

Dell SonicWALL Capture Advanced Threat Protection Service

Multiply the effectiveness of your advanced threat protection sandbox

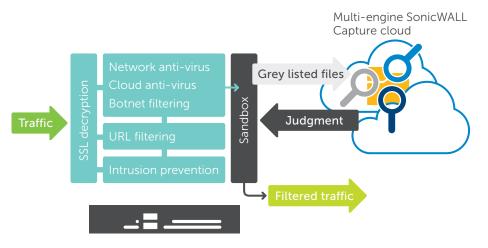
For effective zero-day threat protection, organizations need solutions that include malware-analysis technologies and can detect evasive advanced threats and malware — today and tomorrow.

To protect customers against the increasing dangers of zero-day threats, Dell SonicWALL Capture Advance Threat Protection Service – a cloudbased 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.

Benefits:

- High security effectiveness
- Fast response times
- Reduced total cost of ownership



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

Features

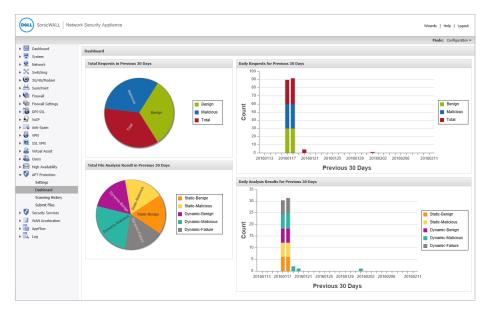
Multi-engine advanced threat analysis - Dell SonicWALL Capture Service extends firewall threat protection to detect and prevent zeroday attacks. The firewall inspects traffic, and detects and blocks intrusions and known malware. Suspicious files are sent to the Dell SonicWALL Capture cloud service for analysis. The multiengine sandbox platform, which includes virtualized sandboxing, full system emulation and hypervisorlevel analysis technology, executes suspicious code and analyzes behavior, provides comprehensive visibility to malicious activity while resisting evasion tactics and maximizing zeroday threat detection.

Broad file type analysis and no filesize 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.

