SONICWALL

LÖSUNGSÜBERSICHT: EIN EINHEITLICHER ANSATZ FÜR DAS GOVERNANCE-, RISIKO- UND COMPLIANCE-MANAGEMENT

Netzwerksicherheit global verwalten

Zusammenfassung

Ein vernetzter Sicherheitsansatz für wichtige Bereiche wie Koordination, Kontrolle, Analyse und Reporting garantiert nicht nur einen soliden Präventivschutz, sondern bildet auch die Grundlage für eine einheitliche Governance-, Compliance- und Risikomanagementstrategie.

Einfacher, präziser, sicherer

Ein schlankes Sicherheitsmanagement verbessert die Koordination und die Entscheidungsfindung bei allen Fragen rund um die Sicherheit. Dafür muss der tägliche Betrieb von allen störenden und manuellen Routineaufgaben befreit werden.

Eine derartige Vereinfachung lässt sich am Besten mithilfe einer Smart-Management-Software erreichen. Diese sollte einen strukturierten Ansatz und einen systematischen Workflow bieten, um die manuellen Eingriffe bei der Verwaltung der Sicherheitsumgebung zu reduzieren. Anstatt auf Systemprobleme oder nicht autorisierte Änderungen von Firewall-Regeln nur zu reagieren, muss eine intelligente Software diese Arten von Sicherheitsrisiken automatisch erkennen, melden und zu deren schnellen Beseitigung beitragen.

Hinzu kommt, dass Unternehmen, die keinen wirklich umfassenden Überblick über ihre Sicherheitsinfrastruktur haben, dem vermeidbaren Risiko von Cyberbedrohungen und Compliance-Verstößen ausgesetzt sind. Eine moderne Managementplattform bietet Organisationen jeder Größenordnung, wie z. B. dezentral organisierten Unternehmen und Serviceprovidern, detaillierte Einblicke, um fundierte Sicherheitsentscheidungen zu treffen. Außerdem können Sicherheitsteams schneller handeln, zusammenarbeiten und kommunizieren und ihr Wissen in einem gemeinsamen Sicherheitsframework austauschen.

Integriertes, sicheres und erweiterungsfähiges Management

Eine optimale Lösung sollte eine integrierte, sichere und erweiterungsfähige cloudbasierte Architektur zur Verwaltung des gesamten Sicherheitsportfolios nutzen, um die nötige Vereinfachung und Vereinheitlichung sicher zu stellen. Mit dieser einheitlichen Cloud-Plattform wären Sicherheitsteams in der Lage, die Verwal-

tung aller Sicherheitsappliances und die operativen Aspekte der Sicherheitsinfrastruktur zusammenzufassen: zentralisierte Richtlinienverwaltung und -durchsetzung, Echtzeit-Ereignisüberwachung, Benutzeraktivitäten, Anwendungssteuerung, Datennutzung, Drill-Down-Daten und Flow Analytics sowie Forensik, Compliance- und Audit-Reporting und vieles mehr. Mithilfe einer Funktion zur Workflow-Automatisierung könnten Unternehmen zudem alle Änderungen an Ihren Firewalls effektiv verwalten.

Governance-, Compliance- und Risikomanagement

Ein umfassender Ansatz bildet die Grundlage für eine einheitliche Security-Governance-, Compliance- und Risikomanagementstrategie. Um alle operativen Aspekte des Netzwerksicherheitsökosystems abzudecken, sollte die Sicherheitskoordination ganzheitlich und vernetzt erfolgen. Die richtige Lösung sollte in der Lage sein, diverse Aufgaben zu vereinfachen und automatisieren, um die Komplexität, den Zeitaufwand und die Kosten für Sicherheitsprozesse und deren Administration zu reduzieren. Beispiele für solche Aufgaben sind:

- Bereitstellung von Sicherheits- und Netzwerkfunktionen
- Richtliniendurchsetzung
- Patching
- Geräteermittlung
- Bestandsverwaltung
- Konfiguration und Diagnose
- Überwachung
- Reporting
- Analyse
- Auditing
- Erfassung von Sicherheitsstatistiken

