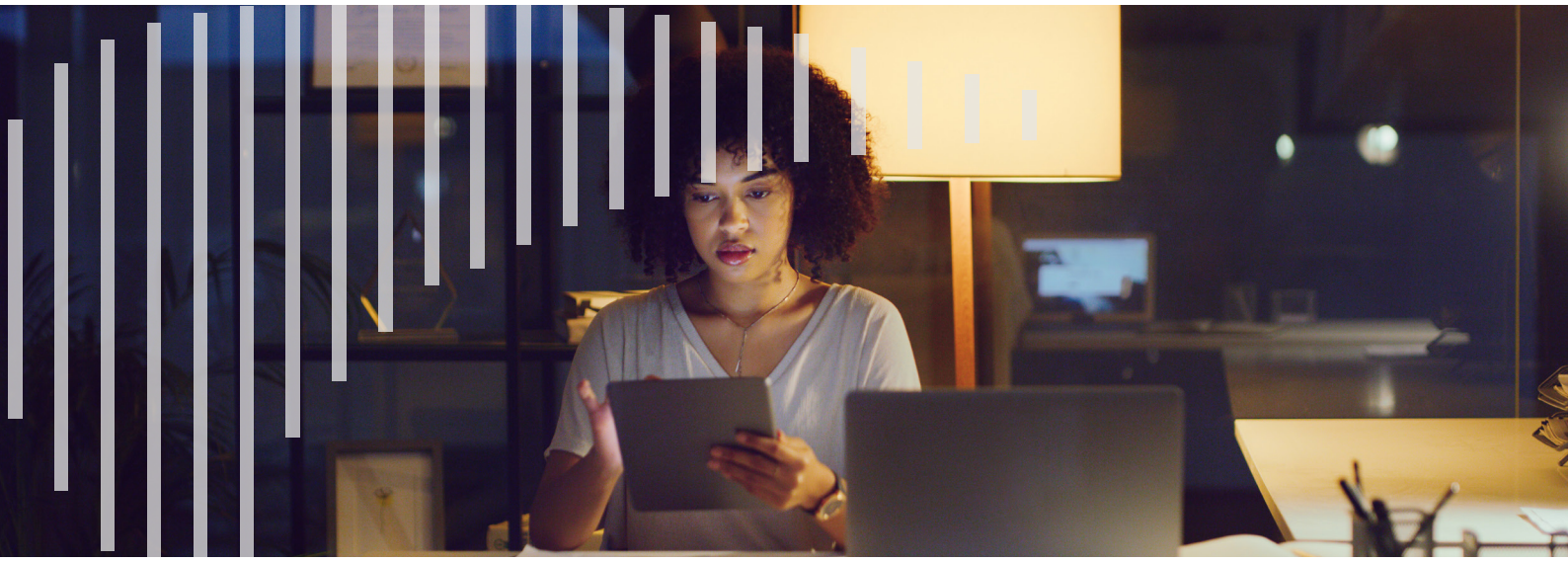

KURZDARSTELLUNG

Worauf Administratoren vor Kauf einer Endpoint-Security-Lösung achten sollten

Eine neue Sicht auf die Herausforderungen der Endpoint-Security

Zusammenfassung

Das Thema Endpoint-Security bereitet vielen Administratoren Kopfzerbrechen. Diese Kurzdarstellung befasst sich mit den häufigsten Herausforderungen, wie zum Beispiel:

- Wartung und Umsetzung der Sicherheitslösung
- verschlüsselte und ausgeklügelte Bedrohungen
- Verwaltung von Warnmeldungen und Problembehebung
- Erstellung und Pflege von Richtlinien
- transparenter Einblick in den Sicherheitsstatus von Mandanten
- ungepatchte Sicherheitslücken

