LÖSUNGSPROFIL: EINE EINHEITLICHE CLIENT-PLATTFORM FÜR ENDPUNKTSICHERHEIT AUF ENTERPRISE-EBENE

SonicWall Capture Client bietet erweiterte Funktionen wie verhaltensbasierten Anti-Malware-Schutz, Sandboxing, Rollback und Informationen über Anwendungsschwachstellen

Zusammenfassung

Mehr Telearbeit, Mobilität und die Nutzung eigener Geräte am Arbeitsplatz (BYOD, Bring Your Own Device) führen zu einem vermehrten Auftreten von Schadsoftware und Umgehungsversuchen, weshalb der kontinuierliche Schutz aller Endpunkte dringender denn je ist. Eine wirksame Lösung, wie SonicWall Capture Client, muss mindestens Folgendes bieten:

- Erweiterten verhaltensbasierten Malware-Schutz
- Sandboxing von Dateien in der Cloud
- Content-Filtering
- Unterstützung für die Visualisierung von verschlüsseltem Verkehr
- Informationen über Anwendungsschwachstellen
- Gerätekontrolle

Einführung

Management und Sicherheit von Endpunkten sind im heutigen Geschäftsklima unabdingbar. Wenn sich Endbenutzer mit ihren Geräten innerhalb und außerhalb des Netzwerks bewegen und verschlüsselte Bedrohungen ungehindert Endpunkte erreichen können, muss etwas zum Schutz dieser Geräte getan werden. Angesichts der Zunahme von Ransomware und dem fortgesetzten Diebstahl von Benutzerdaten sind Endpunkte zu den Schlachtfeldern in der heutigen Bedrohungslandschaft geworden.

Problem: Der Kampf um Endpunktsicherheit

Mehr Mobilität und BYOD erschweren den Administratoren oft die Aufrechterhaltung von Transparenz und Wahrung ihrer Sicherheitshaltung. Auch die konstante Sicherstellung der Client-Sicherheit und der Erhalt von benutzerfreundlichen und umsetzbaren Informationen und Berichten können zur Herausforderung werden.

Produkte für die Endpunktsicherheit gibt es seit Jahren, aber Administratoren haben immer noch Probleme damit:

- Sicherheitsprodukte auf dem aktuellen Stand zu halten
- Richtlinien und Compliance durchzusetzen
- Berichte einzuholen
- Verschlüsselte, gerätebasierte und dateilose Angriffe abzuwehren
- Warnhinweise und Schritte zur Wiederherstellung zu verstehen
- Ihre Lizenzen zu verwalten
- Bedrohungen wie Ransomware zu stoppen
- Webnutzung abseits von der Firewall zu kontrollieren
- Zu wissen, welche Anwendungen auf Geräten installiert sind und welche davon Schwachstellen aufweisen

SonicWall Capture Client ist eine einheitliche Endpunkt-Plattform für die Bedrohungslandschaft von heute.

Lösung: Eine einheitliche Client-Plattform für Endpunkt-Sicherheit, die allen Unternehmen gerecht wird

Zur Lösung dieser anhaltenden Probleme brauchen Administratoren (selbst in den kleinsten Organisationen) eine einheitliche Client-Plattform. Diese Plattform muss Endpunktsicherheit bieten, die den Anforderungen von Unternehmen genügt, einschließlich verhaltensbasiertem Virenschutz, Content-Filtering, Sandboxing, Informationen über Anwendungsschwachstellen und die Visualisierung von verschlüsseltem Verkehr muss unterstützt werden. Bei der Integration mit einer Firewall sollte eine optimale Lösung die Vorteile einer mehrere Schichten umfassenden Schutztechnik, vollständige Berichterstattung und Durchsetzung des Endpunktschutzes bieten.

SonicWall Capture Client

SonicWall Capture Client liefert diese umfassende Endpunktlösung. Capture Client ist eine einheitliche Client-Plattform mit mehreren Schutzfunktionen für Endpunkte, darunter Schutz vor Schadsoftware der nächsten Generation und Unterstützung für die Visualisierung von verschlüsseltem Verkehr. Die Lösung prüft Dateien in einer Cloud-Sandbox, schützt vor Bedrohungen aus dem Netz, bietet Gerätekontrolle und setzt Schutz für Endpunkte durch. Darüber hinaus bietet sie fortlaufende Gewährleistung der Client-Sicherheit mit benutzerfreundlichen und umsetzbaren Informationen und Berichten, z. B. über installierte Anwendungen, die Schwachstellen darstellen.

Die SonicWall Lösung gibt es in zwei Ausführungen: SonicWall Capture Client Basic bietet die neuesten Funktionen zum Schutz gegen Schadsoftware und zur Wiederherstellung sowie DPI-SSL-Support. SonicWall Capture Client Advanced bietet alle oben aufgeführten Funktionsmerkmale der Basic-Funktion plus erweiterte Rollback-Fähigkeiten, Capture ATP-Integration, Content-Filtering, Angriffsvisualisierung, Gerätekontrolle und Informationen über Anwendungsschwachstellen.

Mit der Integration der SonicWall Capture Advanced Threat Protection (ATP) können verdächtige Dateien, die Capture Client als moderate Bedrohung einstuft (die aber noch unter dem Grenzwert für Warnhinweise liegen), automatisch zur Analyse hochgeladen werden. Mit der Integration der Urteils-Datenbank von Capture ATP können Administratoren bekannte Urteile zu verdächtigen Dateien an Endpunkten und Servern abfragen, die von Capture Client Advanced geschützt werden. Darüber hinaus können Administratoren ihre eigenen Anwendungen auf eine Whitelist setzen und damit falsche Positivmeldungen verhindern.

