Forcepoint

Die Lösung im Überblick

Cloud Access Security Broker

Sichere Daten in jeder Cloud-App mit Zugriff von jedem Gerät

Herausforderung

- Schutz und Kontrolle des Zugriffs auf verwaltete Anwendungen von BYOD-Geräten
- Kontrolle des Uploads und Downloads sensibler Daten in jede verwaltete SaaS-Anwendung
- Abwehr versteckter Malware in geschäftlichen Datendateien
- Erkennung und Kontrolle von Schatten-IT

Lösung

- SaaS-App-Sicherheit mit integrierten DLP-Funktionen und Schutz vor komplexen Bedrohungen
- Detaillierter Zero-Trust-Zugriff und Datenkontrollen basierend auf Benutzer, Gerät und Standort
- Hyperskalierende AWS-Plattform für maximale Betriebszeit und minimale Latenz
- DLP-Durchsetzung auf allen verwalteten und nicht verwalteten Geräten

Ergebnis

- Höhere Produktivität durch nahtlosen und sicheren Benutzerzugriff auf Informationen von jedem Standort
- Geringeres Risiko durch Kontrolle sensibler Daten in der Cloud und Malware-Schutz
- Niedrigere Kosten durch vereinfachte Sicherheitsmaßnahmen, indem Richtlinien zentral festgelegt werden
- Optimierte Compliance mit nachweisbaren Prozessen zur Kontrolle von Informationen

Die neuen Arbeitsmodelle verlangen, dass Benutzer überall einen schnellen und dennoch kontrollierten Zugriff auf Geschäftsdaten haben. Das bedeutet, dass Benutzer von jedem Gerät oder Ort aus auf Daten in SaaS-Anwendungen wie Microsoft 365, Google Workspace, Slack, Jira und Salesforce zugreifen können müssen. Bei mehr als 250 SaaS-Anwendungen für das durchschnittliche Unternehmen können Transparenz und Kontrolle unüberschaubar werden.

Schutz des Zugriffs auf Unternehmensanwendungen von BYOD- und nicht verwalteten Geräten aus

Forcepoint vereinfacht die Cloud-Sicherheit. Der Sicherheitsservice CASB von Forcepoint ONE implementiert Zero-Trust-Zugriff, damit geschäftskritische SaaS-Cloud-Apps von den privaten Geräten von Mitarbeitern (BYOD) und nicht verwalteten Geräten von Partnern und Auftragnehmern aus sicher verwendet werden können.

Kontrolle des Uploads und Downloads sensibler Daten in jede verwaltete SaaS-Anwendung

Sie erhalten einen Satz von Sicherheitsrichtlinien zur Kontrolle sensibler Daten mit branchenführender Leistung, unabhängig davon, wo und wie sich Mitarbeiter und Auftragnehmer mit dem Internet verbinden. Die Verwaltung des Zugriffs auf diese Apps von mobilen Geräten aus erleichtert die Einführung und die Produktivität, während unterschiedliche Richtlinien auf der Grundlage von Identität und Standort granulare Zero-Trust-Kontrollen bieten. Inline-Scans nach sensiblen Daten und Malware sorgen für die Sicherheit der Daten in allen SaaS-Anwendungen. Sie gewinnen mehr Sicherheit darüber, wie vertrauliche Daten in Unternehmensanwendungen geteilt werden, und dank der integrierten Data Loss Prevention (DLP) benötigen Sie keine Einzelprodukte, um Datenverletzungen zu verhindern.

