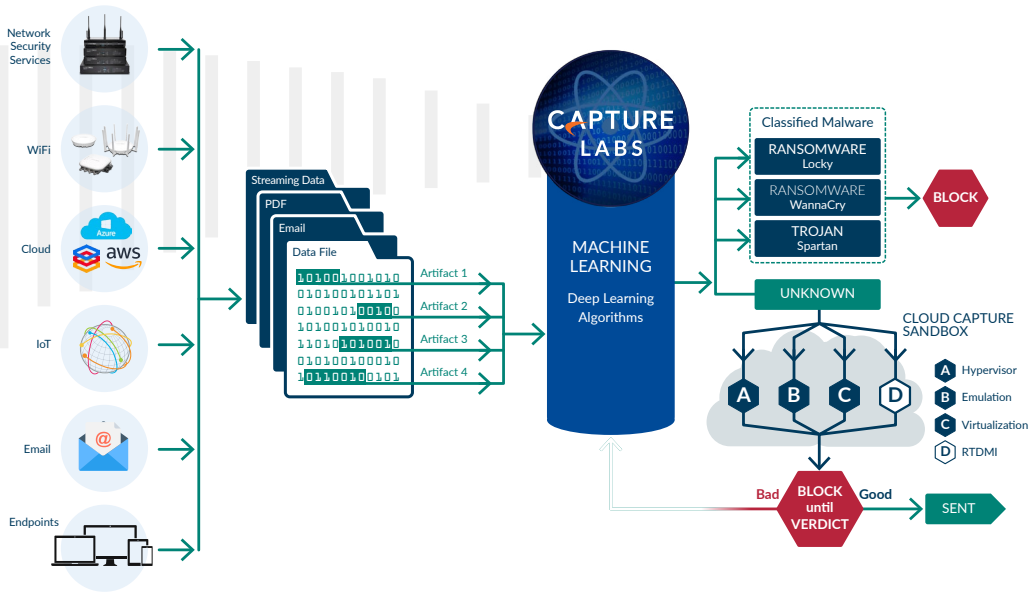
Discover and stop zero-day and other unknown attacks

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. Capture Advanced Threat Prevention (Capture ATP), was the industry's first multi-engine sandbox that could block until verdict. This technology quickly returns an accurate verdict on suspicious files and can be used across the ecosystem of SonicWall products.

HIGHLIGHTS

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

Read the Solution Brief:

sonicwall.com/sandbox-strategy

DATASHEET

To protect customers against the increasing dangers of zero-day threats, SonicWall Capture Advanced Threat Protection (ATP) Service — a cloud-based service available with SonicWall firewalls — detects 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 SonicWall's Real-Time Deep Memory Inspection (RTDMI™), 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.

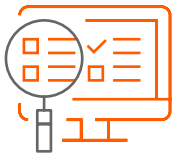
Features

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

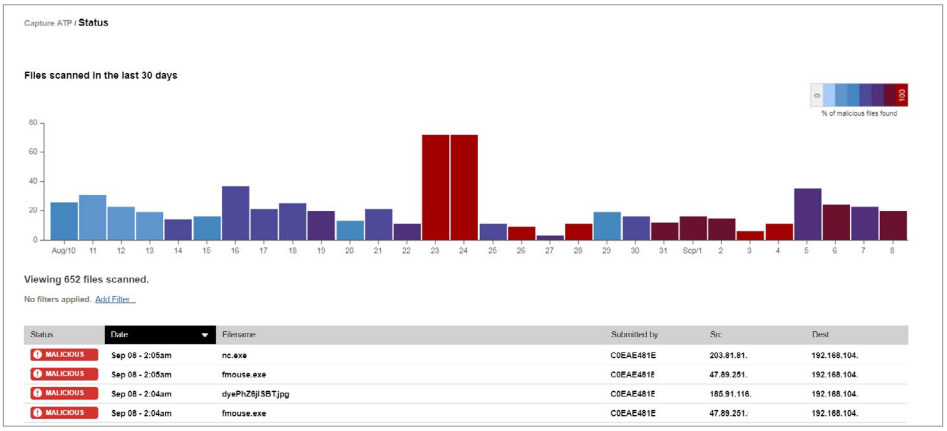
To prevent potentially malicious files from entering the network, files sent to the cloud service for analysis can be held at the gateway until a verdict is determined.

RAPID DEPLOYMENT OF REMEDIATION SIGNATURES

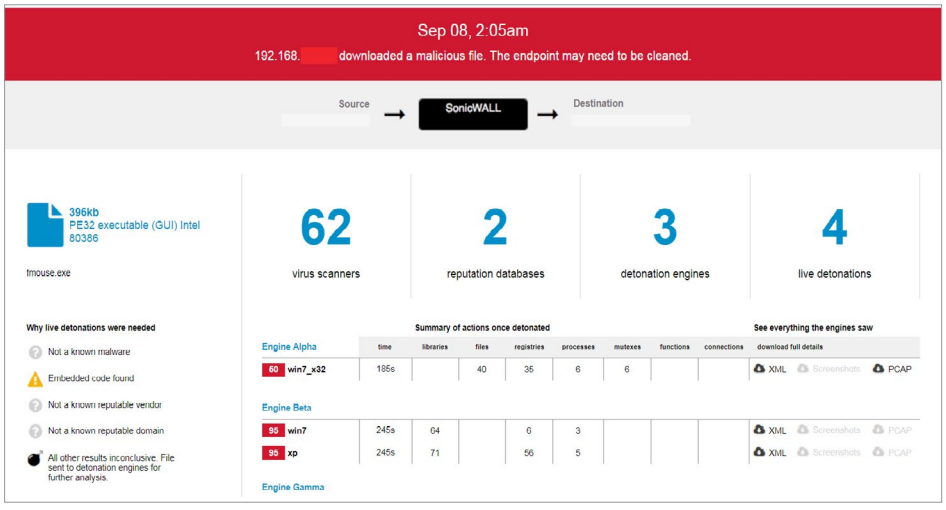
When a file is identified as malicious, a signature is immediately available to firewalls with the SonicWall Capture ATP subscription to prevent follow-on attacks. In addition, the malware is submitted to the SonicWall Capture Labs threat research team for further analysis and inclusion with threat information 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.



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.



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* 15700	NS*sp* 12800	NS*sp* 12400
NS*a* 9650	NS*a* 6650	NS*a* 3700
NS*a* 9450	NS*a* 5650	NS*a* 3650
NS*a* 9250	NS*a* 4700	NS*a* 2700
NS*a* 6700	NS*a* 4650	NS*a* 2650
TZ670 series	TZ500 and 570 series	TZ300, 350 and 370 series
TZ600 series	TZ400 and 470 series	SOHO 250 series
Email Security appliances, software and Hosted Email Security (OS 9.0 and above)		
WAF Series		
SMA 6200, 7200, 8200v (OS 12.0 and above)		
SMA 200, 400, 500v (OS 9.1 and above)		
Capture Client Advanced		

Ask Sales@SonicWall for a Next-generation Firewall demo with Capture ATP enabled today

sales@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 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