In einer Welt, in der Cyberkriminelle ihre Angriffe ständig weiterentwickeln, spielt die Verwaltung und Sicherheit von Endpunkten eine wichtige Rolle. Heutige Benutzer checken ständig mit ihren Endpunktgeräten in das Netzwerk ein und aus. Doch genau diese Endpunkte stehen im Mittelpunkt modernster und extrem raffinierter Cyberbedrohungen. Immer mehr verschlüsselte Bedrohungen erreichen Endpunkte ungeprüft, Ransomware befindet sich auf dem Vormarsch und auch Anmeldedaten sind ständig von Diebstahl betroffen. Die zunehmende Bedrohung durch Ransomware und andere bösartige Malware-basierte Angriffe zeigt, dass die Effektivität von Client-Sicherheitslösungen nicht ausschließlich auf der Grundlage der Endpoint-Compliance gemessen werden darf.

Noch schwieriger wird es, wenn mehrere Mandanten – innerhalb einer einzigen Organisation oder für mehrere Kunden – im Spiel sind. Dann sind oft unterschiedliche Richtlinien und Konfigurationen je nach Benutzergruppe, Gerät und Standort nötig.

Die Herausforderungen rund um den Endpunktschutz

Obwohl es bereits seit Jahren Produkte für die Endpoint-Security gibt, tun sich Administratoren immer noch in folgenden Bereichen schwer:

- Sicherheitsprodukte auf dem neuesten Stand halten
- Durchsetzung von Regeln und Web-Compliance-Vorgaben
- Zugriffsverwaltung und Erstellung von Berichten
- Identifizierung von Bedrohungen, die durch verschlüsselte Kanäle übermittelt werden
- Warnmeldungen und Problembehebung
- Verwaltung von Lizenzen
- Abwehr hoch entwickelter Bedrohungen wie Ransomware
- Unkenntnis darüber, wo kritische Schwachstellen liegen
- Einblick in den Sicherheitsstatus von Mandanten und Einhaltung unternehmensweiter Richtlinien

Sicherheitsprodukte auf dem neuesten Stand halten

Administratoren müssen sicherstellen, dass auf verwalteten Endpunkten die korrekte Version der Sicherheitssoftware gemäß den Compliance-Vorgaben läuft.

Netzwerkadministratoren benötigen verwaltete Endpunkte, um ihr Sicherheitskonzept kontinuierlich prüfen und regelmäßig über den aktuellen Status berichten zu können. Nur so lassen sich neue Bedrohungen effektiv abwehren.

In manchen Fällen müssen Administratoren den Ost-West-Traffic in ihren Rechenzentren stoppen, der oft einen Großteil des Datenverkehrs ausmacht. Geräte, die infiziert oder nicht regelkonform sind, sollten sie lokal unter Quarantäne stellen

können. In solchen Situationen muss die Firewall den Zugang zum Internet und die Verbindung zum LAN blockieren, um so die Netzwerkpfade zu den von der Firewall unter Quarantäne gestellten Orten einzuschränken.

Zur Gewährleistung der Datenintegrität müssen Sicherheitsadministratoren außerdem dafür sorgen, dass die Daten zwischen dem Unified Client und der zentralisierten Verwaltungskonsole während der Übertragung nicht manipuliert werden können.

Durchsetzung von Regeln und Web-Compliance-Vorgaben

Sind die Endpunkte nicht richtlinienkonform, müssen Administratoren verhindern können, dass die Endpunktgeräte UTM-Services nutzen, um Datenverkehr durch die Firewall zu übertragen. Auch Endbenutzer spielen eine wichtige Rolle bei der Endpoint-Security. Da sie für ihre Arbeit häufig Firmenlaptops und andere Endpunkte verwenden, sollten sie umgehend informiert werden, wenn bösartige Software oder ungewöhnliches Verhalten identifiziert werden. Auf diese Weise können sie bei Bedarf entsprechende Maßnahmen treffen oder ein Ticket erstellen.

