

SonicWall Capture Advanced Threat Protection Service

Steigern Sie die Effizienz Ihrer ATP-Sandbox

Für einen effektiven Schutz vor Zero-Day-Bedrohungen benötigen Unternehmen Lösungen mit Malware-Analysetechnologien, die auch in Zukunft raffinierte, schwer zu fassende Bedrohungen und Malware aufspüren können.

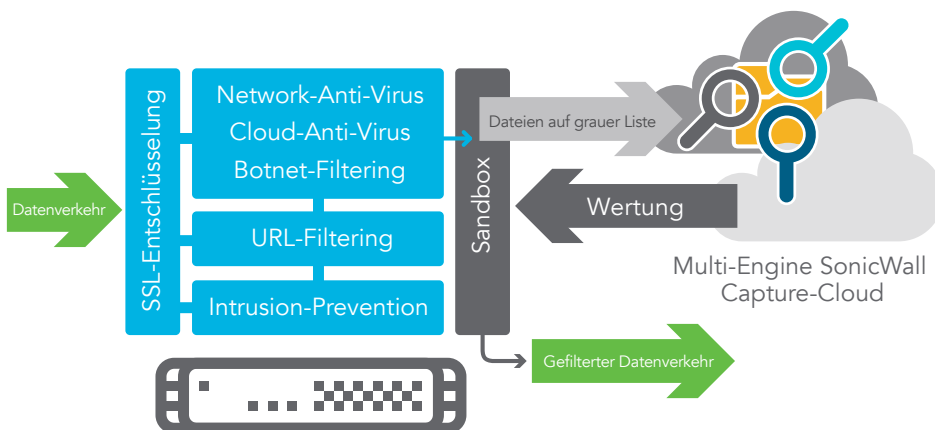
Um Kunden vor den wachsenden Zero-Day-Bedrohungen zu schützen, erkennt und blockiert der mit den SonicWall-Firewalls erhältliche SonicWall Capture Advanced Threat Protection Service raffinierte Bedrohungen am Gateway, bis der Sicherheitsstatus geklärt ist. Bei diesem Cloud-basierten Service handelt es sich um den einzigen erweiterten Bedrohungsschutz, der mehrschichtiges Sandboxing mit umfassender Systemsimulation und Virtualisierungstechniken für die Analyse verdächtiger Codeaktivitäten bietet.

Dank seiner leistungsstarken Features lassen sich mehr Bedrohungen aufspüren als mit umgebungsspezifischen Single-Engine-Sandbox-Lösungen, die leichter zu umgehen sind.

Die Lösung prüft den Datenverkehr und extrahiert verdächtigen Code, um ihn anschließend zu analysieren. Im Gegensatz zu anderen Gateway-Lösungen lassen sich unterschiedlichste Dateitypen unabhängig von der Größe analysieren. Die Global Threat Intelligence-Infrastruktur sorgt für eine schnelle Implementierung von Signaturen für neu identifizierte Bedrohungen auf allen Netzwerksicherheitsappliances von SonicWall und verhindert so eine weitere Verbreitung. Kunden profitieren von hocheffizienten Sicherheitsmechanismen, schnellen Reaktionszeiten und niedrigeren Total Cost of Ownership.

Vorteile:

- Hocheffiziente Sicherheitsmechanismen gegen unbekannte Bedrohungen
- Eine Implementierung von Signaturen nahezu in Echtzeit schützt vor Folgeangriffen
- Niedrigere Total Cost of Ownership



Eine Cloud-basierte Multi-Engine-Lösung, die unbekannte Zero-Day-Angriffe am Gateway stoppt

Größtmöglicher Schutz vor Zero-Day-Bedrohungen: Die Lösung wurde so konzipiert, dass sie neue Malware-Analysetechnologien dynamisch einbindet, sobald sich die Bedrohungslandschaft verändert.

Funktionen

Erweiterte Multi-Engine-

Bedrohungsanalyse: Der SonicWall Capture Service erweitert den Firewall-Bedrohungsschutz, um Zero-Day-Angriffe zu erkennen und zu verhindern. Die Firewall inspiziert den Verkehr und erkennt und blockiert Eindringlinge sowie bekannte Malware. Verdächtige Dateien werden zur Analyse an den SonicWall Capture-Cloud-Service weitergeleitet. Die Multi-Engine-Sandbox-Plattform mit virtualisiertem Sandboxing, umfassender Systemsimulation und einer Analysetechnologie auf Hypervisor-Ebene führt verdächtigen Code aus, analysiert dessen Verhalten und macht böswertige Aktivitäten transparent, ohne sich von Umgehungstaktiken austricksen zu lassen, und sorgt so für einen größtmöglichen Schutz vor Zero-Day-Bedrohungen.