Abwehr versteckter Malware in geschäftlichen Datendateien

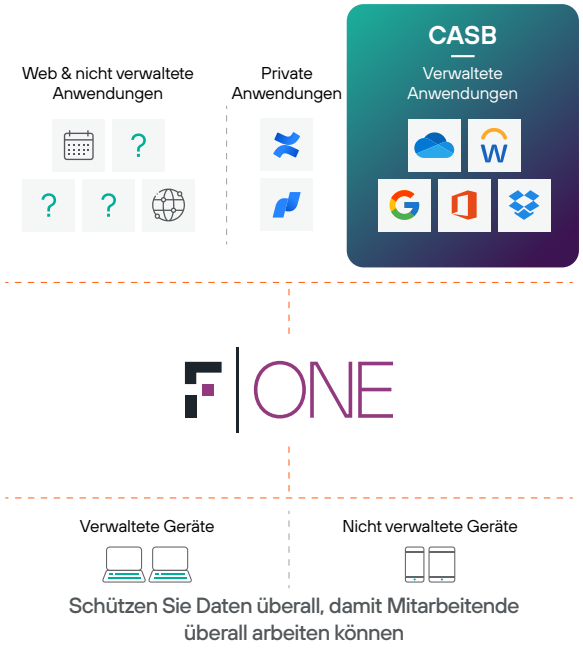
Forcepoint ONE CASB kann Schadsoftware in Daten erkennen und blockieren, die zwischen Benutzern und der SaaS-App übertragen werden, indem es Schadsoftware-Engines von mehreren Drittanbieter-Anti-Malware-Engines verwendet. Zudem kann es Schadsoftware in Dateien in beliebtem SaaS- und IaaS-Speicher entdecken und diese quarantänisieren.

Erkennung und Kontrolle von Schatten-IT

Forcepoint ONE CASB bringt Schatten-IT ans Licht und generiert eine Risikobewertung für nicht genehmigte Apps, indem es mehrere Attribute analysiert. Das gibt IT-Teams ein besseres Verständnis der SaaS-Nutzung in ihrem Unternehmen, damit sie gegebenenfalls Sicherheitsmaßnahmen ergreifen können. Das CASB erkennt nicht verwaltete SaaS-Anwendungen, die verwendet werden, indem es Netzwerkprotokolle von Unternehmens-Firewalls und Proxies nutzt, um zu ermöglichen, dass konsistente Sicherheitsrichtlinien auf zugelassene und nicht zugelassene SaaS-Anwendungen angewendet werden, damit Geschäftsdaten überall dort sicher bleiben, wo sie verwendet werden.

SaaS-Sicherheitslösung, die Betriebszeit, Verfügbarkeit und Produktivität maximiert

Unser CASB basiert auf einer Cloud-nativen, hyperskalierenden Architektur mit über 300 Points of Presence (PoPs), globaler Erreichbarkeit und einer bewährten Verfügbarkeit von 99,99 %, um SaaS-Anwendungen nahtlos zu schützen und die Benutzerproduktivität aufrechtzuerhalten. Andere Lösungen leiten den Netzwerkverkehr zu und von SaaS-Anwendungen in private Datencenter um, anstatt an Standorte, die näher an den Nutzern und den Anwendungen liegen, auf die sie zugreifen. Dies führt zu einer schlechten Leistung, wodurch latenzanfällige Anwendungen wie Slack ausfallen und Mitarbeiter sich riskanter Behelfslösungen bedienen.



Einfachere Cloud-Sicherheit in der Praxis

Von einer einzigen Konsole aus können Administratoren den Zugriff und die Daten von Benutzern sowohl verwalteter als auch nicht verwalteter Geräte (z. B. BYOD und Computer von Auftragnehmern oder Partnern) verwalten.

Sehen wir uns am Beispiel von Kris an, wie CASB die Cloud-Sicherheit vereinfacht. Kris ist Unternehmensanalyst, arbeitet von zu Hause aus und beginnt gerade seinen Arbeitstag.

