Forcepoint

Die Lösung im Überblick

Forcepoint ONE: Einfache Sicherheitslösung für hybride Arbeitsumgebungen in einer Cloud-Plattform

Anwendungsfälle

- Einblick und Kontrolle über die Interaktionen von Hybrid-Mitarbeitern mithilfe von Daten in Web-, Cloud- und privaten Anwendungen
- Verhindern von Missbrauch sensibler Daten, auf die über verwaltete und nicht verwaltete Geräte zugegriffen wird
- Steuern Sie den Zugriff auf risikobehaftete Webinhalte und verschiedene Arten von GenAI-Websites.
- Bereitstellen eines schnellen und sicheren Fernzugriffs auf Unternehmensressourcen und private Anwendungen ohne die Komplexität von VPNs

Lösung

- Eine einzige, einheitliche Plattform ermöglicht die Verwaltung konsistenter Sicherheitsrichtlinien für alle Geschäftsanwendungen.
- Ein integrierter, in der Cloud bereitgestellter Dienst, der dank einer Kombination von Secure Web Gateway (SWG) Cloud Access Broker (CASB) und Zero Trust Network Access (ZTNA) Zugriff und Daten schützt.
- Integrierter erweiterter Schutz vor Bedrohungen und Datensicherheit, damit Angreifer außen vor und sensible Daten sicher bleiben.
- Zusätzliche Funktionen wie Remote Browser Isolation (RBI), Cloud Security Posture Management (CSPM) zum Überprüfen von Mandanten in öffentlichen Clouds auf problematische Konfigurationen, Content Disarm and Reconstruction (CDR) zum Entfernen von Bedrohungen aus Inhalten u. a.
- Forepoint Classification für die Datenkennzeichnung.

Ergebnis

- Vereinfacht– vereint die Sicherheit für Web-, Cloud- und private Apps in einer einheitlichen Plattform (mit agentenloser Unterstützung).
- Modernität: Sie verknüpft Zero-Trust-Prinzipien mit einer SASE-Architektur und verbesserter Sicherheit durch Remote Browser Isolation und Bereinigung heruntergeladener Dateien.
- Globale Verfügbarkeit: mehr als 300 Points-of-Presence (PoPs).
- Zuverlässigkeit: bestätigte Betriebszeit von 99,99 % seit 2015.Hohe Geschwindigkeit: arbeitet zur Vermeidung von Engpässen mit dezentraler Durchsetzung und automatischer Skalierung.

Data-First-Sicherheit

Daten zu schützen wird immer komplexer, aber es gibt einen besseren Weg. Benutzer arbeiten jetzt von überall aus mit Daten, die überall verteilt sind – auf Websites, Cloud-Apps und privaten Apps.

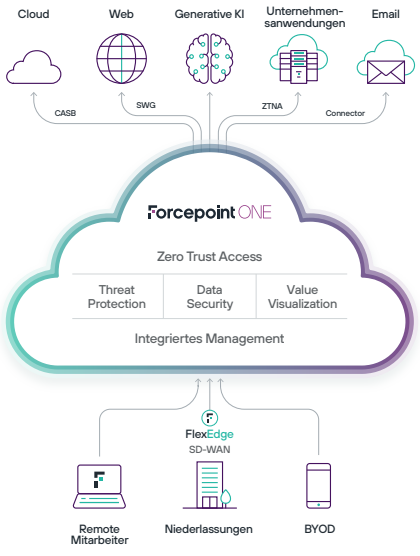
Um die Rückkehr ins Büro und hybride Mitarbeitende zu unterstützen, benötigen Sicherheitsteams eine konvergierte Sicherheitsplattform, bei denen Daten im Mittelpunkt stehen. Sicherheitskontrollen müssen sich auf Web-, Cloud- und private Anwendungen erstrecken und dabei einheitliche Transparenz und Kontrolle bieten, damit Unternehmen Datenverlust rechtzeitig verhindern können.

Mit einer Data-First-Lösung können Geschäftsdaten überall gesichert werden, für Menschen, die überall arbeiten.

Sicherheit leicht gemacht mit Forcepoint ONE

Forcepoint ONE ist eine integrierte Cloud-Plattform, die Sicherheit einfach macht. Sie können Zero Trust und Security Service Edge schnell einführen (SSE, die Sicherheitskomponente von SASE), weil wir wichtige Sicherheitsdienste, einschließlich SWG, CASB und ZTNA zusammengebracht haben.

Entfesseln Sie die Produktivität durch die sichere Übernahme neuer Technologien wie GenAI durch die Kontrolle des Zugriffs auf verschiedene Arten von GenAI-Websites und der Durchsetzung von Schutzmaßnahmen zum Absichern sensibler Daten und zur Vermeidung von Malware-Exposition.



Forcepoint ONE bietet folgende, für die Cloud konzipierte Zero Trust-Funktionen

- **Agentenlose DLP-Sicherheit für Cloud- und private Apps.** Nutzen Sie private geschäftliche Web-Apps sicher von persönlichen Geräten aus und schützen Sie gleichzeitig vertrauliche Daten.
- **Integrierter fortschrittlicher Bedrohungsschutz und Daten-Sicherheit.** Verhindern Sie Datenverlust oder Exfiltration und stoppen Sie Hacker vom Eindringen mit konsistenten Kontrollen überall.
- **Einheitliche Gateways für den Zugriff auf Cloud-, Web- und private Anwendungen.** Identitätsbasierte Zugriffskontrolle für Geschäftsanwendungen, die für SWG, CASB und ZTNA an einem Ort verwaltet werden.
- **Dynamische Skalierbarkeit mit globalem**
- **Zugriff:** 300 in AWS eingerichtete PoPs bieten schnelle Konnektivität mit niedriger Latenz und eine Betriebszeit von 99,99 % unabhängig davon, wo Mitarbeiter arbeiten.