Analyse unterschiedlichster

Dateitypen: Der Service unterstützt die Analyse unterschiedlichster Dateitypen unabhängig von ihrer Größe, darunter ausführbare Programme (PE), DLL, PDFs, MS Office-Dokumente, Archive,

JAR und APK sowie unterschiedliche Betriebssysteme wie Windows und Android. Administratoren können die Schutzmechanismen personalisieren, indem sie Dateien auswählen oder ausschließen, die zur Analyse in die Cloud geschickt werden. Die Analyse kann dabei nach Dateityp, Dateigröße, Absender, Empfänger oder Protokoll erfolgen. Darüber hinaus können Administratoren Dateien manuell zur Analyse an den Cloud-Service weiterleiten.

Blockieren bis zur Klärung des

Sicherheitsstatus: Um zu verhindern, dass potenziell böswertige Dateien in das Netzwerk eindringen, können die zur Analyse an den Cloud-Service gesendeten Dateien am Gateway festgesetzt werden, bis der Sicherheitsstatus geklärt ist.

Schnelle Implementierung von

Signaturen zur Problemlösung: Wird eine Datei als böswertig identifiziert, erhalten die mit SonicWall Capture-Abos ausgestatteten Firewalls umgehend



Die SonicWall Capture Service Status-Seite enthält ein übersichtliches Balkendiagramm mit der Anzahl an weitergeleiteten Dateien und dem Prozentsatz der für verdächtig befundenen Dateien über einen Zeitraum von 30 Tagen. Die Tabelle zur Dateihistorie zeigt alle geprüften Dateien, das Ergebnis der Analyse sowie die Quelle und das Ziel an. Mithilfe von Filtern können Sie die Daten schnell und einfach nach Datum, Dateistatus, Dateiname, Quelle oder Ziel aufschlüsseln. Durch Auswählen einer Datei erscheint ein detaillierter Analysebericht.

eine Signatur, um Folgeangriffe zu verhindern. Außerdem wird die Malware an das SonicWall Threat Intelligence-Team zur weiteren Analyse und zum Einpflegen der Bedrohungsinformationen in die Gateway-Anti-Virus- und IPS-Signaturendatenbanken weitergeleitet. Zusätzlich erfolgt innerhalb von 48 Stunden eine Übermittlung an URL-, IP- und Domain-Reputation-Datenbanken.

Berichte und Warnungen: Der SonicWall Capture Service bietet ein übersichtliches Bedrohungsanalyse-Dashboard und Berichte mit detaillierten Analyseergebnissen für die an den Service weitergereichten Dateien, z. B. Quelle, Ziel und eine Zusammenfassung mit Details zu den eingeleiteten Anti-Malware-Maßnahmen. Firewall-Protokollwarnungen melden, wenn verdächtige Dateien an den SonicWall Capture Service gesendet werden, und teilen das Ergebnis der Dateianalyse mit.

Über uns

Seit über 25 Jahren ist SonicWall als zuverlässiger Sicherheitspartner bekannt. Von Access-Security über Netzwerksicherheit bis zu E-Mail-Security: Wir haben unser Produktportfolio kontinuierlich weiterentwickelt, damit unsere Kunden Innovationen realisieren, Prozesse beschleunigen und wachsen können. Mit über einer Million Sicherheitsgeräte in nahezu 200 Ländern und Regionen weltweit bietet SonicWall seinen Kunden alles, was sie brauchen, um für die Zukunft gerüstet zu sein.

Unterstützte Plattformen:

Der SonicWall Capture Service wird von folgenden SonicWall-Netzwerksicherheitsappliances unter SonicOS 6.2.6 und höher unterstützt:

