Sichere Konnektivität für die moderne hybride Belegschaft

Einleitung

Die Umstellung auf Remote-Arbeit und hybride Netzwerke (On-Premise- und Cloud-Lösungen) hat die Cybersicherheitslandschaft erheblich verändert. Herkömmliche Netzwerksicherheitsmodelle, die auf On-Premise-Firewalls und VPNs basieren, haben Schwierigkeiten, eine dezentrale Belegschaft effektiv zu schützen.

WatchGuard FireCloud Internet Access, die erste Version der Secure Service Edge (SASE)-Strategie von WatchGuard, behandelt die Herausforderungen der Sicherung von Remote-Mitarbeitern beim Zugriff auf das Internet und Cloud-Anwendungen von verschiedenen Standorten auf der ganzen Welt. Diese Lösung erweitert den robusten Schutz von Firebox-Firewalls auf Remote-Mitarbeiter, verbessert die Benutzererfahrung und vereinheitlicht Sicherheitsrichtlinien weltweit, wodurch die Verwaltung erheblich vereinfacht wird.

Die Herausforderung: Gewährleistung der Sicherheit der dezentralen Belegschaft

Die Ausweitung von Remote- und Hybrid-Arbeitskräften hat neue Sicherheitsherausforderungen geschaffen, darunter inkonsistente Sicherheitsrichtlinien in verschiedenen Netzwerken, erhöhte Angriffsflächen aufgrund ungesicherter privater und öffentlicher Netzwerke, Leistungsengpässe im Zusammenhang mit herkömmlichen VPN-Lösungen und komplexe Managementanforderungen für IT-Teams. Da sich Unternehmen in Richtung Cloud-basierter Anwendungen und Dienste bewegen, besteht ein dringender Bedarf für eine Sicherheitslösung, die unabhängig vom Standort eine nahtlose und sichere Konnektivität gewährleistet.

Lösungsübersicht: WatchGuard FireCloud Internet Access

FireCloud Internet Access ist eine Cloud-basierte SASE-Lösung, die entwickelt wurde, um Remote-Mitarbeiter unabhängig vom Standort beim Zugriff auf das Internet und Cloud-Anwendungen zu schützen. Sie basiert auf einem globalen Netzwerk von Points-of-Presence (PoPs) und bietet eine konsistente Durchsetzung von Sicherheitsrichtlinien sowie optimierte Leistung. Zu ihren Funktionen gehören Firewall as a Service, der einen Cloud-basierten Firewall-Schutz bietet; ein Secure Web Gateway, das URL Filtering, Malware-Scans und Anwendungskontrolle umfasst; und DNS-Filterung, die bösartige Domains blockiert und DNS-basierte Angriffe verhindert.

Wichtige Funktionen und Vorteile

Erhöhte Sicherheit

FireCloud Internet Access bietet eine proaktive Bedrohungsabwehr, indem Malware, Ransomware und Phishing-Versuche blockiert werden, bevor sie Benutzer erreichen. Es setzt globale Sicherheitsrichtlinien durch, um sicherzustellen, dass Benutzer und Geräte nur auf genehmigte Websites und Anwendungen zugreifen, und dadurch die Wahrscheinlichkeit einer Malware-Infektion zu minimieren.

- **Web-Blockierung und Inhaltsfilterung:** Die Umstellung auf Remote-Arbeit und hybride Netzwerke (On-Premise- und Cloud-Lösungen) hat die Cybersicherheitslandschaft erheblich verändert. Herkömmliche Netzwerksicherheitsmodelle, die auf On-Premise-Firewalls und VPNs basieren, haben Schwierigkeiten, eine dezentrale Belegschaft effektiv zu schützen.