Kris meldet sich auf seinem firmeneigenen Laptop bei seinem Salesforce-Konto an.	Der CASB-Service in Forcepoint ONE verwaltet die Verbindungen mit Unternehmensanwendungen, damit die Mitarbeiter sich nahtlos und sicher anmelden können.
Kris ruft salesforce.com direkt im Browser oder über ein Anwendungsportal des Unternehmens auf.	Salesforce leitet die Sitzung (über SAML) an die CASB weiter, wo geprüft wird, ob das Gerät verwaltet wird, wo es sich befindet und welchen Sicherheitsstatus es hat. Anhand vordefinierter Sicherheitsrichtlinien prüft die CASB die Identität von Kris mithilfe von Multifaktor-Authentifizierung.
Kris wird der Zugriff auf die verwaltete Anwendung gewährt.	Die vom Administrator definierten Richtlinien kontrollieren auch den direkten Zugriff auf die Anwendung: Sie gewähren entweder den kontrollierten Zugriff oder blockieren ihn ganz. Dieser Prozess dauert nur Millisekunden und hat keinen Einfluss auf die Produktivität des Mitarbeiters. Der gesamte Datenverkehr vom Gerät von Kris und von der Anwendung (mithilfe eines Reverse- or Forward-Proxys) passiert die CASB.
Kris möchte eine Umsatzprognose von Salesforce herunterladen.	Die CASB überprüft alle Dateien, die aus der Anwendung heruntergeladen werden, auf Malware und sensible Daten. Abhängig vom Ergebnis und von der Richtlinie können Malware-Dateien blockiert und sensible Daten blockiert, nachverfolgt oder verschlüsselt werden. Wenn eine Richtlinie das Herunterladen sensibler Daten auf nicht verwaltete Geräte einschränkt, wird der Download erlaubt, da Kris einen firmeneigenen Laptop verwendet.
Kris versucht, sensible Daten oder eine mit Malware verseuchte Datei über Slack zu übertragen.	Das CASB kann auch Dateien überprüfen, die in SaaS-Apps hochgeladen werden. Das CASB kann den Upload automatisch blockieren. Mit dem geräteinternen einheitlichen Agenten ist es sogar möglich, das Hochladen von Dateien in nicht genehmigte Anwendungen zu unterbinden.

Teil des Forcepoint-Ansatzes „Data Security Everywhere“

Forcepoints Mission „Data Security Everywhere“ ermöglicht es Unternehmen, Daten über SaaS, Web, E-Mail, Netzwerk und Endpunkte hinweg zu schützen, damit Menschen überall sicher mit Daten arbeiten können.

Erweiterung branchenführender DLP-Funktionen auf SaaS-Anwendungen

Mit Forcepoint können Unternehmen ihre bestehenden Forcepoint DLP-Richtlinien zum Schutz von Daten in SaaS-Anwendungen nutzen und denselben branchenführenden Datenschutz mit nur wenigen Klicks auf die Cloud ausweiten. Einheitliche DLP-Richtlinien, die über eine einzige Konsole durchgesetzt werden, helfen dabei, SaaS-Anwendungen eine konsistente Datensicherheit der Unternehmensklasse zu bieten, die Datensicherheitsverwaltung zu vereinfachen, Verstöße zu minimieren und gleichzeitig die Compliance zu optimieren. Diese Integration bringt Kunden die folgenden Vorteile:

- → Vereinfachte Cloud-Datensicherheit mit einheitlichen Richtlinien und Konsole.
- → 1.700 standardmäßige Klassifikatoren und Richtlinienvorlagen für eine umfassende Abdeckung und Compliance-Unterstützung für über 150 Regionen.
- → Konfigurationseinrichtung und Einrichtungszeit in Minuten, was die Produktivität von IT-/Sicherheitsteams verbessert.
- → Eliminieren von redundanten und fragmentierten Sicherheitsprodukten, um erhebliche Kosteneinsparungen zu erzielen.

Weitere Informationen finden Sie in der Forcepoint DLP-Broschüre.

Möchten Sie Daten in Cloud-Apps von jedem Gerät aus schützen?

Lassen Sie uns mit einer Demo beginnen.

forcepoint.com/contact

[FP-Forcepoint ONE CASB-Solution-Brief-DE] 09Dec2024