DATENBLATT

FireCloud Internet Access

Schutz auf Enterprise-Niveau, überall

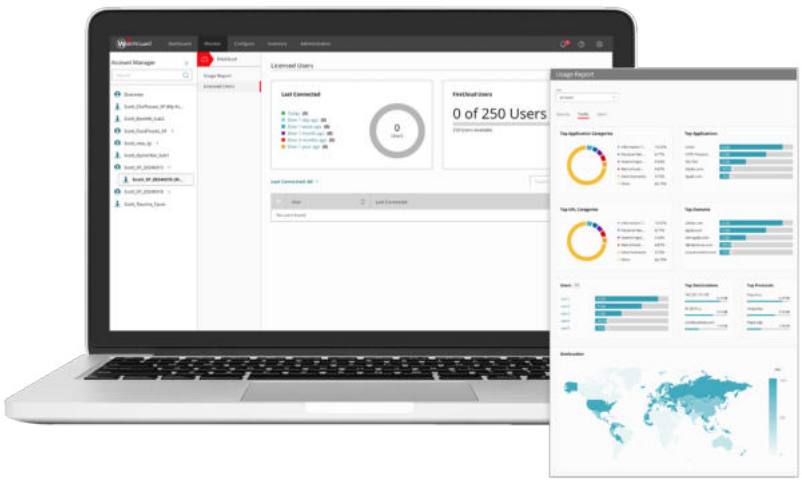
Der moderne Arbeitsplatz hat sich über das traditionelle Büro hinaus weiterentwickelt. Heutzutage arbeiten Mitarbeiter effektiv von abgelegenen Standorten und von zu Hause aus. Diese erhöhte Flexibilität stärkt Unternehmen, hat aber auch dazu geführt, dass die Grenzen traditioneller Netzwerke verschwommen sind, was zu erheblichen Sicherheitsherausforderungen führt. FireCloud Internet Access ist eine cloudbasierte Sicherheitslösung, die entwickelt wurde, um diese Sicherheitsprobleme zu lösen und gleichzeitig die Produktivität von Anwendern aufrechtzuerhalten. Als wichtige Komponente einer SASE (Secure Access Service Edge)-Lösung adressiert FireCloud Internet Access die große Herausforderung, den Remote-Zugriff von Anwendern auf das Internet und auf Cloud-Anwendungen weltweit zu verwalten und zu sichern.

Leistungsstarke Sicherheit über die Netzwerkgrenzen hinaus

Herkömmliche Perimeter-Sicherheitslösungen sind zwar für den Schutz eines jeden Unternehmens unerlässlich, ist aufgrund der steigenden Zahl von Remote-Mitarbeitern und der Mängel bestehender Tools eine Lösung erforderlich, die die Sicherheit für Remote-Anwender stärkt und Schutz vor der komplexen Bedrohungslandschaft sicherstellt. Dieser neue Ansatz soll Remote-Mitarbeitern das gleiche Maß an Schutz bieten wie den Mitarbeitern vor Ort im Unternehmen.

FireCloud Internet Access ist eine cloudbasierte Sicherheitslösung, die On-Premises Sicherheitsdienste auf Remote-Mitarbeiter überall auf der Welt ausdehnt. Sie bietet verschiedene robuste Sicherheits- und Verwaltungsfunktionen, darunter Schutzmechanismen, die für On-Premises Mitarbeiter erforderlich sind, einschließlich URL-Filterung, Intrusion Prevention Systems (IPS) und DNS-Sicherheit, um einen sicheren Zugriff auf das Internet und Cloud-Anwendungen sicherzustellen.

Nutzen Sie FireCloud Internet Access, um Ihr Unternehmen vor Malware, Phishing-Versuchen und anderen Online-Bedrohungen zu schützen – und das alles mit dem Grad an Flexibilität, den Sie für die Bereitstellung und Skalierung Ihrer Sicherheit benötigen.



Die wichtigsten Vorteile von FireCloud Internet Access:

- **Verbesserte Sicherheitsleistung:** Erweitern Sie die Firewall-Sicherheitsrichtlinien und den blitzschnellen Schutz mit einer nahtlosen Benutzererfahrung auf Remote-Mitarbeiter.
- **Optimierte Verwaltung und Effizienz:** Setzen Sie einheitliche Sicherheitsrichtlinien im gesamten Unternehmen durch, um die Implementierung zu vereinfachen, Umgebungen zu stärken, die Effizienz zu steigern und Angriffsrisiken zu reduzieren.
- **Umfassender Schutz vor Bedrohungen:** Schützen Sie sich mit Intrusion Prevention-Systemen und Malware-Erkennung gegen aufkommende Bedrohungen.
- **Sicherer Internetzugang:** Steuern Sie den Internetzugang von Remote-Mitarbeitern, um die Compliance zu verbessern und sich vor webbasierten Angriffen zu schützen.
- **Zentralisierte Administration:** Die Cloud-basierte Verwaltung reduziert den Verwaltungsaufwand, automatisiert Updates und Wartung und optimiert die Berichterstattung über Sicherheitsereignisse.