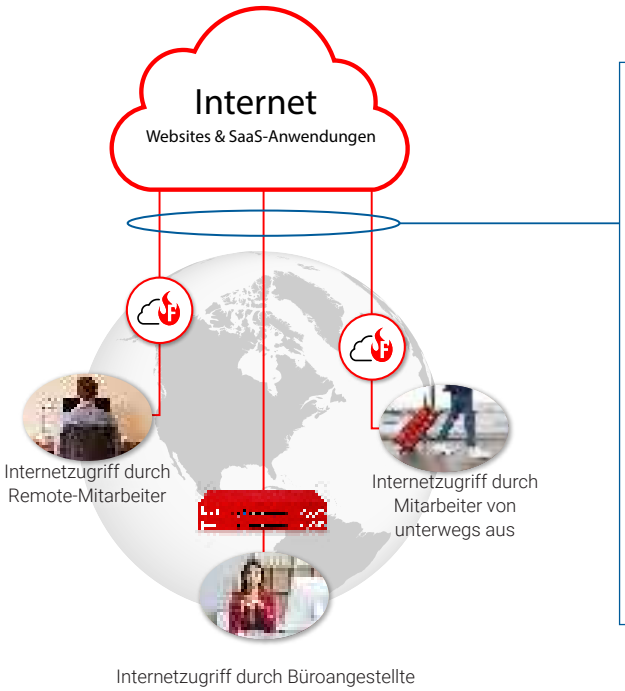
Abbildung 1: Benutzeroberfläche für FireCloud-Protokolle, gefiltert nach blockiertem Datenverkehr

- **Geolokalisierungsfilterung:** Die einzigartige Geolokalisierungsfunktion von FireCloud ermöglicht es Administratoren, den Netzwerkverkehr basierend auf geografischen Standorten zu erkennen und zu steuern. Durch die Aktivierung der Geolokalisierungsfilterung können Unternehmen den Zugang zu oder aus bestimmten Ländern oder Regionen blockieren und so die Exposition gegenüber potenziellen Cyberbedrohungen reduzieren, die von Standorten mit hohem Risiko ausgehen. Diese Funktion erhöht die Sicherheit, indem Verbindungen nur auf vertrauenswürdige geografische Gebiete beschränkt werden. Dadurch wird die Abwehr von Cyberangriffen im Unternehmen weiter gestärkt.
- **Botnet Detection und Netzwerkblockierung:** FireCloud bietet erweiterte Funktionen für die Netzwerkblockierung, einschließlich Botnet Detection und Intrusion Prevention. Die Botnet Detection-Funktion verwaltet eine aktualisierte Liste bekannter Botnet-IP-Adressen und fügt sie automatisch der Liste blockierter Websites hinzu, wodurch verhindert wird, dass Benutzer eine Verbindung zu bösartigen Domains herstellen. Darüber hinaus nutzt der Intrusion Prevention Service (IPS) von FireCloud eine signaturbasierte Erkennung in Echtzeit, um vor Netzwerkangriffen wie Spyware, SQL-Injections, Cross-Site-Scripting und Pufferüberläufen zu schützen. Administratoren können die IPS-Einstellungen so konfigurieren, dass bei erkannten Bedrohungen geeignete Maßnahmen ergriffen werden, um einen proaktiven Netzwerkschutz zu gewährleisten.

Vereinfachte Bereitstellung und Verwaltung

FireCloud-Sicherheitsrichtlinien verbessern Firebox-Richtlinien durch zentrale Verwaltung in der WatchGuard Cloud. Administratoren können Sicherheitsrichtlinien über eine einzige Schnittstelle konfigurieren und durchsetzen, was die Verwaltung durch die Verwendung konsistenter Richtlinienstrukturen und Terminologie in Firebox und FireCloud vereinfacht.

Administratoren pushen die FireCloud Agents einfach auf Zielgeräte aus der WatchGuard Cloud. Sobald die Sicherheitseinstellungen gespeichert wurden, werden sie automatisch an allen von WatchGuard gehosteten Points-of-Presence (PoPs) weltweit bereitgestellt. Dadurch wird eine konsistente Durchsetzung der Richtlinien unabhängig vom Standort des Benutzers gewährleistet.