Um die Webnutzungsrichtlinien Ihrer Organisation auch außerhalb des Büros durchzusetzen (etwa wenn Ihre Mitarbeiter im Homeoffice sind), können Sie Web- oder Content-Filter in Ihre Sicherheitslösung einbetten. Bekannte bösartige Websites sollten Sie unbedingt blockieren und auch produktivitätsmindernde und nicht jugendfreie Seiten sollten besser gesperrt werden. Wenn User Videodaten über lokale Server per VPN beziehen, wäre es außerdem eine Überlegung wert, die Bandbreite für datenintensive Websites zu drosseln.

Zugriffsverwaltung und Erstellung von Berichten

Es kann vorkommen, dass Administratoren für mehrere Firewalls zuständig sind, deren Benutzer aber in einem einzigen Pool konfiguriert sind. Um Client-Regeln zu verwalten, ist es wichtig, dass sie von Firewall-Administratoren oder über Sicherheitsmanagementkonsolen einen Single-Sign-on(SSO)-Zugriff erhalten. Gleichzeitig verlangt die Compliance oft, dass sich alle administrativen Rollen am Least-Privilege-Prinzip orientieren. Somit sollte das Unified-Client-Management eine ausreichende rollenbasierte Zugriffskontrolle für einen privilegierten Zugriff haben. Diese könnte sich beispielsweise auf zwei Rollen beschränken: eine mit Read-/Write-Zugriff und eine andere mit Read-only-Zugriff.

Bedrohungen über verschlüsselte Kanäle

Bedenkt man, dass heute immer mehr Webanwendungen über verschlüsselte Kanäle wie HTTPS geschützt werden und auch Malware Verschlüsselungstechnologien nutzt, um eine netzwerkbasierte Prüfung zu umgehen, ist eine Prüfung des SSL-/TLS-Verkehrs mittels Deep Packet Inspection (DPI-SSL) unbedingt notwendig. Möchte man allerdings Probleme mit der Benutzererfahrung und der Sicherheit vermeiden, ist ein massiver Einsatz vertrauenswürdiger SSL-/TLS-Zertifikate für alle Endpunkte in den meisten Fällen unumgänglich. Dies erfordert einen Mechanismus für die Distribution und Verwaltung von Zertifikaten sowie für die Kriterien, anhand derer der Browser diese Zertifikate als vertrauenswürdig einstuft.

Warnmeldungen und Problembehebung

Endbenutzer kennen sich mit Sicherheitsrisiken in der Regel weniger gut aus als Sicherheitsexperten. Daher ist es wichtig, dass ihre Endpoint-Security-Plattform sie auf ein verändertes Risikoprofil hinweist – zum Beispiel wenn sie mit ihrem Laptop verreisen – und Sicherheitstipps gibt.

Um die Einhaltung unternehmensspezifischer Regeln zu vereinfachen, kann es sowohl für Endbenutzer als auch für die IT hilfreich sein, wenn Endbenutzer darüber informiert werden, wie sie Probleme selbst beheben können. Wenn das Gerät eines Benutzers nicht regelkonform ist und unter Quarantäne gestellt wird, benötigt der User auch Unterstützung und Informationen darüber, wie er die Compliance wiederherstellen kann.

Lizenzverwaltung

Administratoren müssen sicherstellen, dass ihre Endpoint-Security-Lösungen automatisch aktualisiert und an ihre Verwaltungsschnittstelle angepasst werden, sodass eine korrekte Lizenzierung der Endpunkte gewährleistet ist. Beispielsweise sollten sämtliche Lizenzdaten für einen Kunden zentral überwacht und gespeichert werden. Beim Erwerb einer neuen Lizenz sollte die zentralisierte Unified-Client-Management-Lösung einen Hinweis erhalten, um den Berechtigungsprozess für die Software zu starten.

Manche Administratoren müssen außerdem regelmäßig Compliance-Berichte für alle implementierten Drittanbieterlizenzen erstellen, um ihre Partner zu bezahlen.

