Eine echte SASE und Zero Trust Security-as-a-Service-Lösung

Dynamic Edge Protection

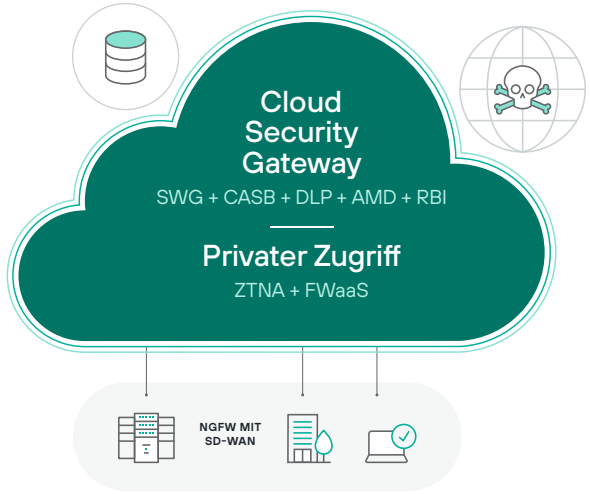
Verwaltung des Zugriffs auf Web-, Cloud- und interne Anwendungen bei gleichzeitigem Schutz vor komplexen Bedrohungen und Datendiebstahl

Wichtigste Resultate

- **Höhere Produktivität:** Ermöglichen Sie mobilen Benutzern einen schnelleren Zugriff auf Cloud-Apps, ohne Ihr Unternehmen dabei einem Risiko auszusetzen.
- **Niedrigere Kosten:** Senken Sie Investitions- und Betriebskosten, indem Sie Kauf, Bereitstellung und Verwaltung von Sicherheitshardware -und -software bestehend aus vielen Einzelkomponenten überflüssig machen.
- **Geringeres Risiko:** Stellen Sie zuverlässige, erweiterbare Sicherheitsfunktionen bereit, die ohne Schlupflöcher oder Redundanzen vor komplexen Bedrohungen und Datenverlusten schützen.
- **Optimierte Compliance:** Steigern Sie Transparenz und Kontrolle, um schneller auf Vorfälle reagieren zu können.

Ab jetzt bestimmt der Mensch die Grenzen

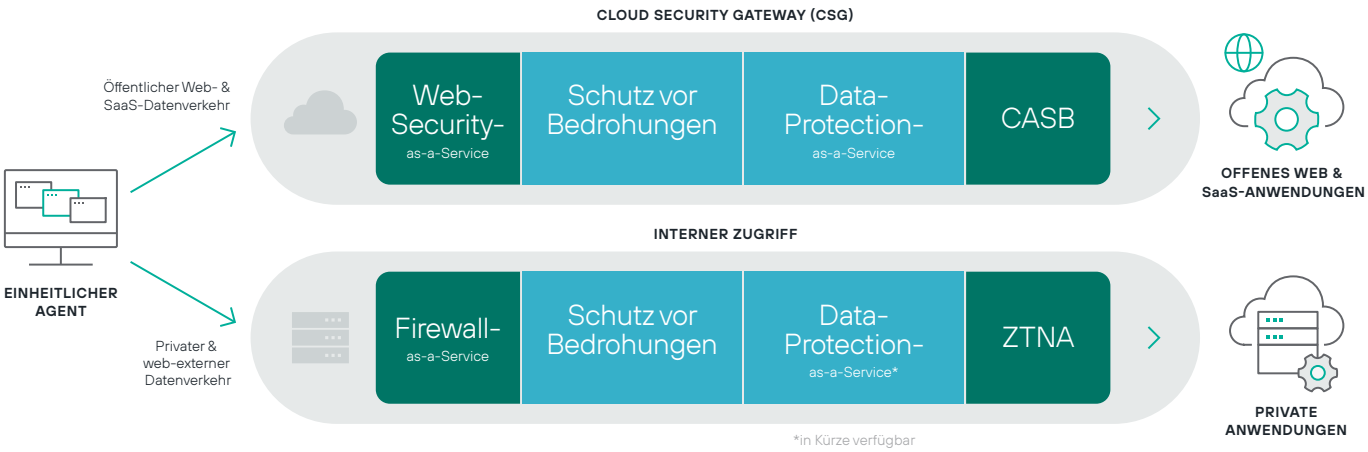
Da sich Ihre Anwendungen, Daten und Mitarbeiter immer häufiger außerhalb der traditionellen Unternehmensgrenzen bewegen, reichen herkömmliche Sicherheitskonzepte nicht mehr aus. Jeden Standort mit Hardware-Stacks auszustatten oder eigenständige Produkte für Remote-Mitarbeiter zu verwenden, sorgt nicht nur für Sicherheitslücken, sondern ist zudem äußerst kostspielig und strapaziert die ohnehin schon knappen IT-Ressourcen. Deshalb haben wir Forcepoint Dynamic Edge Protection (DEP) entwickelt, eine Suite von SASE- und Zero Trust-Lösungen. DEP ermöglicht es Ihnen, allen Mitarbeitern – egal ob diese zu Hause, im Büro oder unterwegs arbeiten – einen kontrollierten Zugriff auf Web-, Cloud- und interne Anwendungen bereitzustellen und sie vor komplexen Bedrohungen und Datenverlusten zu schützen.