Workflow-Automatisierung

Der Workflow-Prozess sorgt mithilfe strenger Prüf- und Durchsetzungsverfahren vor der Implementierung für die Richtigkeit und Konformität von Richtlinienänderungen. Freigabegruppen sollten flexibel sein und den Unternehmensrichtlinien für Mitarbeitersicherheit entsprechen. Auf diese Weise lassen sich Risiken und Fehler reduzieren und gleichzeitig eine hohe Effizienz sowie die Wirksamkeit der Sicherheitsmaßnahmen gewährleisten. Eine effiziente Workflow-Automatisierung mit Funktionen zum Auditing von Richtlinienänderungen gibt Sicherheitsteams die nötige Sicherheit, um die richtigen Firewall-Regeln flexibel, zur richtigen Zeit und entsprechend den Compliance-Vorgaben zu implementieren.

Vollautomatische Bereitstellung

Die ideale Lösung ist cloudbasiert und vereinfacht und beschleunigt die Remote-Implementierung und -Bereitstellung von Firewalls. Geräte können schneller, kostengünstiger und einfacher konfiguriert werden. Gleichzeitig können Sicherheits- und Connectivity-Funktionen automatisch und unmittelbar bereitgestellt werden. Administratoren können eine große Anzahl von Firewalls mit minimalem Benutzereingriff in Betrieb nehmen. Über eine einzelne webbasierte Managementkonsole können Richtlinien verteilt, die Firmware auf allen Geräten aktualisiert und Lizenzen synchronisiert werden.

Analyse

Mit einer geeigneten Lösung könnte die IT-Abteilung gründliche Nachforschungen sowie eine forensische Analyse von angereicherten Sicherheitsdaten durchführen. Auf diese Weise könnten alle Stakeholder über dieselben Informationen und eine einheitliche, situativ angepasste, Ansicht der Netzwerksicherheitsumgebung verfügen. So könnten sie fundierte

> Sicherheitsteams sollten die Flexibilität und Sicherheit haben, jederzeit geeignete Firewall-Regeln in Übereinstimmung mit geltenden Compliance-Vorgaben zu implementieren.

Entscheidungen zu Sicherheitsregeln auf Basis zeitkritischer und konsolidierter Bedrohungsinformationen treffen. Zudem könnte die IT-Abteilung im Fall neuer Risiken und Bedrohungen die Sicherheitsregeln und -maßnahmen entsprechend anpassen. Dank aussagekräftiger Echtzeitdaten zu Bedrohungen würden sich dadurch auch die Reaktionszeiten bei Vorfällen verkürzen.

Fazit

Mit der richtigen cloudbasierten Sicherheitsmanagement-Plattform können Unternehmen und Serviceprovider eine vollständig koordinierte Security-Governance-, Compliance- und Risikomanagementstrategie implementieren. Mit der richtigen Plattform lassen sich zudem die Kosten und der Aufwand für den Betrieb einer eigenen Infrastruktur reduzieren. Gleichzeitig erhält man ein Maximum an Visibilität, Flexibilität und Funktionalität, um das Netzwerksicherheitsökosystem von SonicWall einfacher, präziser und schneller von zentraler Stelle aus zu verwalten.

Auf sonicwall.com/capture-security-center **erfahren Sie mehr darüber**, welche Vorteile der SonicWall Capture Security Service bietet

Über uns

Seit über 25 Jahren schützt SonicWall kleine, mittlere und große Unternehmen weltweit vor Cyberkriminalität. Mit unseren Produkten und Partnerschaften können wir eine Echtzeit-Cyberabwehrlösung für die individuellen Anforderungen von über 500.000 Organisationen in über 150 Ländern bereitstellen, damit sie sich voll und ganz auf ihr Geschäft konzentrieren können.

Wenn Sie Fragen zur Nutzung dieser Unterlagen haben, wenden Sie sich an:

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, Kalifornien 95035, USA

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

SolutionBrief-AUnifiedApproach-US-KJ-MKTG2858