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



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

De	shboard	Scanning History	Submit Files					
	Result	Serial Number	From JP	To IP	Submit Time	File Type	File Size	Status
8	Benign	C0EAE45C5782	10.217,55.90	10.217.56.145	Wed Jan 27 14:35:35 2016	PE32 executable (GUI) Intel 80386	2660576	success
в	Denign	C0EAE45C5782	10.217.55.90	10.217.55.145	Wed Jan 27 14:35:35 2016	PE32 executable (GUI) Intel 80386	3363228	success
Ð	Benign	C0EAE45C5782	10.217.55.90	10.217.55.145	Wed Jan 27 14:35:34 2016	PE32 executable (GUI) Intel 80386	3362780	success
Ð	Nalicious	OIEAE45C5782	10.217.55.90	10.217.55.145	Wed Jan 27 14:35:34 2016	PE32 executable (GUI) Intel 80386	118728	SUCCESS
Ð	Benign	C0EAE45C5782	10.217.55.90	10.217.56.145	Wed Jan 27 14:35:34 2016	PE32 executable (GUI) Intel 80386	13598768	success
9	Benign	OIEAE45C5782	10.217.55.90	10.217.56.145	Wed Jan 27 14:35:31 2016	PE32 executable (GUI) Intel 80386	16642528	SUCCESS
	serial: md5: sha1: sha256:	CDEAE45C5782 9efad03658d2511d6a0d d986924b5854582d39c3	i3de013c8d49d 2f9f55082703ceb500769 4e9f338923ad57b527f954					
				new report. Saming rep	210			
	Nalicious	OIEAE45C5782	10.217.55.90	10.217.55.145	Wed Jan 27 14:35:28 2016	PE32 executable (GUI) Intel 80386	2320109	SUCCESS
	Malicious Benign	OIEAE45C5782 C0EAE45C5782				PE32 executable (GUE) Entel 80386 PE32 executable (GUE) Entel 80386	2320109	SUCCESS
Ð			10.217.55.90	10.217.55.145	Wed Jan 27 14:35:28 2016	PE32 executable (GUI) Intel 80386 PE32 executable (GUI) Intel 80386		
•	Benign	C0EAE45C5782 C0EAE45C5782 C0EAE45C5782	10.217.55.90 10.217.55.90 10.217.55.90 10.217.55.90 10.217.55.90	10.217.56.145 10.217.56.145 10.217.56.145 10.217.56.145 10.217.56.145	Wed Jan 27 14:35:28 2016 Wed Jan 27 14:35:27 2016 Wed Jan 27 14:35:24 2016 Wed Jan 27 14:35:24 2016 Wed Jan 27 14:35:22 2016	PE32 executable (GUI) Intel 80386 PE32 executable (GUI) Intel 80386 PE32 executable (GUI) Intel 80386	15217095 221184 86441121	success
10 10 10	Benign Malicious	C0EAE45C5782 C0EAE45C5782	10.217.55.90 10.217.55.90 10.217.55.90	10.217.56.145 10.217.56.145 10.217.56.145	Wed Jan 27 14:35:28 2016 Wed Jan 27 14:35:27 2016 Wed Jan 27 14:35:24 2016	PE32 executable (GUI) Intel 80386 PE32 executable (GUI) Intel 80386	15217095 221184	success success
	Benign Malicious Benign	C0EAE45C5782 C0EAE45C5782 C0EAE45C5782	10.217.55.90 10.217.55.90 10.217.55.90 10.217.55.90 10.217.55.90	10.217.56.145 10.217.56.145 10.217.56.145 10.217.56.145 10.217.56.145	Wed Jan 27 14:35:28 2016 Wed Jan 27 14:35:27 2016 Wed Jan 27 14:35:24 2016 Wed Jan 27 14:35:24 2016 Wed Jan 27 14:35:22 2016	PE32 executable (GUI) Intel 80386 PE32 executable (GUI) Intel 80386 PE32 executable (GUI) Intel 80386	15217095 221184 86441121	success success success
	Benign Malicious Benign Malicious	C0EAE45C5782 C0EAE45C5782 C0EAE45C5782 C0EAE45C5782	10.217.55.90 10.217.55.90 10.217.55.90 10.217.55.90 10.217.55.90	10.217.55.145 10.217.55.145 10.217.55.145 10.217.55.145 10.217.55.145 10.217.55.145	Wed Jan 27 14:35:28 2016 Wed Jan 27 14:35:27 2016 Wed Jan 27 14:35:24 2016 Wed Jan 27 14:35:22 2016 Wed Jan 27 14:35:22 2016 Wed Jan 27 14:35:03 2016	PE32 executable (GUI) Intel 80386 PE32 executable (GUI) Intel 80386 PE32 executable (GUI) Intel 80386 PE32 executable (GUI) Intel 80386	15217095 221184 86441121 5012949	SUCCESS SUCCESS SUCCESS SUCCESS