SuperMassive 9600
SuperMassive 9400
SuperMassive 9200

NSA 6600
NSA 5600
NSA 4600
NSA 3600
NSA 2600

TZ600
TZ500 und TZ500 Wireless
TZ400 und TZ400 Wireless
TZ300 und TZ300 Wireless

SonicWALL | Advanced Persistent Threat Protection Report

Result	Serial Number	From IP	To IP	Submit Time	File Type	File Size	Status
Benign	CEAE49C5792	10.217.55.90	10.217.55.145	Wed Jan 27 14:35:35 2016	PE32 executable (GUI) Intel 80386	2660576	success
Benign	CEAE49C5792	10.217.55.90	10.217.55.145	Wed Jan 27 14:35:35 2016	PE32 executable (GUI) Intel 80386	3363228	success
Benign	CEAE49C5792	10.217.55.90	10.217.55.145	Wed Jan 27 14:35:34 2016	PE32 executable (GUI) Intel 80386	3362780	success
Malicious	CEAE49C5792	10.217.55.90	10.217.55.145	Wed Jan 27 14:35:34 2016	PE32 executable (GUI) Intel 80386	118728	success
Benign	CEAE49C5792	10.217.55.90	10.217.55.145	Wed Jan 27 14:35:34 2016	PE32 executable (GUI) Intel 80386	12098769	success
Benign	CEAE49C5792	10.217.55.90	10.217.55.145	Wed Jan 27 14:35:33 2016	PE32 executable (GUI) Intel 80386	16642528	success
<p>file name: CEAE49C5792-10.217.55.145-1453934119.880 file size: 16642528 serial: CEAE49C5792 uri: [contentType]TubeT@193.exe md5: 9ef801494d51110640d34e011c6549d header md5: 286c1c74939c0ce061e7d789c0864 sha1: d586804c5854583d38249495098705c4e000769 sha256: 4f10e72797df410d7ce4ef338923ad57652795fd427e68e1467241f0632c file type: PE32 executable (GUI) Intel 80386 view report: scanthis_report</p>							
Malicious	CEAE49C5792	10.217.55.90	10.217.55.145	Wed Jan 27 14:35:28 2016	PE32 executable (GUI) Intel 80386	2320004	success
Benign	CEAE49C5792	10.217.55.90	10.217.55.145	Wed Jan 27 14:35:27 2016	PE32 executable (GUI) Intel 80386	15217095	success
Malicious	CEAE49C5792	10.217.55.90	10.217.55.145	Wed Jan 27 14:35:24 2016	PE32 executable (GUI) Intel 80386	221184	success
Benign	CEAE49C5792	10.217.55.90	10.217.55.145	Wed Jan 27 14:35:22 2016	PE32 executable (GUI) Intel 80386	86941121	success
Malicious	CEAE49C5792	10.217.55.90	10.217.55.145	Wed Jan 27 14:35:03 2016	PE32 executable (GUI) Intel 80386	5012999	success
Malicious	CEAE49C5792	10.217.55.90	10.217.55.145	Wed Jan 27 14:34:46 2016	PE32 executable (GUI) Intel 80386	112275472	success
Malicious	CEAE49C5792	10.217.55.90	10.217.55.145	Wed Jan 27 14:34:25 2016	PE32 executable (GUI) Intel 80386	112275208	success
Benign	CEAE49C5792	10.217.55.90	10.217.55.145	Wed Jan 27 14:33:45 2016	PE32 executable (GUI) Intel 80386	103040	success
Malicious	CEAE49C5792	10.217.55.90	10.217.55.145	Wed Jan 27 14:33:40 2016	PE32 executable (GUI) Intel 80386	24576	success
Benign	CEAE49C5792	10.217.55.90	10.217.55.145	Wed Jan 27 14:33:40 2016	PE32 executable (GUI) Intel 80386	990594	success
Benign	CEAE49C5792	10.217.55.90	10.217.55.145	Wed Jan 27 14:33:39 2016	PE32 executable (GUI) Intel 80386	1210216	success
Benign	CEAE49C5792	10.217.55.90	10.217.55.145	Wed Jan 27 14:33:39 2016	PE32 executable (GUI) Intel 80386	6295329	success
Benign	CEAE49C5792	10.217.55.90	10.217.55.145	Wed Jan 27 14:33:38 2016	PE32 executable (GUI) Intel 80386	37999376	success
Malicious	CEAE49C5792	10.217.55.90	10.217.55.145	Wed Jan 27 14:33:36 2016	PE32 executable (GUI) Intel 80386	5004448	success
Benign	CEAE49C5792	10.217.55.90	10.217.55.145	Wed Jan 27 14:33:29 2016	PE32 executable (GUI) x86-64	1964912	success
Benign	CEAE49C5792	10.217.55.90	10.217.55.145	Wed Jan 27 14:33:29 2016	PE32 executable (GUI) Intel 80386	36618240	success
Benign	CEAE49C5792	10.217.55.90	10.217.55.145	Wed Jan 27 14:33:22 2016	PE32 executable (GUI) Intel 80386	7616878	success

Um die Problemhebung zu erleichtern, steht ebenfalls ein detaillierter Bericht zu den analysierten Dateien zur Verfügung.

SonicWall, Inc.

5455 Great America Parkway | Santa Clara, CA 95054
Weitere Informationen erhalten Sie auf unserer Website.
www.sonicwall.com

© 2016 SonicWall Inc. ALLE RECHTE VORBEHALTEN. SonicWall ist eine Marke oder eingetragene Marke von SonicWall Inc. und/oder deren Tochtergesellschaften in den USA und/oder anderen Ländern. Alle anderen Marken und eingetragenen Marken sind Eigentum der jeweiligen Inhaber.
Datasheet-AdvancedThreatProtection-US-K-J-24691

