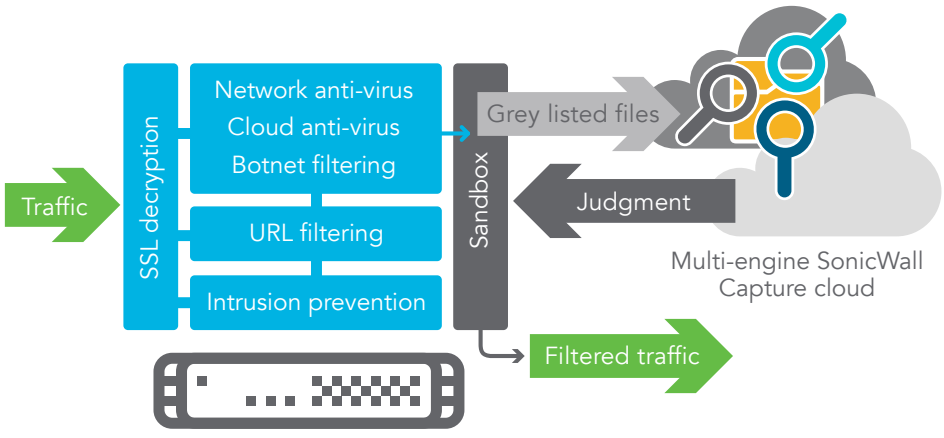
SonicWall Capture Advanced Threat Protection Service

Multiply the effectiveness of your advanced threat protection sandbox

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 Advance 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.



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

Benefits:

- High security effectiveness against unknown threats
- Near real-time signature deployment protects from follow on attacks
- Reduced total cost of ownership

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 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 cloud service for analysis. The multi-engine sandbox platform, which includes 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.

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.

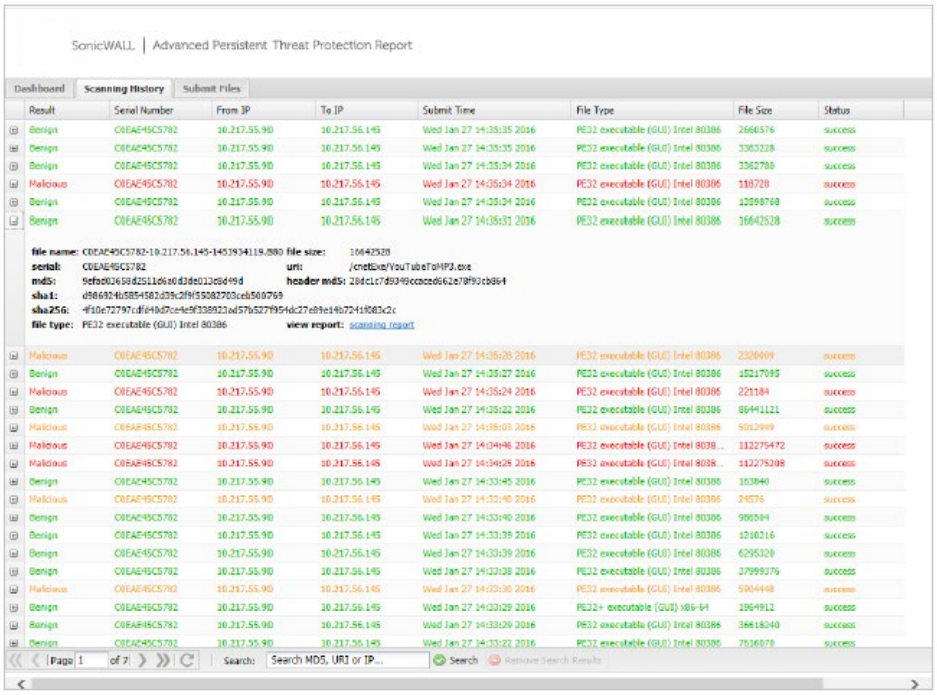
Rapid deployment of remediation signatures — When a file is identified as malicious, a signature is immediately available to firewalls with SonicWall Capture subscriptions to prevent follow-on attacks. In addition, the malware is submitted to the SonicWall Threat Intelligence Team for further analysis 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.

The SonicWall Capture Service Status page displays an at-a-glance bar chart that indicates the number of files submitted and the percentage of files found to be malicious over a 30 day period. The file history table lists all files scanned, the verdict of analysis and the source and destination. Filters allow you to quickly drill down by date, file status, file name, source or destination. Selecting a file displays a detailed file analysis report.

Reporting and alerts — The SonicWall Capture 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 Service, and file analysis verdict.

About Us

Over a 25 year history, SonicWall has been the industry's trusted security partner. From network security to access security to email security, SonicWall has continuously evolved its product portfolio, enabling organizations to innovate, accelerate and grow. With over a million security devices in almost 200 countries and territories worldwide, SonicWall enables its customers to confidently say yes to the future.



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

Supported platforms:

Dell SonicWall Capture Service is supported on the following Dell SonicWall network security appliances running SonicOS 6.2.6 and higher:

SuperMassive 9600
SuperMassive 9400
SuperMassive 9200

NSA 6600
NSA 5600
NSA 4600
NSA 3600
NSA 2600

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

SonicWall, Inc.
5455 Great America Parkway | Santa Clara, CA 95054
Refer to our website for additional information.
www.sonicwall.com

Datasheet-AdvancedThreatProtection-US-KJ-24691