Firewall as a Service (FWaaS)

- DNS-Filterung
- Botnet Detection
- Intrusion Prevention (IPS)
- APT Blocker Cloud Sandboxing
- TLS Inspection
- Blockierung der Geolokalisierung
- Gateway Anti-Virus (GAV)

Secure Web Gateway (SWG)

- WebBlocker URL Filtering
- Anwendungskontrolle

Anwenderauthentifizierung

- Verbindungsmanager
- Identity Provider (IdP)

Management Services

- Gemeinsame Richtlinien und Konfiguration
- Einfacher Einrichtungsassistent
- SAML-Integration für Identity Provider oder lokale Konten festlegen
- Eine Plattform: NetSec, Identity und Endpoint

Abbildung 2. FireCloud Internet Access erweitert den Firebox-Schutz auf Remote-Mitarbeiter

Bessere Benutzererfahrung

Optimiertes Routing durch ein globales Netzwerk von PoPs reduziert die Latenz und gewährleistet einen nahtlosen Zugriff auf Cloud-basierte Anwendungen und Dienste. Die skalierbare Architektur ermöglicht es Unternehmen, steigende Bandbreitenanforderungen mühelos zu bewältigen. Mitarbeiter können ohne Unterbrechung ihrer Konnektivität oder ihres Schutzes zwischen Büro- und Remote-Umgebungen wechseln.

Dashboards und Reporting

FireCloud Reporting bietet umfassende Einblicke in Netzwerkaktivitäten, Sicherheitsereignisse und Benutzerverbindungen über ein intuitives Dashboard. Der FireCloud-Nutzungsbericht liefert Echtzeit- und historische Daten und ermöglicht es Administratoren, Verkehrsmuster zu überwachen, Sicherheitsrichtlinien durchzusetzen und die Leistung zu optimieren.

- **Ansichten der Sicherheitsanalyse:** Die Registerkarte „Sicherheit“ bietet detaillierte Daten zu Netzwerkbedrohungen und blockiertem Datenverkehr. Administratoren können bestimmte Sicherheitsereignisse untersuchen, einschließlich blockierter Angriffe. Sie werden in einem Liniendiagramm angezeigt, das die Häufigkeit von Angriffsversuchen und blockierten Malware-Bedrohungen darstellt, die von FireCloud abgefangen werden. Vom APT Blocker identifizierte Zero-Day-Malware wird hervorgehoben, zusammen mit einer Aufschlüsselung der von WebBlocker blockierten URL-Kategorien. Berichte identifizieren auch die am häufigsten blockierten Anwendungen, blockierten Benutzeranfragen und die am häufigsten blockierten Ziele und Kommunikationsprotokolle. Die Geolokalisierungsfilterung stellt eine geografische Aufschlüsselung des blockierten Datenverkehrs nach Land dar, sodass Administratoren Sicherheitsmaßnahmen basierend auf dem Standort bewerten können.

