Security

Dell SonicWALL Capture Advanced Threat Protection Service

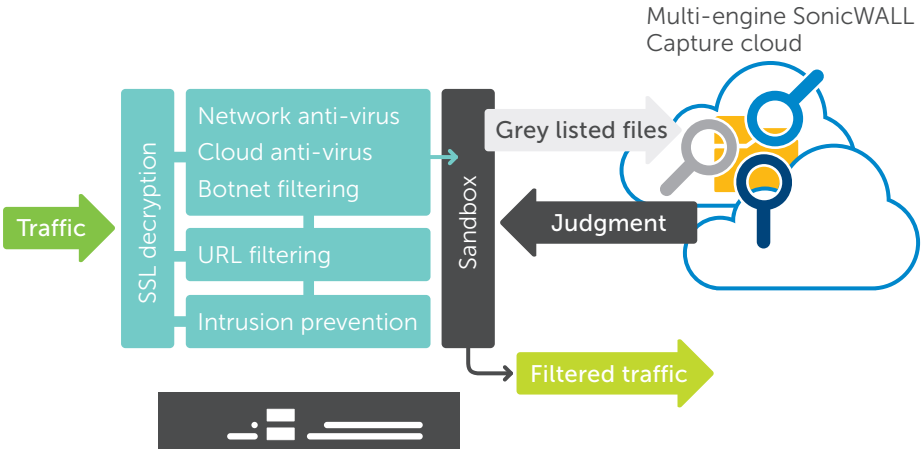
Multiply the effectiveness of your advanced threat protection sandbox

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, Dell SonicWALL Capture Advance Threat Protection Service — a cloud-based service available with Dell SonicWALL firewalls — detects and blocks until verdict advanced threats at the gateway. 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, has no file size limitation. Global-threat intelligence infrastructure rapidly deploys remediation signatures for newly identified threats to all Dell 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
- Fast response times
- 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 — Dell 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 Dell 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 and no file-size limitation — The service supports analysis of files of any size and for a broad range of file types, including executable programs (PE), DLL, PDFs, MS Office documents, archives, JAR and APK, plus multiple operating systems including Windows, Android and Mac OSX. 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 deployed to firewalls with Dell SonicWALL Capture subscriptions to prevent follow-on attacks. In addition, the malware is submitted to the Dell 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 Dashboard displays the number of malicious and benign file scanned over the previous 30 days.

Supported platforms:

Dell SonicWALL Capture Service is supported on the following Dell SonicWALL network security appliances running SonicOS 6.2.5 and higher:

SuperMassive 9600
SuperMassive 9400
SuperMassive 9200

NSA 6600
NSA 5600
NSA 4600
NSA 3600
NSA 2600

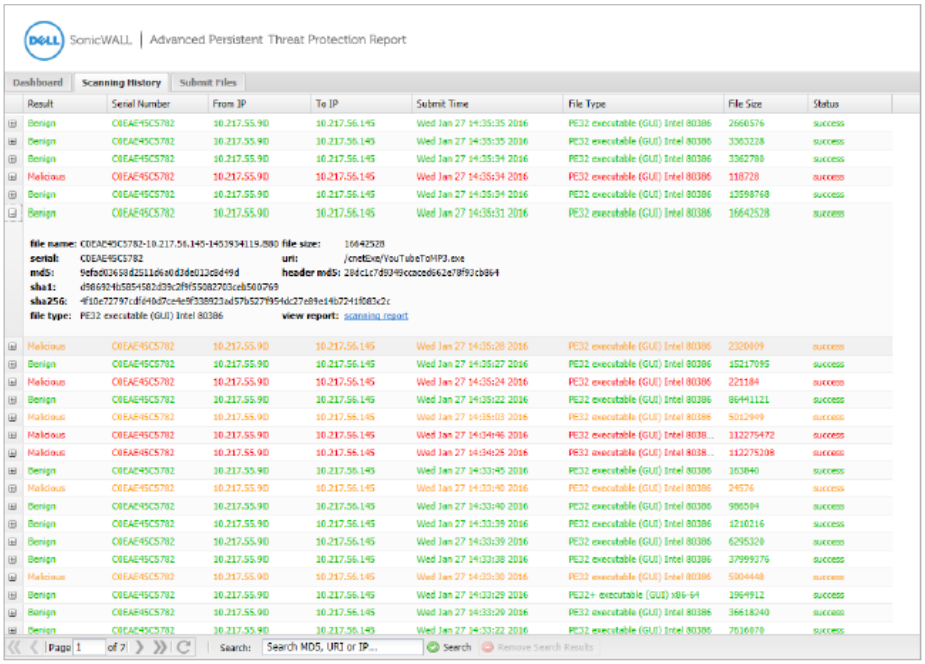
TZ600
TZ500 and TZ500 Wireless
TZ400 and TZ400 Wireless
TZ300 and TZ300 Wireless

SOHO Wireless

Reporting and alerts — The Dell SonicWALL Capture Service provides an at-a-glance threat analysis dashboard and reports, which details out the analysis results for files sent to the service. Information included in these reports include session data, OS information, and OS and network activity. Firewall log alerts provide notification of suspicious files sent to the Dell SonicWALL Capture Service, and file analysis verdict.

About Dell Security

Dell Security solutions help you create and maintain a strong security foundation with interconnected solutions that span the enterprise. From endpoints and users to networks, data and identity, Dell Security solutions mitigate risk and reduce complexity so you can drive your business forward. www.dell.com/security



The file history report lists all files scanned, analyzed and the verdict of analysis. A detailed analysis report is also available for analyzed files.

Dell
5455 Great America Parkway, Santa Clara, CA 95054
www.dell.com/security
If you are located outside North America, you can find local office information on our web site.

Datasheet-SonicWALL-APTSandboxing-US-VG-27700