	Benign Malicious Benign Malicious Malicious	C0EAE45C5782 C0EAE45C5782 C0EAE45C5782 C0EAE45C5782 C0EAE45C5782 C0EAE45C5782	10.217.55.90 10.217.55.90 10.217.55.90 10.217.55.90 10.217.55.90 10.217.55.90 10.217.55.90	10217.56.145 10217.56.145 10217.56.145 10217.56.145 10217.56.145 10217.56.145 10217.56.145	Wed Jan 27 14:35:28 2016 Wed Jan 27 14:35:27 2016 Wed Jan 27 14:35:24 2016 Wed Jan 27 14:35:22 2016 Wed Jan 27 14:35:03 2016 Wed Jan 27 14:35:03 2016	PE32 executable (GUI) Intel 80396 PE32 executable (GUI) Intel 80396 PE32 executable (GUI) Intel 80396 PE32 executable (GUI) Intel 80396 PE32 executable (GUI) Intel 8038	15217095 221184 86441121 5012949 112275472	success auccess success success success
	Benign Melicious Benign Nalicious Nalicious Nalicious	C0EAE45C5782 C0EAE45C5782 C0EAE45C5782 C0EAE45C5782 C0EAE45C5782 C0EAE45C5782 C0EAE45C5782	10.217,55.90 10.217,55.90 10.217,55.90 10.217,55.90 10.217,55.90 10.217,55.90 10.217,55.90 10.217,55.90	10.217.56.145 10.217.56.145 10.217.56.145 10.217.55.145 10.217.55.145 10.217.56.145 10.217.55.145	Wed Jan 27 14:35:28 2016 Wed Jan 27 14:35:27 2016 Wed Jan 27 14:35:24 2016 Wed Jan 27 14:35:22 2016 Wed Jan 27 14:35:83 2016 Wed Jan 27 14:34:25 2016 Wed Jan 27 14:34:25 2016	PE32 executable (GUI) Intel 80396 PE32 executable (GUI) Intel 80396 PE32 executable (GUI) Intel 80396 PE32 executable (GUI) Intel 80398. PE32 executable (GUI) Intel 8038.	15217095 221184 86441121 5012949 112275472 112275208	SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS
	Benign Melicious Benign Malicious Nalicious Nalicious Denign	C0EAE45C5782 C0EAE45C5782 C0EAE45C5782 C0EAE45C5782 C0EAE45C5782 C0EAE45C5782 C0EAE45C5782 C0EAE45C5782	10.217.55.90 10.217.55.90 10.217.55.90 10.217.55.90 10.217.55.90 10.217.55.90 10.217.55.90 10.217.55.90 10.217.55.90	10.217.55.145 10.217.55.145 10.217.55.145 10.217.55.145 10.217.55.145 10.217.55.145 10.217.55.145 10.217.55.145	Wed Jan 27 14:35:28 2016 Wed Jan 27 14:35:27 2016 Wed Jan 27 14:35:27 2016 Wed Jan 27 14:35:22 2016 Wed Jan 27 14:35:22 2016 Wed Jan 27 14:35:23 2016 Wed Jan 27 14:35:23 2016 Wed Jan 27 14:35:23 2016 Wed Jan 27 14:35:42:52 2016 Wed Jan 27 14:35:42:52 2016 Wed Jan 27 14:35:42:52 2016	PE32 executable (GUT) Intel 80386 PE32 executable (GUT) Intel 80386 PE32 executable (GUT) Intel 80386 PE32 executable (GUT) Intel 80386 PE32 executable (GUT) Intel 80380 PE32 executable (GUT) Intel 80380	15217095 221184 86441121 5012949 112275472 112275208 163840	SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS
	Benign Nalicious Benign Nalicious Nalicious Denign Nalicious	C0EAE45C5782 C0EAE45C5782 C0EAE45C5782 C0EAE45C5782 C0EAE45C5782 C0EAE45C5782 C0EAE45C5782 C0EAE45C5782	10 217.55.90 10 217.55.90 10 217.55.90 10 217.55.90 10 217.55.90 10 217.55.90 10 217.55.90 10 217.55.90 10 217.55.90	10,217,56,145 10,217,56,145 10,217,56,145 10,217,56,145 10,217,56,145 10,217,56,145 10,217,56,145 10,217,56,145	Wed Jan 27 14:05:02 2016 Wed Jan 27 14:05:02 0016 Wed Jan 27 14:04:04 0016	PE32 executable (GUI) Intel 80396 PE32 executable (GUI) Intel 80396 PE32 executable (GUI) Intel 80396 PE32 executable (GUI) Intel 8038. PE32 executable (GUI) Intel 8038. PE32 executable (GUI) Intel 8039. PE32 executable (GUI) Intel 8039.	15217095 221184 86441121 5012949 112275472 112275208 103840 24576	SUCCES SUCCES SUCCES SUCCES SUCCES SUCCES SUCCES
	Benign Melicious Benign Malicious Malicious Benign Malicious Benign	C0EAE45C5782 C0EAE45C5782 C0EAE45C5782 C0EAE45C5782 C0EAE45C5782 C0EAE45C5782 C0EAE45C5782 C0EAE45C5782 C0EAE45C5782 C0EAE45C5782	10.217.55.90 10.217.55.90 10.217.55.90 10.217.55.90 10.217.55.90 10.217.55.90 10.217.55.90 10.217.55.90 10.217.55.95 10.217.55.95	10217.56.145 10217.56.145 10217.56.145 10217.56.145 10217.56.145 10217.56.145 10217.56.145 10217.56.145 10217.56.145	Wed Jan 27 14/35/28 2016 Wed Jan 27 14/35/27 2016 Wed Jan 27 14/35/27 2016 Wed Jan 27 14/35/27 2016 Wed Jan 27 14/35/07 2016 Wed Jan 27 14/35/07 2016 Wed Jan 27 14/35/27 2016 Wed Jan 27 14/36/27 2016 Wed Jan 27 14/36/27 2016 Wed Jan 27 14/36/27 2016 Wed Jan 27 14/36/2016	PE22 executable (GUT) Intel 80396 PE22 executable (GUT) Intel 80396 PE22 executable (GUT) Intel 80396 PE22 executable (GUT) Intel 80386 PE22 executable (GUT) Intel 80396 PE22 executable (GUT) Intel 80396 PE22 executable (GUT) Intel 80396 PE22 executable (GUT) Intel 80396	15217095 221184 86441121 5012949 112275472 112275208 163840 24576 900594	SUCCES SUCCES SUCCES SUCCES SUCCES SUCCES SUCCES SUCCES
	Benign Malicious Benign Malicious Malicious Denign Benign Benign	C0EAE45C5782 C0EAE45C5782 C0EAE45C5782 C0EAE45C5782 C0EAE45C5782 C0EAE45C5782 C0EAE45C5782 C0EAE45C5782 C0EAE45C5782	10 217.55.90 10 217.55.90 10 217.55.90 10 217.55.90 10 217.55.90 10 217.55.90 10 217.55.90 10 217.55.90 10 217.55.90 10 217.55.90	10217.56.145 10217.56.145 10217.56.145 10217.56.145 10217.56.145 10217.56.145 10217.56.145 10217.56.145 10217.56.145	Wed Jan 27 14:35:28 2016 Wed Jan 27 14:35:27 2016 Wed Jan 27 14:35:27 2016 Wed Jan 27 14:35:27 2016 Wed Jan 27 14:35:27 2016 Wed Jan 27 14:35:40 2016 Wed Jan 27 14:35:40 2016 Wed Jan 27 14:33:40 2016 Wed Jan 27 14:33:40 2016 Wed Jan 27 14:33:40 2016 Wed Jan 27 14:33:40 2016	PE22 executable (GUT) Intel 80306 PE32 executable (GUT) Intel 80306	15217095 221184 86441121 5012949 112275472 112275208 103840 24576 900594 1210216	SUCCES SUCCES SUCCES SUCCES SUCCES SUCCES SUCCES SUCCES SUCCES
	Benign Małkiowa Benign Małkiowa Nałkiowa Denign Benign Benign Benign	C0EAE45C5792 C0EAE45C5792 C0EAE45C5792 C0EAE45C5792 C0EAE45C5792 C0EAE45C5792 C0EAE45C5792 C0EAE45C5792 C0EAE45C5792 C0EAE45C5792 C0EAE45C5792	10.217.55.90 10.217.55.90 10.217.55.90 10.217.55.90 10.217.55.90 10.217.55.90 10.217.55.90 10.217.55.90 10.217.55.90 10.217.55.90	10/217.56.145 10/217.56.145 10/217.56.145 10/217.56.145 10/217.56.145 10/217.56.145 10/217.56.145 10/217.56.145 10/217.56.145 10/217.56.145	Wed Jan 27 14:35:28 2016 Wed Jan 27 14:35:27 3036 Wed Jan 27 14:35:22 3016 Wed Jan 27 14:35:22 3016 Wed Jan 27 14:35:22 3016 Wed Jan 27 14:34:46 3016 Wed Jan 27 14:34:46 3016 Wed Jan 27 14:34:40 3016 Wed Jan 27 14:32:40 3016 Wed Jan 27 14:32:40 3016 Wed Jan 27 14:32:40 3016 Wed Jan 27 14:33:40 3016 Wed Jan 27 14:33:9 3016	PE22 executable (GUI) Intel 80386 PE32 executable (GUI) Intel 80386	15217095 221184 86441121 5012449 112275472 112275208 105040 24556 986594 1210216 6295329	SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS
