SonicWall Capture Advanced Threat Protection Service (01-SSC-8930)

SonicWall Capture Advanced Threat Protection Service - Subscription licence (1 year) - for NSa 6650, 6650 High Availability

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 agai Threat Protection Service - a cloud-based service available with SonicWall firewalls - detects and can block advanced threats at the gateway until verdict. This service combines multi-layer sandboxing, including full system emulation and virtualization techniques, to analyze suspicious code behavior.The solution scans 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.

Key Selling Points

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

Product 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. 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.

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.

Main Specifications

Product Description	*SonicWall Capture Advanced Threat Protection Service - subscription licence (1 year) - 1 licence*
Product Type	*Subscription licence - 1 year*
Category	*Online & appliance based services - advanced threat detection*
Licence Qty	*1 licence*
Designed For	*NSa 6650, 6650 High Availability*

Extended Specification

General

Category	*Online & appliance based services - advanced threat detection*
Product Type	*Subscription licence - 1 year*

Compatibility Information

Designed For	*SonicWall NSa 6650, 6650 High Availability*

Licencing

Licence Qty	*1 licence*