Forcepoint

Die Lösung im Überblick

Forcepoint ONE: Einfache Sicherheitslösung für hybride Arbeitsumgebungen dank vollständig integrierter 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
- Kontrollieren des Zugriffs auf kritische Web-Inhalte
- Bereitstellen eines schnellen und sicheren Fernzugriffs auf Unternehmensressourcen und private Anwendungen ohne die Komplexität von VPNs

Lösung

- Eine zentrale, einheitliche Plattform ermöglicht über eine Konsole und einen Endpunkt-Agenten die Verwaltung eines Satzes an Richtlinien für alle Anwendungen.
- 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. (weitere Details finden Sie auf Seite 2).

Ergebnis

- Vereinfachung: Die Lösung vereint Sicherheit für Web-, Cloud- und private Anwendungen in einem Satz an Richtlinien, einer Konsole und einem Agenten (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.

Komplexe Punktlösungen bergen Risiken

Das Thema „Sicherheit" wird stetig komplexer. Wenn 75 % der Beschäftigten im Homeoffice arbeiten, verschwimmen die Grenzen zwischen Heim und Büro. Daten befinden sich mittlerweile überall – auf Websites sowie in Cloud- und privaten Anwendungen.

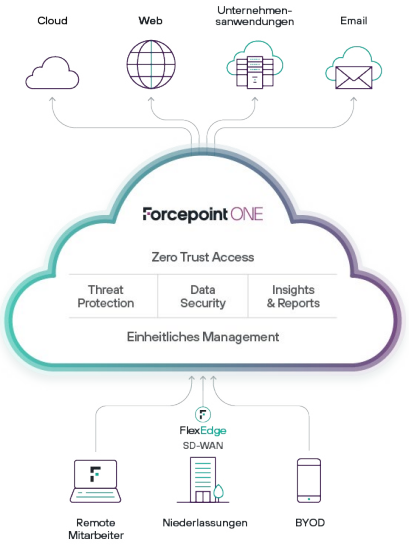
Extern tätige Mitarbeiter, Partner und Auftragnehmer mit nicht verwalteten Geräten nach dem BYOD-Prinzip machen Sie angreifbar. Geräte verbinden sich über veraltete, langsame VPNs. Auch die Anwendungen, die Sie für Zusammenarbeit und Kommunikation nutzen, sind mit Risiken behaftet. Cyber-Diebe und staatlich gelenkte Akteure haben es auf Ihre Daten abgesehen und nutzen jeden Trick, um sich Zugang zu verschaffen.

Das bisherige Portfolio von Einzelprodukten war dafür nicht ausgelegt. Sie brauchen einen einfacheren Ansatz.

Sicherheit leicht gemacht mit Forcepoint ONE

Forcepoint ONE ist eine integrierte Cloud-Plattform, mit der sich Sicherheit ganz einfach erreichen lässt. Sie können Zero Trust und Security Service Edge (SSE, die Sicherheitskomponente von SASE) rasch einführen, da wir wichtige Sicherheitsdienste miteinander verknüpft haben, darunter Secure Web Gateway (SWG), Cloud Access Security Broker (CASB) und Zero Trust Network Access (ZTNA).

Trennen Sie sich von fragmentierten Produkten. Wir bieten Ihnen eine Plattform, eine Konsole und einen Agenten mit zahlreichen Lösungsansätzen. Verschaffen Sie sich Transparenz, Zugriffskontrolle und Datensicherheit für verwaltete und nicht verwaltete Anwendungen und alle Geräte – mit nur einem einzigen Satz an Sicherheitsrichtlinien.



Absolute Cloud-Sicherheit bei jeder Interaktion

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

- → **Einheitliche Gateways für den Zugriff auf Web-, Cloud- und private Anwendungen:** identitätsbasierte Zugriffssteuerung auf Unternehmensanwendungen, die für SWG, CASB und ZTNA zentral verwaltet werden.
- → **Agentenlose BYOD-Sicherheit für Cloud- und private Anwendungen:** Private Unternehmensanwendungen im Web lassen sich sicher auf privaten Geräten nutzen, wobei sensible Daten geschützt bleiben.
- → **Integrierter erweiterter Schutz vor Bedrohungen und Datensicherheit** auf allen Gateways verhindern Datenverlust oder -exfiltration und verhindern das Eindringen von Hackern.
- → **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

- → **Web:** SWG überwacht und kontrolliert Interaktionen mit Websites basierend auf Risiko und Kategorie und blockiert das Herunterladen von Schadsoftware und Hochladen sensibler Daten in private File-Sharing- und E-Mail-Konten. Unser geräteinternes SWG setzt auf verwalteten Geräten an beliebigen Standorten Richtlinien für angemessene Nutzung durch.
- → **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.
- → **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.

Vereinfachte Durchsetzung mithilfe eines einzelnen Satzes an Richtlinien

- → **Zentrale Verwaltungskonsole** für Konfiguration, Überwachung und Berichterstattung.
- → **Einzelner Satz an Anmelderichtlinien** zur Kontrolle des Zugriffs auf Web-, Cloud- oder private Anwendungen basierend auf Benutzerstandort, Gerätetyp, Gerätezustand, Benutzerverhalten und Benutzergruppe. Diese Parameter tragen zur Verhinderung von Kontoübernahmen bei.
- → **Einzelner Satz an DLP-Richtlinien** zur Kontrolle des Herunterladens und Hochladens von sensiblen Daten und Schadsoftware für verwaltete SaaS-Anwendungen, private Anwendungen und Websites sowie für Daten, die in verwalteten SaaS- und IaaS-Systemen gespeichert sind.
- → **Vereinheitlichter geräteinterner Agent** für Windows und MacOS zur Unterstützung von SWG, CASB und ZTNA für Client-Anwendungen außerhalb des Browsers und zur Kontrolle von Schatten-IT.
- → **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-, Azure- und GCP-Mandanten auf problematische Konfigurationen und bietet manuelle und automatisierte Abhilfemaßnahmen.
- → **SaaS Security 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.
- → **Zero Trust Content Disarm and Reconstruction (CDR):** Entfernt in einem Dokument eingebettete Schadsoftware und generiert die Datei neu, bevor der Benutzer sie öffnet.

Auf Einfachheit ausgelegte Abonnements

Folgende Jahresabonnements sind pro Benutzer verfügbar:

- → Die **vollständige Edition** für Sicherheit von Web-, Cloud- und privaten Anwendungen.
- → Die **Web Security-Edition** ermöglicht es Kunden, Unterstützung für Cloud- und private Anwendungen nachträglich hinzuzufügen.
- → **Alle Abonnements** bieten eine zentrale Cloud-Verwaltung, einheitliche Richtlinien mit Schutz vor Datenverlust, automatisierten Zugriff über einen einheitlichen Endpunkt-Agenten und umfassende Berichte.

forcepoint.com/contact

© 2023 Forcepoint. Forcepoint und das FORCEPOINT-Logo sind Marken von Forcepoint.
Alle anderen hier genannten Marken sind Eigentum ihrer jeweiligen Inhaber.
[FP-Forcepoint ONE-Solution-Brief-DE] 18April2023