Für Administratoren ist die Durchsetzung von Web-Nutzungsrichtlinien schwierig, wenn Mitarbeiter außerhalb des Netzwerkperimeters arbeiten. Mittels Content-Filtering können Unternehmen Nutzungsrichtlinien festsetzen, die Bandbreitennutzung regeln und sogar den Zugriff auf bekannte bösartige URLs, IP-Adressen und Domänen blockieren.

Unter Nutzung der SentinelOne Engine liefert Capture Client erweiterten Schutz vor Bedrohungen mit kontinuierlicher Überwachung von Verhaltensmustern, Machine Learning und Windows System Rollback (nur in der Advanced-Version). In Kombination mit SonicWall Firewalls ermöglicht Capture Client mittels Verwaltung vertrauenswürdiger SSL-Zertifikate, die zur Deep Packet Inspection von SSL/TLS-Verkehr herangezogen werden, die Sicht auf verschlüsselten Verkehr.

Capture Client kann darüber hinaus nicht nur Malware, die in böser Absicht über den Netzwerkverkehr eingeschleust wird, sondern auch mit dem Endpunkt verbundene infizierte Geräte und Speichermedien erkennen. Des Weiteren können Administratoren mithilfe von Device Control granulare Regeln erstellen und somit unbekannte Geräte daran hindern, Verbindungen zu Endpunkten herzustellen und diese dann zu infizieren; damit lässt sich die Angriffsfläche mit minimalem Aufwand eingrenzen.

Für Administratoren ist es oft schwierig, zu bestimmen, welche Anwendungen auf den Endpunkten installiert sind und ob diese bekannte Schwachstellen enthalten. Die durch Capture Client bereitgestellten Informationen über Anwendungsschwachstellen geben Administratoren einen Katalog aller installierten Anwendungen mit einer Liste aller darin enthaltenen bekannten Schwachstellen.

Capture Client bietet optional auch integrierte Bedrohungsschutzfähigkeiten, die über SonicWall Firewalls bereitgestellt werden und für die Durchsetzung von Client-Schutzrichtlinien und die grundlegende Sicherheitshaltung sorgen. Die Cloud-basierte Managementkonsole von Capture Client bietet komplette Integration mit den Firewalls der nächsten Generation von SonicWall.

Capture Client Advanced ist in die SonicWall Capture Advanced Threat Protection (ATP) integriert und profitiert damit von der Möglichkeit, Dateien zu manipulieren und zu testen, die von Endpunkten und Servern in der Regel nicht untersucht werden können. Darüber hinaus können Administratoren Urteile über verdächtige Dateien auf der Grundlage des Hash-Codes abfragen, ohne dass die Dateien auf Endpunkte und Server geladen werden müssen. Administratoren können falsche Positivmeldungen reduzieren, indem sie bekannte gute Anwendungen, die auf Endpunkten und Servern laufen, auf eine Whitelist setzen. Capture Client Advanced bietet auch Content-Filtering, um Endbenutzer vor den über das Internet eingeschleusten Malware-Bedrohungen zu schützen und Web-Nutzungsrichtlinien auch außerhalb des Netzwerkperimeters durchzusetzen.

Administratoren von Capture Client können jetzt mit einem Cleaner-Tool unvollständige oder korrumptierte Installationen ersetzen. Organisationen haben die Kontrolle darüber, welche Version der Software sie einsetzen, was das Austesten vor ihrem allgemeinen Einsatz erleichtert.

Durch Integration mit dem Capture Security Center bietet Capture Client die Möglichkeit, den Sicherheitsbetrieb ganz einfach von einer zentralen SPOG-Benutzerfläche aus zu steuern; gleichzeitig bleibt die Flexibilität zum Einsatz von rollenbasierter Zugangskontrolle gewahrt, damit Nutzern Zugangsprivilegien auf Basis ihrer Arbeitsfunktionen erteilt werden können.

Mehr über Capture Client erfahren Sie auf Sonicwall.com/endpoint.

Über SonicWall

SonicWall bietet Boundless Cybersecurity für das hyperverteilte Umfeld einer neuen Arbeitsrealität, in der jeder remote, mobil und ungeschützt ist. SonicWall schützt Organisationen bei der Mobilisierung für die neue Geschäftsnormalität mit nahtlosem Schutz, der die raffiniertesten Cyberangriffe an den durch eine zunehmend grenzenlose Remote-, Mobil- und Cloud-fähige Belegschaft entstehenden Schwachstellen stoppt. Indem SonicWall das Unbekannte kennt, Echtzeit-Transparenz und skalierbare Ökonomien ermöglicht, werden Cybersicherheitslücken bei Unternehmen, Regierungen und KMU weltweit geschlossen. Weitere Informationen finden Sie auf www.sonicwall.com oder folgen Sie uns auf Twitter, LinkedIn, Facebook und Instagram.

Bei Fragen zu Ihrer möglichen Verwendung dieses Materials setzen Sie sich bitte mit uns in Verbindung:

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, CA 95035 USA

Weitere Informationen erhalten Sie auf unserer Website.
www.sonicwall.com