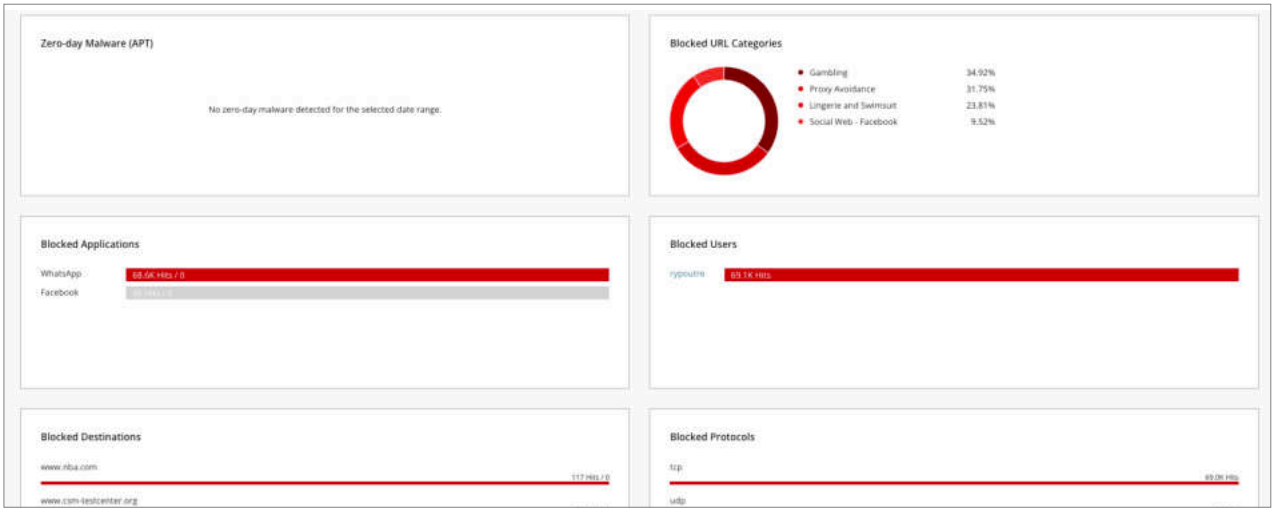


Abbildung 3: Ansicht des FireCloud-Sicherheitsberichts mit blockiertem Datenverkehr und Benutzerdetails

- **Ansichten der Datenverkehrseinblicke:** Die Registerkarte „Datenverkehr“ bietet einen Überblick über die zulässigen Netzwerkaktivitäten sowie Einblicke in das Benutzerverhalten und die Anwendungsnutzung. Sie beschreibt die am häufigsten aufgerufenen Anwendungskategorien und einzelnen Anwendungen sowie häufig besuchte Websites und Domains. Informationen über die aktivsten FireCloud-Benutzer werden zusammen mit Daten über die am häufigsten aufgerufenen Standorte und Kommunikationsprotokolle angezeigt. Eine geografische Ansicht der genehmigten Verbindungen ist verfügbar, die das Ausmaß der Netzwerkaktivitäten in verschiedenen Regionen zeigt.

- **Ansichten von Benutzeraktivität und Geräte-Monitoring:** Die Registerkarte „Benutzer“ verfolgt benutzerspezifische Daten, einschließlich authentifizierter Benutzerdetails, Geräteinformationen und Benutzergruppenmitgliedschaft. Administratoren können die Geräte sehen, von denen Benutzer eine Verbindung herstellen, die Sicherheitsrichtlinien, die auf jeden Benutzer basierend auf seiner Gruppe angewendet werden, und die Client- und Betriebssystemversionen, die auf verbundenen Geräten ausgeführt werden. Filter können angewendet werden, um die Benutzerliste zu verfeinern. Dadurch wird es einfacher, inaktive Benutzer oder Benutzer mit bestimmten installierten Clientversionen zu identifizieren.

