SASE Spickzettel

Durch die zunehmende Verlagerung von Arbeitsplätzen ins Homeoffice oder in mobile Arbeitsumgebungen befinden sich Mitarbeiter heute häufig außerhalb des klassischen Unternehmensnetzwerks. Der Schutz durch die zentrale Firmenfirewall entfällt dabei in vielen Fällen. Unternehmen, die ausschließlich auf VPN-Lösungen setzen, bieten ihren Mitarbeitern daher oftmals keinen umfassenden und zeitgemäßen Schutz vor modernen Cyberangriffen.

Eine SASE-Lösung (Secure Access Service Edge) schafft hier einen deutlich erweiterten Sicherheitsansatz. Hierbei wird auf dem jeweiligen Endgerät ein Client installiert, der eine sichere Verbindung zu einem sogenannten Point of Presence (PoP) herstellt. Der gesamte Datenverkehr wird anschließend nicht direkt über das öffentliche Internet geleitet, sondern zunächst über den nächstgelegenen PoP — beispielsweise in Frankfurt am Main — und von dort über ein leistungsstarkes, globales Backbone-Netzwerk weitergeführt.

Dadurch profitieren Anwender unabhängig vom Standort von zentral verwalteten Sicherheitsrichtlinien, umfassendem Schutz vor unautorisierten Zugriffen sowie einer sicheren Anbindung an Cloud- und Unternehmensressourcen. Moderne SASE-Plattformen verfügen inzwischen über weltweit verteilte PoPs und ermöglichen so hohe Performance bei gleichzeitig reduziertem Administrationsaufwand.

Cloudbasierte SASE-Lösung

WatchGuard FireCloud ist eine cloudbasierte SASE-Lösung, die Remote- und Hybrid-Benutzer mit Firewall-as-a-Service, Secure Web Gateway und Zero Trust Network Access schützt. Die Verwaltung erfolgt zentral über WatchGuard Cloud mit einem Agenten und einheitlichen Richtlinien. Anstelle klassischer VPNs setzt FireCloud auf Zero Trust auf Anwendungsebene: Benutzer werden kontinuierlich verifiziert, Anwendungen bleiben vor dem Internet verborgen und Zugriffe sind auf das notwendige Maß beschränkt. So werden Angriffswege reduziert und Sicherheit, Transparenz sowie die Verwaltung und Berichterstellung vereinfacht.

Die SASE-Architektur von WatchGuard

1. **Für hybride Umgebungen optimiert**
   Zentrale Verwaltung, einheitliche Sicherheitsrichtlinien und geringere Kosten für hybride IT-Umgebungen – ideal für kleine IT-Teams und MSPs.

2. **Einfache Bereitstellung**
   Zentrale Verwaltung der Sicherheitsrichtlinien mit automatischer Verteilung auf alle weltweiten PoPs sowie schnelle Bereitstellung und Verwaltung der FireCloud-Clients über WatchGuard Cloud.

3. **Flexibel und skalierbar**
   Mit WatchGuard FlexPay lassen sich Lizenzen bedarfsgerecht erweitern. Die Firewall-as-a-Service bietet dabei eine konstant hohe Leistung unabhängig von der Anzahl der Benutzer.

WatchGuard FireCloud im Detail erklärt:

Identitätsbasierter Zero-Trust-Netzwerkzugriff
Überprüft die Benutzeridentität und den Gerätestatus für jede Sitzung und gewährt nur genehmigten Anwendungen Zugriff.

Durchsetzung von Richtlinien auf Sitzungsebene
Bewertet kontinuierlich den Zugriff während jeder Verbindung, um Missbrauch, Übernahme und seitliche Ausbreitung zu verhindern.

Verschleierung interner Anwendungen
Interne Anwendungen werden vor dem Internet verborgen und sind nur für autorisierte Benutzer zugänglich.

Cloudbasierter Webschutz
Blockiert Malware, Phishing und schädliche Websites, bevor der Datenverkehr Benutzer oder Anwendungen erreicht.

VPN-freier Fernzugriff
Ersetzt herkömmliche VPNs durch Zugriffe auf Anwendungsebene, um die Angriffsfläche und das operative Risiko zu verringern.

Einheitliches SASE-Management
Verwaltet FWaaS, SWG und ZTNA über einen einzigen Agenten und die WatchGuard Cloud-Konsole.