Eine echte SASE und Zero Trust Security-as-a-Service-Lösung

Analysten nennen diesen neuen Cloud-nativen Ansatz Secure Access Service Edge (SASE) und Zero Trust. DEP ist eine Suite spezialisierter Cloud-Lösungen, darunter Forcepoint Cloud Security Gateway (CSG) und Forcepoint Private Access (PA), die fortschrittliche Sicherheits-Mikrodienste miteinander kombinieren. Dazu gehören Web-Content-Prüfung, URL-Filterung, Kontrolle von Schatten-IT, Zero Trust Network Access (ZTNA), Firewalls mit Eindringschutz, Malware-Scanning, Data Loss Prevention und vieles mehr. Durch diese Bündelung von Funktionen lassen sich die Sicherheitslücken und Redundanzen beseitigen, mit denen Sie früher bei Einzelprodukten zu kämpfen hatten. Außerdem gibt DEP Ihren Mitarbeitern die Freiheit ortsunabhängig zu arbeiten und sorgt gleichzeitig dafür, dass Ihr Unternehmen effizient und sicher bleibt.

Dynamic Edge Protection



Umfassender Schutz vor Bedrohungen und Datenverlusten für Web-, Cloud- und interne Anwendungen

Sie müssen sich in alle Richtungen absichern, um Bedrohungen abzuwehren und nur relevanten Datenverkehr durchzulassen. Unsere verhaltensbasierte Plattform kann beides leisten und Sie darüber hinaus einem noch stärker automatisierten und persönlicheren Schutz näherbringen. Durch diese verhaltens-zentrierte Architektur können verschiedene Richtlinien auf Basis des Risikos angewendet werden, das sich aus den Handlungen der einzelnen Benutzer ergibt. Das schafft Sicherheit und niemand wird bei der Arbeit ausgebremst. Und da wir in einer hybriden IT-Welt leben, können Sie mit DEP dort Sicherheitsmechanismen anwenden und Bedrohungen stoppen, wo es am sinnvollsten ist: in der Cloud oder vor Ort an Standorten mit besonderen Anforderungen an die Datenhoheit.

FUNKTION	VORTEILE
Erweiterte Internetsicherheit	Schützen Sie sich durch Sicherheitsrichtlinien, die dank unserer automatisierten Website-Kategorisierung stets aktuell sind, vor schädlichem Code, der in Websites und Inhalten lauert.
Sicherheit beim Cloud-Zugriff	Kontrollieren Sie Schatten-IT, indem mit nur wenigen Klicks der Zugriff auf Tausende von Cloud-Apps anhand des Namens und der Kategorie verwaltet wird.
Netzwerksicherheit der nächsten Generation	Wehren Sie Angreifer aus dem Internet ab durch eine bewährte, alle Ports und Protokolle umfassende Firewall- und Intrusion Prevention-Technologie der nächsten Generation.
Zero Trust Network Access	Gewähren Sie mobilen Benutzern sicheren Zugriff auf interne Anwendungen in Ihren Rechenzentren und Virtual Private Clouds, ohne dabei die komplexen Anforderungen, Nachteile und Risiken von VPNs in Kauf nehmen zu müssen.
Datenschutz auf Enterprise-Niveau	Vermeiden Sie, dass bei der Nutzung von Web-, Cloud- und internen Anwendungen sensible Daten und geistiges Eigentum gestohlen werden oder verloren gehen.
Schutz vor Malware und Sandboxing	Verhindern Sie, dass komplexe Bedrohungen wie Ransomware oder Zero-Day-Angriffe über infizierte Dateien durch HTTP-, HTTPS-, FTP- oder weitere Protokolle in Ihr Netzwerk gelangen.
Remote Browser Isolation	Verhindern Sie, dass Bedrohungen in Webseiten und -inhalten Ihre Geräte oder Netzwerke gefährden.
Verschlüsselte Scans mit Datenschutzkontrollen	Entschlüsseln Sie den Netzwerkverkehr, ohne dass Ihr Unternehmen dabei Kenntnis persönlicher Benutzerdaten erlangt (z. B. auf Websites von Finanzinstituten).
Branchenübliche Site-to-Site-Konnektivität	Vernetzen Sie Remote-Standorte über GRE-Tunnel oder IPsec und nutzen Sie hierzu Ihre vorhandenen Internet-Router oder Netzwerkeinrichtungen.
Automatisierte Konnektivität für Remote-Mitarbeiter	Sorgen Sie mit unserem schlanken Forcepoint One Endpunkt-Agenten für Windows und macOS dafür, dass Ihre Mitarbeiter auch remote stets geschützt sind.

forcepoint.com/contact

[Dynamic-Edge-Protection-Datasheet-DE-DE] 27July2020

Forcepoint