SonicWall Capture Advanced Threat Protection Service

Wie Sie Zero-Day-Angriffe und andere unbekannte Bedrohungen identifizieren und abwehren

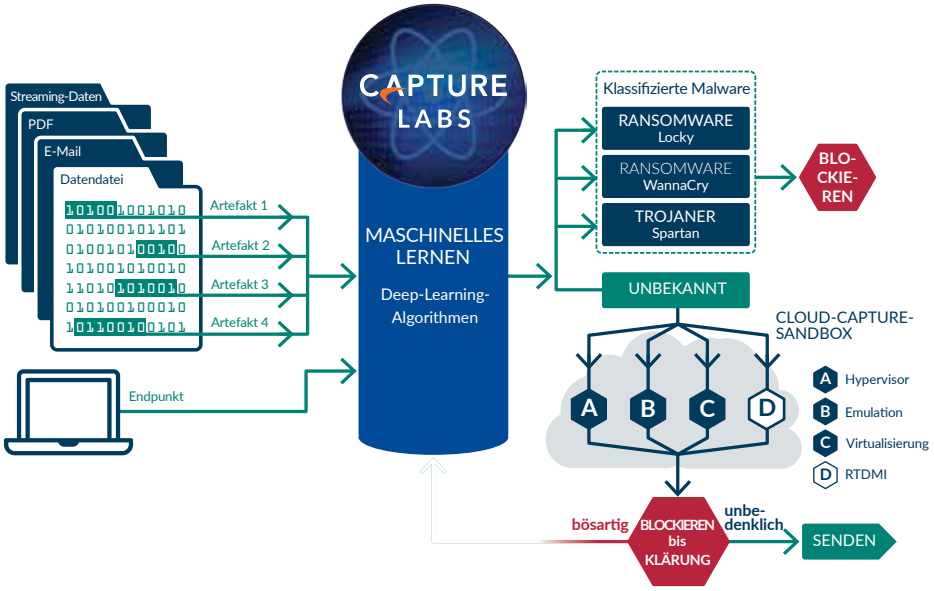
Für einen effektiven Schutz vor Zero-Day-Bedrohungen benötigen Unternehmen Lösungen mit Malware-Analysetechnologien, die auch in Zukunft raffinierte, schwer zu fassende Bedrohungen und Malware aufspüren können.

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. Dieser Service ist die einzige Lösung zur Erkennung raffinierter Bedrohungen, die mehrschichtiges Sandboxing, umfassende Systemsimulation, Virtualisierungstechniken und die Real-Time Deep Memory Inspection (RTDMI™)-Technologie von SonicWall vereint, um verdächtige Codeaktivitäten zu analysieren. 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 lässt sich ein breites Spektrum an Dateitypen unabhängig von ihrer 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
- Blockieren von Dateien am Gateway bis zur Klärung des Sicherheitsstatus
- Mehrere Engines verarbeiten Dateien parallel, um schnelle Ergebnisse zu ermöglichen
- Die RTDMI-Engine von SonicWall blockiert unbekannte Massenmalware mittels speicherbasierter Echtzeit-Prüfmethoden.



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.

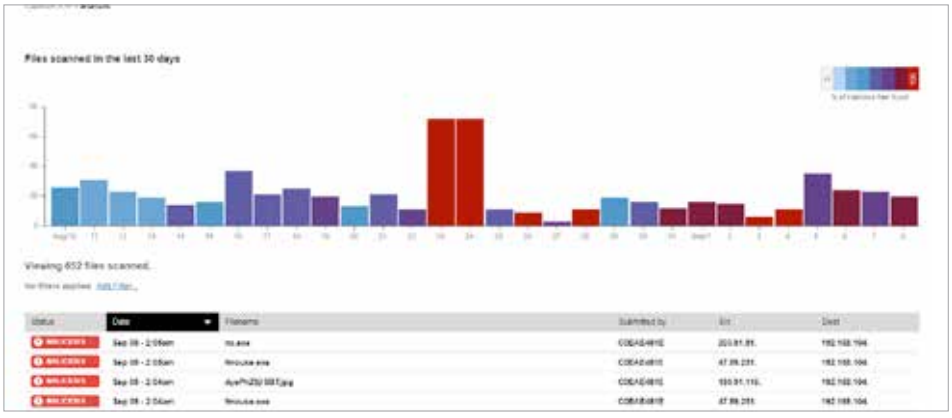
Funktionen

Erweiterte Multi-Engine-Bedrohungsanalyse: Der SonicWall Capture ATP-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 die SonicWall Capture ATP-Cloud weitergeleitet. Die Multi-Engine-Sandbox-Plattform mit RTDMI, virtualisiertem Sandboxing, umfassender Systemsimulation und einer Analysetechnologie auf Hypervisor-Ebene führt verdächtigen Code aus, analysiert dessen Verhalten und macht bösartige Aktivitäten transparent, ohne sich von Umgehungstaktiken austricksen zu lassen. So sorgt sie für einen größtmöglichen Schutz vor Zero-Day-Bedrohungen.