Anwendungsfälle:

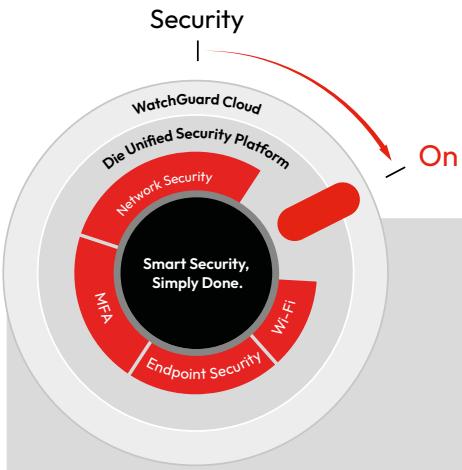
Sicherheit für Remote-Mitarbeiter
Schützen Sie Benutzer vor Angriffen aus dem Internet,egal wo sie sich verbinden.

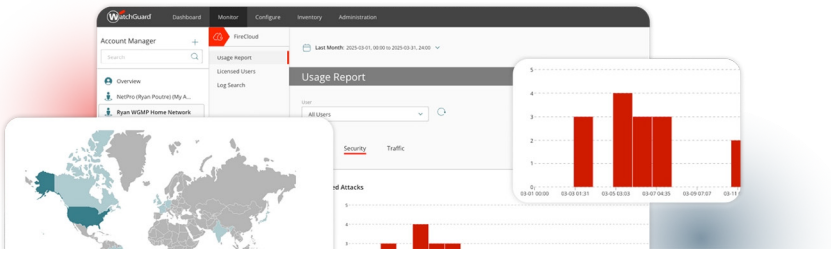
Hybrider Zugriff
Stellen Sie Benutzern eine sichere Verbindung sowohl zu SaaS- als auch zu internen Anwendungen her.

Durchsetzung von Compliance-Vorgaben
Setzen Sie das Prinzip der geringsten Berechtigungen und nachvollziehbare Kontrollen durch.

Bereitstellung von MSP-Diensten
Bieten Sie mandantenfähigen verwalteten Zugriff und Schutz über die zentrale WatchGuard Cloud-Plattform an.

infinigate | WatchGuard





Offene Fragen

- Wie viele Ihrer Mitarbeiter arbeiten mobil bzw. nicht aus dem Büro heraus?
- Wie werden diese Mitarbeitenden und ihre Geräte abgesichert?
- Was kostet Sie diese Absicherung heute?
  - Bessere Konditionen durch größere Abnahmemenge (Single- statt Multivendor-SASE)
  - Reduzierung der Fixkosten und damit laufenden Kosten aufgrund von 50% weniger Lösungen/Geräten im Einsatz.
  - Verringerung des IT-Budgets auf Langzeit durch umfassendere Absicherung
- Was würde Sie ein Ausfall der Produktion für einen Tag kosten?
  - Aufrechterhaltung der Business-Continuity für alle relevanten Applikationen
- Welche WatchGuard Lösungen haben Sie bereits im Einsatz?
  - Nahtlose Überführung der bestehenden WatchGuard-Struktur ins SASE
- Was erwarten Sie von einem cloudbasierten Management?
  - z.B. Transparenz, Berichterstattung und Protokollierung, Analysen
- Wie groß / ausgelastet ist Ihr IT-Team? Wo benötigen Sie am meisten Unterstützung von externen Fachleuten?
- SSL-VPN stirbt aus – wie sieht die Zukunft der Remote-Arbeit bei Ihnen aus?
  - Bei SSL-VPN kann ein Remote-Nutzer nach Eingabe seiner Zugangsdaten über den aufgebauten Tunnel Zugriff auf das gesamte Netzwerk erhalten, was als klare Sicherheitslücke gilt.

Sie haben Fragen zu WatchGuard SASE?

Unser Experte kennt die Antworten.

Florian Fabbro
Business Development Manager
T +49 40 237301 244
M +49 170 5587885
E Florian.Fabbro@infinigate.de

Weiterführende Informationen zu WatchGuard

Jetzt informieren

https://www.infinigate.com/de/hersteller/watchguard/

Alle Trainings, Termine & Webinare

Zu den Terminen

https://grco.de/INF-WatchGuard-Events

Infinigate Deutschland GmbH
Richard-Reitzner-Allee 8
85540 Haar/München

+49 89 89048-553
watchguard@infinigate.de
www.infinigate.de

infinigate
spark your growth