	Benign Natious Benign Natious Natious Denign Natious Denign Benign Benign Benign	016AE45C5792 016AE45C5792 016AE45C5792 016AE45C5792 016AE45C5792 016AE45C5792 016AE45C5792 016AE45C5792 016AE45C5792 016AE45C5792 016AE45C5792	10.217.55.90 10.217.55.90 10.217.55.90 10.217.55.90 10.217.55.90 10.217.55.90 10.217.55.90 10.217.55.90 10.217.55.90 10.217.55.90 10.217.55.90	10.217.55.145 10.217.55.145 10.217.55.145 10.217.55.145 10.217.55.145 10.217.55.145 10.217.55.145 10.217.55.145 10.217.55.145 10.217.55.145 10.217.55.145	Wed Jan 27 14:35:28 2016 Wed Jan 27 14:35:27 2016 Wed Jan 27 14:35:27 2016 Wed Jan 27 14:35:21 2016 Wed Jan 27 14:35:21 2016 Wed Jan 27 14:35:2016	PE22 executable (GUI) Intel 8036 PE22 executable (GUI) Intel 8036 PE22 executable (GUI) Intel 8036 PE22 executable (GUI) Intel 8036. PE22 executable (GUI) Intel 8036. PE22 executable (GUI) Intel 8036 PE22 executable (GUI) Intel 8036	15217095 221184 86441121 5012949 112275472 112275208 163840 24575 980594 1210216 6295320 37999376	success auccess auccess auccess auccess auccess auccess auccess auccess auccess auccess auccess auccess auccess
	Benign Natious Benign Natious Natious Denign Natious Denign Benign Benign Benign Benign Benign	CODARISCIPIC CODARISCIPIC CODARISCIPIC CODARISCIPIC CODARISCIPIC CODARISCIPIC CODARISCIPIC CODARISCIPIC CODARISCIPIC CODARISCIPIC CODARISCIPIC CODARISCIPIC CODARISCIPIC CODARISCIPIC CODARISCIPIC CODARISCIPIC	10.217.55.90 10.217.55.90 10.217.55.90 10.217.55.90 10.217.55.90 10.217.55.90 10.217.55.90 10.217.55.90 10.217.55.90 10.217.55.90 10.217.55.90 10.217.55.90	10,217,55,145 10,217,55,145 10,217,55,145 10,217,55,145 10,217,55,145 10,217,55,145 10,217,55,145 10,217,55,145 10,217,55,145 10,217,55,145 10,217,55,145	Wed Jan 27 14:35:28 2016 Wed Jan 27 14:35:27 2016 Wed Jan 27 14:35:27 2016 Wed Jan 27 14:35:22 2016 Wad Jan 27 14:35:22 2016 Wad Jan 27 14:35:22 2016 Wed Jan 27 14:35:23 2016 Wed Jan 27 14:35:24 2016 Wed Jan 27 14:35:24 2016 Wed Jan 27 14:35:25 2016 Wed Jan 27 14:35:29 2016 Wed Jan 27 14:35:20 2016 Wed Jan 27 14:35:20 2016	PE22 executable (GUT) Intel 80306 PE32 executable (GUT) Intel 80306	15217095 221184 8644121 501209 112275472 112275208 163840 24576 986594 1210215 986594 1210215 24576 986594 1210215 24576 5004448	SUCCES SUCCES SUCCES SUCCES SUCCES SUCCES SUCCES SUCCES SUCCES

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

© 2016 Dell Inc. ALL RIGHTS RESERVED. Dell and Dell Security logo and products—as identified in this document—are trademarks or registered trademarks of Dell, Inc. in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners. Datasheet-SonicWALL-APTSandboxing-US-VG-27700