Real-Time Deep Memory Inspection (RTDMI): Optimiert wird der SonicWall-Multi-Engine-Service Capture ATP durch die zum Patent angemeldete Real-Time Deep Memory Inspection-Technologie. Die RTDMI-Engine ist durch eine direkte Prüfung des Speichers in der Lage, die in großer Zahl vorkommenden Zero-Day-Bedrohungen sowie unbekannte Malware proaktiv aufzudecken und abzuwehren. Aufgrund ihrer Echtzeitarchitektur arbeitet die RTDMI-Technologie von SonicWall extrem präzise und reduziert die Anzahl von Falschmeldungen auf ein Minimum. Außerdem ist sie in der Lage, ausgeklügelte Attacken zu identifizieren und abzuwehren.

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 bösartige Dateien in das Netzwerk eindringen, können die zur Analyse an den Cloud-Service gesendeten Dateien am Gateway festgesetzt werden, bis der Sicherheitsstatus geklärt ist.



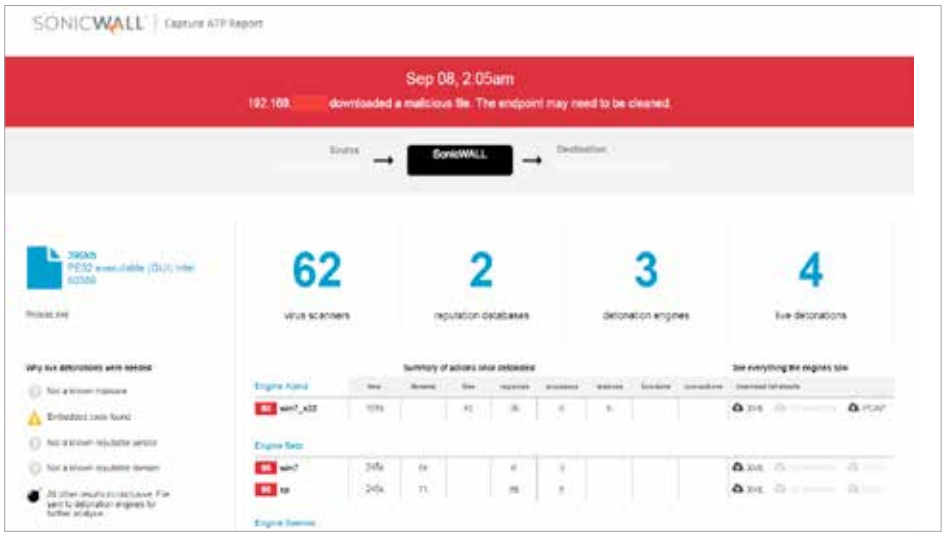
Die SonicWall Capture ATP-Reporting-Seite bietet eine Übersicht zu den Ergebnissen des jeweiligen Tages. Anhand der farbigen Balken im Bericht kann man sehen, an welchen Tagen Malware entdeckt wurde. Administratoren können einfach auf die gewünschten Tagesergebnisse klicken und Filter anwenden, um bösartige Dateien sowie die entsprechenden Ergebnisse im Handumdrehen anzuzeigen.

Schnelle Implementierung von Signaturen zur Problemlösung: Wird eine Datei als bösartig identifiziert, erhalten die mit SonicWall Capture ATP-Abos ausgestatteten Firewalls umgehend eine Signatur, um Folgeangriffe zu verhindern. Außerdem wird die Malware an das SonicWall Capture Labs Threat Research-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 ATP-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 ATP-Service gesendet werden, und teilen das Ergebnis der Dateianalyse mit.

Über uns

Seit über 27 Jahren bekämpft SonicWall Cyberkriminalität, um kleinen, mittleren und großen Unternehmen weltweit Schutz zu bieten. Mit unseren Produkten und Partnern können wir eine automatisierte Echtzeitlösung zur Erkennung und Prävention von Sicherheitslücken für die individuellen Anforderungen von mehr als 500.000 Organisationen in über 215 Ländern und Regionen bereitstellen, damit sie sich voll und ganz auf ihr Geschäft konzentrieren können.



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

UNTERSTÜTZTE PLATTFORMEN

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

NS*sp* 12800
NS*sp* 12400

NS*a* 9650
NS*a* 9450
NS*a* 9250
NS*a* 6650
NS*a* 5650
NS*a* 4650
NS*a* 3650
NS*a* 2650

TZ600 Series
TZ500 Series
TZ400 Series
TZ300 Series

NSv 1600
NSv 800
NSv 400
NSv 300
NSv 200
NSv 100
NSv 50
NSv 25
NSv 10

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, Kalifornien 95035, USA
Weitere Informationen erhalten Sie auf unserer Website.
www.sonicwall.com

DataSheet-CaptureAdvancedThreatProtection-US-VG-MKTG4093