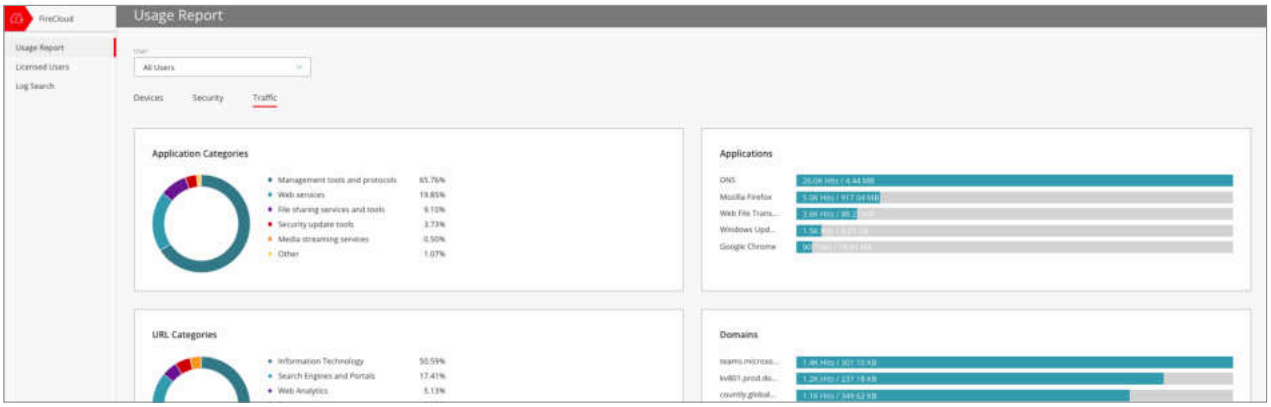


Abbildung 4: FireCloud-Nutzungsberichte beschreiben die wichtigsten Benutzeraktivitäten nach Anwendungen und Zielen

Abgedeckte Anwendungsfälle

Schutz von Remote-Mitarbeitern

Unternehmen, die Remote-Arbeit nutzen, benötigen eine Sicherheitslösung, mit der Mitarbeiter geschützt bleiben, ohne auf traditionelle VPNs angewiesen zu sein. FireCloud Internet Access ermöglicht direkte und sichere Verbindungen zu Cloud-Anwendungen, beseitigt Leistungsengpässe und sorgt für eine einheitliche Durchsetzung von Sicherheitsrichtlinien, unabhängig davon, wo die Mitarbeiter arbeiten.

Abwehr neuartiger Bedrohungen

Moderne Cyberbedrohungen, einschließlich Ransomware, Phishing und Malware, erfordern proaktive Sicherheitsmaßnahmen. FireCloud Internet Access überprüft den Netzwerkverkehr in Echtzeit und blockiert bösartige Aktivitäten, bevor sie die Benutzer erreichen. Durch die Nutzung von Cloud-basierten Bedrohungsinformationen wird die Lösung kontinuierlich weiterentwickelt, damit sie aufkommenden Cyberbedrohungen begegnen und das Risiko von Datensicherheitsverletzungen und Cyberangriffen minimieren kann.

Durchsetzung einheitlicher Sicherheitsrichtlinien

Die Einhaltung konsistenter Sicherheitsrichtlinien in einer dezentralen Belegschaft kann eine Herausforderung darstellen. FireCloud Internet Access vereinfacht die Durchsetzung von Richtlinien, indem es Unternehmen ermöglicht, Sicherheitsregeln für alle Benutzer und Geräte zu konfigurieren und anzuwenden. Die zentrale Verwaltung über die WatchGuard Cloud gewährleistet eine nahtlose Richtlinienbereitstellung und einheitliche Sicherheitsstandards für das gesamte Unternehmen.

FireCloud-Alleinstellungsmerkmale

- **Hybrid:** FireCloud Internet Access zeichnet sich durch einen hybriden Sicherheitsansatz aus, der sich nahtlos in bestehende WatchGuard Firebox-Bereitstellungen integrieren lässt. Seine einfache Bereitstellung und zentrale Verwaltung vereinfachen die IT-Administration, während das kostengünstige Preismodell die Lösung zu einer attraktiven Alternative zu Wettbewerbern wie Zscaler und Fortinet macht.
- **Umfassend:** Die Kombination aus Firewall as a Service, Secure Web Gateway und DNS-Filterung ergibt eine umfassende Sicherheitslösung, die auf moderne Arbeitsumgebungen zugeschnitten ist.
- **Übersichtlich:** Die Integration von FireCloud in Firebox und WatchGuard Cloud bedeutet, dass ein einziger Satz von Sicherheitsrichtlinien sowohl für On-Premise- als auch für Cloud-/SaaS-Anwendungen für Büro- und Remote-Mitarbeiter definiert werden kann. Bei Lean IT-Teams oder MSPs gewährleistet dieser Ansatz eine einfachere Verwaltung, konsistente Sicherheitskontrollen und niedrigere Kosten im Vergleich zu anderen SASE-Angeboten.
- **Einfach:** Die einfache Bereitstellung ist ein entscheidender Vorteil – FireCloud verwendet den gleichen universellen Agent wie WatchGuard EPDR und gewährleistet dadurch einen leichten und stabilen SASE-Client. In Kombination mit der globalen PoP-Infrastruktur von WatchGuard und der zentralen Verwaltung der WatchGuard Cloud lässt sich FireCloud problemlos bereitstellen.
- **Integriert:** Durch die Integration in die WatchGuard-Funktionen zur Erkennung und Reaktion auf Bedrohungen wird die Sicherheit weiter gestärkt. FireCloud-Protokolle werden in ThreatSync aufgenommen und bieten eine einheitliche und korrelierte Erkennung und Reaktion auf Bedrohungen für Anwendungsfälle von Remote-Mitarbeitern. Dies ermöglicht es MSPs, eine überlegene SASE-Lösung anzubieten und gleichzeitig die Umgebung kontinuierlich auf Risiken und Bedrohungen zu überwachen.

