SonicWall Capture Client

Stoppt Sicherheitsvorfälle schneller als jede andere Lösung – völlig autonom

Angesichts der ständig zunehmenden Bedrohung durch Ransomware und andere bösartige malwarebasierte Angriffe hat sich gezeigt, dass die Effektivität von Client-Sicherheitslösungen nicht ausschließlich auf der Grundlage der Endpoint-Compliance gemessen werden kann. Herkömmliche Virenschutztechnologien nutzen einen veralteten signaturbasierten Ansatz, der mit den neuen Malware- und Umgehungstechniken seit Langem überfordert ist.

Mit der zunehmenden Verbreitung von Telearbeit, Mobilitätslösungen und BYOD ist es außerdem dringend nötig, unter anderem durchgängigen Schutz, Informationen zu Anwendungsschwachstellen und Funktionen zur Durchsetzung von Webregeln für Endgeräte bereitzustellen, egal wo sich diese befinden. Genau hier kommt SonicWall Capture Client ins Spiel – eine einheitliche Endpoint-Lösung mit einer Vielzahl an EPP- und EDR-Funktionen.

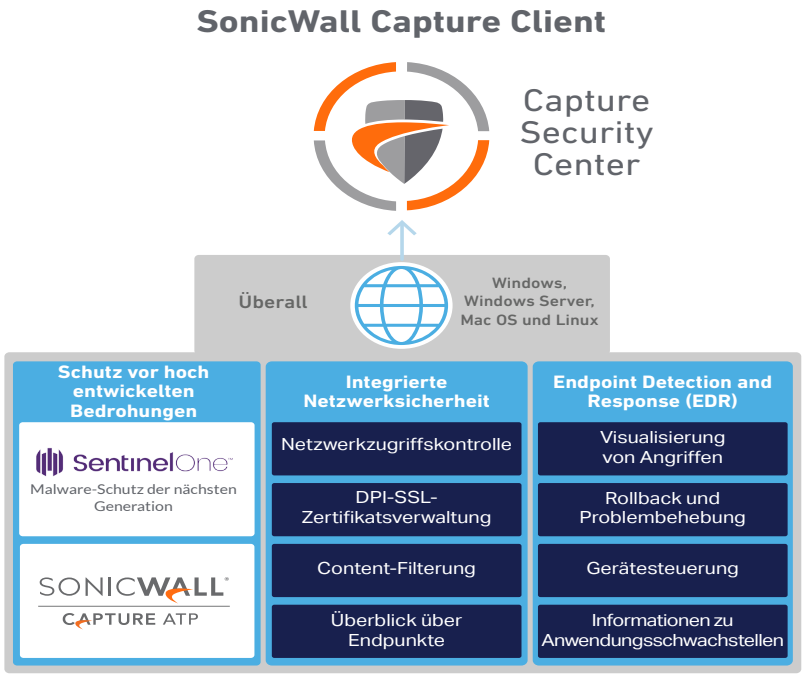
HIGHLIGHTS

- Effiziente, aussagekräftige Informationen zu erkannten Bedrohungen, wobei nur relevante Daten angezeigt werden
- Zentralisierte, cloudbasierte Verwaltung mit echter Mandantenfähigkeit zur Stärkung der Netzwerk- und Endgerätesicherheit
- Verbesserung der Sicherheit und Unterstützung von IT-Teams mit einer benutzerfreundlichen, intuitiven Lösung, die moderne Angriffe stoppt

Maßgeschneiderte Endpoint-Security für Ihre Organisation

Lesen Sie die Lösungsübersicht: sonicwall.com

DATENBLATT



Capture Client nutzt einen verhaltensbasierten Schutz vor ausgeklügelten Bedrohungen auf Basis von SentinelOne-NGAV-Funktionen.

Die Integration mit Capture ATP sorgt für einen effektiveren Schutz, kürzere Reaktionszeiten und geringere Gesamtbetriebskosten.

Funktionen und Vorteile

Kontinuierliche Verhaltensüberwachung

- Komplettes Profil der Datei-, Anwendungs-, Prozess- sowie Netzwerkaktivitäten
- Schutz vor dateibasierter und dateiloser Malware
- 360-Grad-Sicht auf Angriffe inklusive aussagekräftiger Informationen

Threat-Hunting mit Deep Visibility

- Nutzung von Deep Visibility, um nach Bedrohungen auf Basis von Verhaltensindikatoren sowie Kompromittierungsindikatoren (Indicators of Compromise, IoCs) über alle unterstützten Windows-, MacOS- und Linux-Geräte hinweg zu suchen
- Automatisierung von Threat-Hunting und Bedrohungsreaktionen mit benutzerdefinierten Regeln und Warnmeldungen

Integration von Capture Advanced Threat Protection (ATP)