Abwehr hoch entwickelter Bedrohungen wie Ransomware

Mit traditionellen Lösungen ist es nicht immer möglich, alle administrativen Anforderungen zu lösen. Der veraltete signaturbasierte Ansatz herkömmlicher Antivirentechnologien ist angesichts der schnellen Entwicklungszyklen neuer Malware sowie der immer raffinierteren Umgehungsmethoden keine Lösung mehr. Für einen effektiven Endpunktschutz sind deshalb neue Strategien gefragt, die nicht nur auf hoch entwickelte Engines zur Bedrohungserkennung setzen, sondern auch einen mehrschichtigen Schutz auf Endpunkten unterstützen, zum Beispiel durch die Integration einer Sandbox-Umgebung.

Ein großes Problem aktueller Insellösungen (bekannt als Enforced AV-Clients) besteht darin, dass sie speziell für einen bestimmten Drittanbieter entwickelt und in die Produkte dieses Drittanbieters integriert wurden. Administratoren benötigen ein offeneres Modell, das eine relativ schnelle Implementierung zusätzlicher Sicherheitsmodule erlaubt, wenn dies aus Sicht des Unternehmens oder der Industrie erforderlich ist.

Unkenntnis darüber, wo kritische Schwachstellen liegen

Mit der zunehmenden Verbreitung von Geschäftsanwendungen ist die Bedrohung durch Anwendungsschwachstellen exponentiell gestiegen. Allein im Jahr 2019 gab es viele Schwachstellen mit einem kritischen CVSS-Score von 9,0 und mehr – ein Umstand, der nicht nur IT-Administratoren Kopfzerbrechen bereitete, sondern vor allem auch zu Sicherheitsverletzungen führte. Viele Unternehmen haben immer noch keine Möglichkeit, die Anzahl von Schwachstellen zu ermitteln bzw. diese zu klassifizieren. Daher können sie nicht ohne Weiteres einen Plan erstellen, um riskante Anwendungen zu patchen oder zu deinstallieren.

Einblick in den Sicherheitsstatus von Mandanten und Einhaltung unternehmensweiter Richtlinien

Zahlreiche große Organisationen müssen eine Vielzahl von Endpunkten und/oder die Endpoint-Security über mehrere Regionen, Benutzergruppen oder Gerätetypen hinweg verwalten. Ob sie dabei erfolgreich sind, hängt davon ab, wie schnell sie neue Mandanten erstellen können und ob sie über ein globales Dashboard mit einem umfassenden Einblick in den Sicherheitsstatus von Mandanten verfügen. In solchen Fällen benötigen Administratoren eine schnelle Lösung, um eine globale Richtlinie anzupassen, die sowohl auf einzelne Mandanten als auch auf Gruppen ausgerichtet ist. MSSPs und MSPs brauchen außerdem den nötigen Spielraum, um benutzerdefinierte Richtlinien für Mandanten zu erstellen, die von Änderungen der globalen Richtlinie nicht betroffen sind. Sie sollten über umfassende Statistiken zu Infektionen und Schwachstellen verfügen, ohne dass ein Drill-down auf jeden einzelnen Mandanten nötig ist.

Fazit

Immer häufiger werden Endpunkte als Angriffsvektor genutzt. Sicherheitsexperten sind daher gezwungen, Maßnahmen zu ergreifen, um ihre Endpunktgeräte besser zu schützen. Mit der zunehmenden Verbreitung der Telearbeit ist es außerdem extrem wichtig, sämtliche Clients unabhängig von ihrem Standort konsequent zu schützen.

Sicherheitsadministratoren müssen bei der Evaluierung von Endpunktlösungen stets die praxisrelevanten Anforderungen im Auge behalten.

Erfahren Sie mehr dazu: Lesen Sie unsere Lösungsübersicht Maßgeschneiderte Endpoint-Security für Ihre Organisation oder besuchen Sie uns unter www.sonicwall.com/de-de/products/firewalls/security-services/capture-client/.

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 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

SONICWALL®

ExecBrief-WhatAdminNeed-A4-VG-3575