Nahtlose, globale Sicherheit für Ihre Mitarbeiter

Unterstützen Sie Remote-Mitarbeiter und schützen Sie in der Cloud gehostete Anwendungen mit FireCloud Internet Access. Die Verwaltung erfolgt über WatchGuard Cloud, integriert die Funktionen von Firewall-as-a-Service (FWaaS) sowie Secure Web Gateway (SWG) und stellt robuste Sicherheitsfunktionen auf Enterprise-Niveau bereit. Mit WatchGuard Cloud können Administratoren mühelos globale Sicherheitsdienste und -richtlinien konfigurieren, die sofort an unsere globalen Points of Presence (PoPs) weitergegeben werden. Anwender profitieren von reibungslosem Zugang, da sie ihre Anmeldeinformationen einfach auf jedem Gerät im FireCloud-Client eingeben können, um eine zuverlässige und standortunabhängige Sicherheitsabdeckung sicherzustellen.

Stateful Firewall

Überprüft den Netzwerkverkehr, blockiert böswillige Aktivitäten, schützt sensible Daten und bietet erweiterte Funktionen wie Intrusion Prevention, Malware-Erkennung und URL-Filterung, um sich gegen eine Vielzahl von Bedrohungen zu schützen.

Intrusion Prevention Service (IPS)

Bietet Echtzeitschutz vor Netzwerkangriffen wie Spyware, SQL-Injections und Cross-Site Scripting, indem bösartiger Datenverkehr identifiziert und blockiert wird, um Ihr Netzwerk vor potenziellen Sicherheitsverletzungen zu schützen.

Anwendungskontrolle

Verbessert die Netzwerksicherheit, indem die Ausführung nicht autorisierter Software sowie potenzielle Verstöße dadurch verhindert werden, dass genau kontrolliert wird, welche Anwendungen auf Geräten ausgeführt werden dürfen.

WebBlocker

Schützt Ihr Netzwerk, indem bösartige Websites und unangemessene Inhalte blockiert werden, damit Ihr Unternehmen in der Lage ist, eine sichere und produktive Online-Umgebung aufrechtzuerhalten.

Gateway AntiVirus

Scannt den ein- und ausgehenden Datenverkehr auf Viren, Malware und andere Bedrohungen und bietet umfassenden Schutz vor Cyberangriffen, um sensible Daten zu schützen und die Geschäftskontinuität sicherzustellen.

APT Blocker

Nutzt KI und maschinelles Lernen, um komplexe Cyberbedrohungen wie Advanced Persistent Threats (APTs), Zero-Day-Exploits und Ransomware zu identifizieren und zu blockieren.

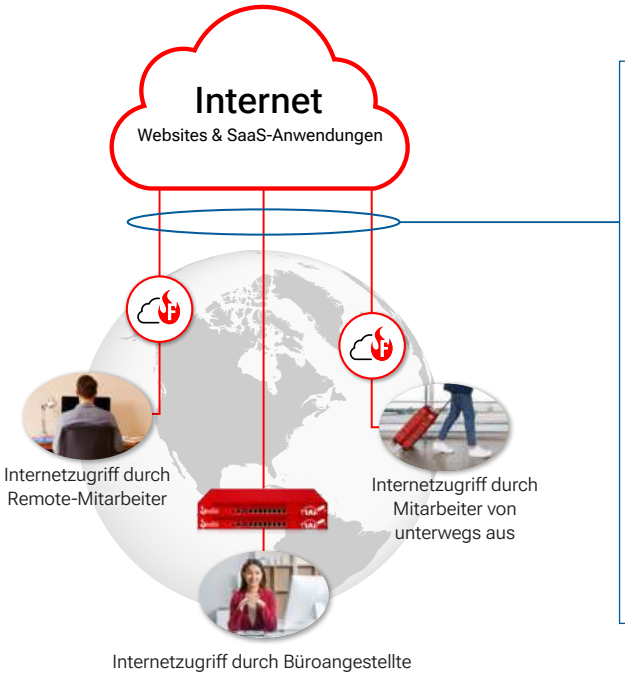
DNSWatch

Bietet erweiterte Bedrohungsinformationen, Echtzeit-Blockierung und DNS-Filterung, um Netzwerke und Anwender über einen cloudbasierten DNS-Sicherheitsdienst zu schützen.

WatchGuard Cloud

Bietet optimierte Transparenz, Kontrolle, Bedrohungsüberwachung in Echtzeit sowie die Aufbewahrung von Protokoll- und Berichtsdaten über eine einzige Schnittstelle, wodurch das Netzwerksicherheitsmanagement vereinfacht, Zeit gespart und eine fundierte Entscheidungsfindung über eine zentrale Managementplattform ermöglicht werden.

Erweitern Sie die Firebox-Sicherheit auf Remote-Mitarbeiter



Firewall as a Service (FWaaS)

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

Secure Web Gateway (SWG)

- WebBlocker-URL-Filterung
- Anwendungskontrolle

Benutzerauthentifizierung

- 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

DEUTSCHLAND, ÖSTERREICH, SCHWEIZ +49 700 92229333 INTERNATIONALER VERTRIEB: +1 206 613 0895 WEB: www.watchguard.de

WatchGuard Technologies, Inc.