Fazit

Da Unternehmen verstärkt Remote-Arbeit und Cloud-basierte Anwendungen nutzen, ist der Schutz dezentraler Belegschaften zu einer Priorität geworden. WatchGuard FireCloud Internet Access bietet umfassende, Cloud-native Sicherheit, die den Schutz verbessert, das IT-Management vereinfacht und die Netzwerkleistung verbessert. Durch die Konsolidierung wichtiger Sicherheitsfunktionen in einer einzigen, einfach zu verwaltenden Plattform ermöglicht es FireCloud, dass Managed Service Provider einen effektiven Sicherheitsdienst für Remote-Mitarbeiter bereitstellen und Unternehmen die heutigen Cybersicherheitsherausforderungen mit Zuversicht meistern.

Über WatchGuard

WatchGuard® Technologies, Inc. gehört zu den führenden Anbietern im Bereich Cybersicherheit. WatchGuards Unified Security Platform®-Ansatz ist speziell auf Managed Service Provider ausgelegt, damit sie erstklassige Sicherheit bieten können, die die Skalierbarkeit und Schnelligkeit ihres Unternehmens erhöht und gleichzeitig die betriebliche Effizienz verbessert. Über 17.000 Vertriebspartner und Dienstleister im Bereich Sicherheit verlassen sich auf die prämierten Produkte und Services des Unternehmens, die die Bereiche Network Security and Intelligence fortschrittlicher Endpoint-Schutz, Multifaktor-Authentifizierung sowie sicheres WLAN umfassen, und sorgen somit für den Schutz von mehr als 250.000 Kunden. Gemeinsam bieten diese Bereiche die fünf entscheidenden Elemente einer Sicherheitsplattform: umfassende Sicherheit, kollektive Intelligenz, Transparenz und Kontrolle, operative Ausrichtung und Automatisierung. Neben der Zentrale in Seattle im US-Bundesstaat Washington unterhält das Unternehmen Niederlassungen in ganz Nordamerika, Lateinamerika und Europa sowie im asiatisch-pazifischen Raum. **Weitere Informationen finden Sie unter** WatchGuard.com/de.

US-VERTRIEB 1.800.734.9905 INTERNATIONALER VERTRIEB +1.206.613.0895 WEB www.watchguard.com/de WatchGuard Technologies, Inc.

Mit diesem Dokument werden keine ausdrücklichen oder stillschweigenden Gewährleistungen gegeben. Alle hier aufgeführten technischen Daten können sich ändern. Informationen zu zukünftigen Produkten, Ausstattungsmerkmalen und Funktionen werden zu gegebener Zeit zur Verfügung gestellt. © 2025 WatchGuard Technologies, Inc. Alle Rechte vorbehalten. WatchGuard, das WatchGuard-Logo und Firebox sind eingetragene Marken von WatchGuard Technologies, Inc. in den USA und/oder anderen Ländern. Alle weiteren Markennamen sind das Eigentum ihrer jeweiligen Inhaber. Teilenr. WGCE67814_031225