Vereinheitlichte Sicherheitslösung für Web-, Cloud-, und private Anwendungen

- **Cloud:** CASB erzwingt auf jedem Gerät einen differenzierten Zugriff auf unternehmenseigene SaaS-Anwendungen und -Daten. CASB blockiert das Herunterladen sensibler Daten und Hochladen von Schadsoftware in Echtzeit. Die Lösung untersucht ruhende Daten in beliebten SaaS- und IaaS-Systemen auf Schadsoftware und sensible Daten und sorgt bei Bedarf für Abhilfe. CASB erkennt Schatten-IT-Anwendungen und kontrolliert auf allen verwalteten Geräten den Zugriff.
- **Web:** SWG überwacht und steuert Interaktionen mit jede Website basierend auf Risiko und Kategorie, durch Blockierung des Herunterladens von Malware oder des Hochladens sensibler Daten zu persönlichen Dateifreigaben und E-Mail-Konten. Unser On-Device Websicherheit setzt akzeptable Nutzungsrichtlinien um, auf verwalteten Geräten überall.
- **Private Anwendungen:** ZTNA schützt und vereinfacht den Zugriff auf private Anwendungen ohne die mit VPNs verbundenen Komplikationen und Risiken.

Integrierter erweiterter Schutz vor Bedrohungen und Datensicherheit

- **Data Loss Prevention (DLP, Verhinderung von Datenverlust):** Dateien und Texte werden beim Hoch- und Herunterladen auf sensible Daten überprüft und bei Bedarf blockiert, nachverfolgt, verschlüsselt oder entfernt.
- **Überprüfung auf Schadsoftware:** Dateien werden beim Hoch- und Herunterladen auf Schadsoftware überprüft und blockiert, falls diese erkannt wird.

Integrierte Transparenz und Kontrolle

- **Integrierte Managementsuite** für Konfiguration, Überwachung und Berichterstellung über SSE-Kanäle hinweg.
- **Anmelderichtlinien** zur Steuerung des Zugriffs auf Web-, Cloud- oder private Anwendungen basierend auf Benutzerstandort, Gerätetyp, Geräteposition, Benutzerverhalten und Benutzergruppe. Diese Parameter helfen, Kontoübernahmen zu verhindern.
- **Benutzerfreundliche DLP-Richtlinien** zur Downloadkontrolle und Upload sensibler Daten und Malware für verwaltete SaaS-Apps, private Apps und Websites, als auch für Daten, die in Managed SaaS und IaaS gespeichert sind.
- **Geräteeigener Agent** für Windows und MacOS zur Unterstützung von SWG, CASB oder ZTNA für Nicht-Browser Client-Apps und Schatten-IT-Kontrolle.
- **Einheitliche Analysen und die Visualisierung des Mehrwerts** liefern schnelle Einblicke in die Sicherheitsrisiken, Gesamtauslastung und Wirkung der All-in-One-Cloud-Sicherheitsplattform.

Nach Bedarf verfügbare Zusatzfunktionen

- **Cloud Security Posture Management (CSPM):** Überprüft die Einstellungen von AWS-, Azureund GCP-Mandanten auf problematische Konfigurationen und bietet manuelle und automatisierte Abhilfemaßnahmen.
- **SaaSSecurity Posture Management (SSPM):** Überprüft die Einstellungen von Salesforce-, ServiceNow- und Office 365-Mandanten auf problematische Konfigurationen und bietet manuelle und automatisierte Abhilfemaßnahmen.
- **Remote Browser Isolation (RBI):** Schützt den Benutzer vor Schadsoftware aus dem Internet auf seinem lokalen Gerät mithilfe eines Browsers, der auf einer in der Cloud gehosteten VM ausgeführt wird.
- **Forcepoint Classification:** Tagging der Data Classification mit KI-basierten Vorschlägen zur Verbesserung der Tagginggenauigkeit.
- **AMDP:** Analysiert das Dateiverhalten in einer kontrollierten Malware Sandbox zur Identifizierung versteckter und schädlicher Inhalte.

Auf Einfachheit ausgelegte Abonnements

Folgende Jahresabonnements sind pro Benutzer verfügbar:

- Die **vollständige Edition** für Sicherheit von Web-, Cloud- und privaten Anwendungen.
- **Web-Security-Edition** enthält das Web-Gateway plus Inline-CASB für unbegrenzte Cloud-Apps und RBI Essentials für unkategorisierte und neu registrierte Websites, um API-Unterstützung für Cloud-Apps und -Support, für private Apps später hinzuzufügen.
- Die **ZTNA-Edition** schützt eine unbegrenzte Anzahl privater Anwendungen.
- Die **CASB-Edition** schützt eine unbegrenzte Anzahl von Cloud-Anwendungen inline und umfasst APIs für drei Anwendungen mit der Möglichkeit, zusätzliche App-Pakete oder dedizierte API-Abfrageknoten hinzuzufügen.
- **Alle Abonnements** beinhalten ein zentrales Cloud-Management, Richtlinien mit Datenverlustprävention, einen automatisierten Zugriff über einen Endpunkt-Agenten und umfassende Berichterstattung

forcepoint.com/contact