- Automatisches Hochladen verdächtiger Dateien auf Windows-Geräten, um erweiterte Sandboxing-Analysen durchzuführen
- Aufspüren schlummernder Bedrohungen, bevor sie ausgeführt werden, wie z. B. Malware mit eingebauter Zeitverzögerung
- Abgleich der Capture-ATP-Datenbank, die Ergebnisse der verschiedenen Dateien enthält, ohne Dateien in die Cloud hochladen zu müssen

Einzigartige Rollback-Funktionen

- Unterstützung von Regeln, die Bedrohungen komplett beseitigen
- Autonomes Zurücksetzen von Endgeräten auf einen bekannten unbedenklichen Zustand vor der Infektion

Mehrschichtige heuristische Techniken

- Cloud-Informationen, erweiterte statische Analysen und dynamischer, verhaltensorientierter Schutz
- Schutz gegen bekannte und unbekannte Malware vor, während oder nach einem Angriff und Beseitigung der jeweiligen Bedrohung

Informationen zu Anwendungsschwachstellen

- Katalogisierung aller installierten Anwendungen und damit zusammenhängenden Risiken
- Untersuchung bekannter Schwachstellen mit Einzelheiten zu den gemeldeten CVEs und Schweregraden
- Nutzung dieser Daten, um das Patching zu priorisieren und die Angriffsfläche zu reduzieren

Netzwerkkontrollen für Endgeräte

- Hinzufügen firewallähnlicher Kontrollen zum Endgerät
- Zusätzliche Quarantäneregel für infizierte Geräte

Remote Shell[1]

- Keine Notwendigkeit mehr, die Problembehebung, Änderungen lokaler Konfigurationen und forensische Untersuchungen physisch vor Ort durchzuführen

Keine Notwendigkeit mehr, regelmäßige Prüfungen oder Updates durchzuführen

- Hohes Schutzniveau, ohne die Benutzerproduktivität zu beeinträchtigen
- Vollständiger Scan bei der Installation mit anschließender kontinuierlicher Überwachung des Systems auf verdächtige Aktivitäten

Optionale Integration mit den SonicWall-Firewalls

- Prüfung von verschlüsseltem Verkehr mittels Deep Packet Inspection (DPI-SSL) auf Endgeräten
- Einfache Implementierung vertrauenswürdiger Zertifikate auf jedem Endgerät
- Weiterleitung ungeschützter Nutzer zu einer Capture-Client-Downloadseite, bevor sie hinter einer Firewall auf das Internet zugreifen können

Content-Filterung

- Blockieren bösartiger Sites, IP-Adressen und Domains
- Erhöhung der Benutzerproduktivität durch Drosselung der Bandbreite oder Blockieren des Zugriffs auf anstößige oder unproduktive Webinhalte

Gerätesteuerung

- Potenziell infizierte Geräte werden daran gehindert, eine Verbindung zu Endgeräten aufzubauen
- Granulare Regeln für Freigabelisten

Capture Client – Features

Feature	Advanced	Premier
Cloud-Management, -Reporting und -Analytics (CSC)	✓	✓
Netzwerksicherheitsintegrationen		
Einblick in Endgeräte und Durchsetzung von Richtlinien	✓	✓
Implementierung von DPI-SSL-Zertifikaten	✓	✓
Content-Filterung	✓	✓
Erweiterter Endpunktschutz		
Malware-Schutz der nächsten Generation	✓	✓
Capture Advanced Threat Protection-Sandboxing	✓	✓
ActiveEDR (Endpoint Detection and Response – Erkennung von Bedrohungen auf Endgeräten und Einleitung angemessener Reaktionen)		
Visualisierung von Angriffen	✓	✓
Rollback und Problembehebung	✓	✓
Gerätesteuerung	✓	✓
Anwendungsschwachstellen und Application-Intelligence	✓	✓
Erkennung unberechtigter Endgeräte		✓
Netzwerkkontrollen für Endgeräte		✓
ActiveEDR – Threat-Hunting und Bedrohungsinformationen		
Threat-Hunting mit Deep Visibility		✓
Remote Shell[1]		✓
Ausschlussliste		✓

[1] Remote Shell wird on demand in einem neuen Account (mit aktivierter 2FA) direkt auf der S1-Konsole bereitgestellt.

Capture Client – Systemanforderungen | SonicWall

Best Practices rund um globale Endpoint-Security-Prozesse für MSSPs und dezentrale Unternehmen

Lesen Sie die Lösungsübersicht: www.sonicwall.com

Über SonicWall

SonicWall bietet grenzenlose Cybersicherheit für eine extrem dezentrale Arbeitswelt, in der jeder remote, mobil und potenziell gefährdet ist. Durch die Identifizierung unbekannter Bedrohungen, moderne Echtzeit-Überwachungsfunktionen und eine herausragende Wirtschaftlichkeit hilft SonicWall großen Unternehmen, Behörden und KMUs weltweit, die Cybersicherheitslücke zu schließen. Weitere Informationen erhalten Sie unter www.sonicwall.de.

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

Datasheet-CaptureClient-A4-JK-6217