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

- Cloud-App-Sicherheit mit integrierten DLP-Funktionen und erweitertem Bedrohungsschutz
- 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

In der heutigen hybriden Arbeitsumgebung ist der Zugriff auf Cloud-Apps und Daten von Mobilgeräten aus gang und gäbe. Ein durchschnittliches Unternehmen stellt über 280 SaaS-Apps bereit, darunter Tools für die Zusammenarbeit wie Microsoft 365, Google Workplace, Slack oder Jira, die für Remote-Mitarbeiter und Auftragnehmer unerlässlich sind. Wenn es keine Möglichkeit gibt, den Zugriff von Mobilgeräten zu verwalten oder Vertrauen in die Geräte (Gerätestatus) aufzubauen, bringt die Nutzung dieser Dienste mehr Komplexität und Risiken mit sich.

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 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 einzigen Satz an Sicherheitsrichtlinien für die Kontrolle sensibler Daten mit branchenführender Leistung, ganz gleich, von wo aus und wie Mitarbeiter und Auftragnehmer sich mit dem Internet verbinden. Durch die Verwaltung des Mobilgerätezugriffs auf diese Anwendungen werden Einführung und Produktivität verbessert. Gleichzeitig sorgen unterschiedliche, von Gerätestatus und Standort abhängige Richtlinien für eine detaillierte Zero-Trust-Kontrolle und den Schutz der Daten. So haben Sie einen besseren Einblick darin, wie vertrauliche Daten in Unternehmensanwendungen auf den einzelnen (auch privaten) Geräten weitergegeben werden. Dank integrierter Data Loss Prevention (DLP, Verhinderung von Datenverlust) sind Einzelprodukte zur Verhinderung von Datenschutzverletzungen überflüssig.

Abwehr versteckter Malware in geschäftlichen Datendateien

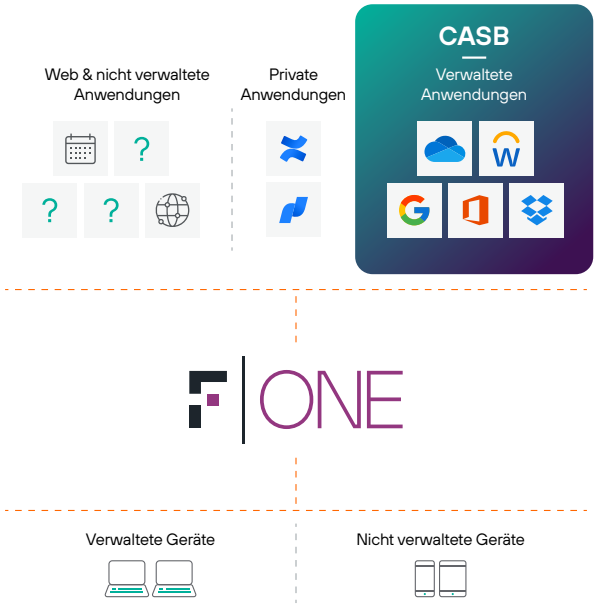
Unsere CASB-Lösung ist in der Lage, mithilfe von Malware-Engines von Bitdefender und CrowdStrike Malware in Daten, die zwischen Benutzern und der SaaS-Anwendung ausgetauscht werden, zu erkennen und zu blockieren. Darüber hinaus kann sie in Dateien verborgene Malware in beliebten SaaS- und IaaS-Speichern erkennen und diese Dateien in Quarantäne verschieben.

Erkennung und Kontrolle von Schatten-IT

Die CASB-Lösung bringt nicht nur Schatten-IT ans Licht, sondern bietet auch Kontrolle und Coaching zur sicheren Nutzung und zu besseren Alternativen. Die CASB-Lösung erkennt und listet nicht verwaltete SaaS-Anwendungen auf, die derzeit verwendet werden. Dadurch können Administratoren Richtlinien für Unternehmensgeräte festlegen, sodass der Zugriff gesperrt oder dem Benutzer eine Nachricht angezeigt wird, die auf genehmigte SaaS-Anwendungen verweist.

CASB in Forcepoint ONE maximiert Betriebszeit, Verfügbarkeit und Produktivität

Unsere CASB-Lösung ist Teil von Forcepoint ONE, unserer Hyperscaler-basierten Cloud-Plattform mit 300 Points-of-Presence (PoPs), globalem Zugriff und einer nachgewiesenen Betriebszeit von 99,99 %, um Cloud-Apps nahtlos zu schützen und die Benutzerproduktivität aufrechtzuerhalten. Bei anderen Lösungen wird der Netzwerkverkehr zu und von Cloud-Anwendungen in private Rechenzentren umgeleitet anstatt an Ziele in Benutzernähe. Dies führt zu einer schlechten Leistung, wodurch latenzanfällige Anwendungen wie Slack ausfallen und Mitarbeiter sich riskanter Behelfslösungen bedienen.



Absolute Cloud-Sicherheit bei jeder Interaktion

Einfachere Cloud-Sicherheit in der Praxis

Mit der Forcepoint ONE Cloud-Plattform ist die Implementierung von Cloud-Sicherheit denkbar einfach.

Administratoren können den Zugriff von einer einzigen Konsole aus verwalten und Datei-Downloads und -Uploads für Benutzer von verwalteten und nicht verwalteten Geräten (wie BYOD-Geräten und Computern von Auftragnehmern und Partnern) kontrollieren.

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 CASB um, wo geprüft wird, ob das Gerät verwaltet wird, wo es sich befindet und welchen Sicherheitsstatus es hat. Anhand vordefinierter Sicherheitsrichtlinien prüft CASB die Identität von Kris mithilfe von Apps zur mehrstufigen 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-Proxys) passiert CASB.
Kris möchte eine Umsatzprognose von Salesforce herunterladen.	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 in verwaltete Geräte einschränkt, wird der Download erlaubt, da Kris einen firmeneigenen Laptop verwendet.
Kris möchte sensible Daten oder eine mit Malware infizierte Datei über Slack senden oder die Daten in seinen persönlichen Dropbox-Speicher hochladen.	CASB kann auch Dateien überprüfen, die in Cloud-Apps hochgeladen werden. 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 einer einheitlichen Sicherheitslösung für Web-, Cloud- und private Anwendungen

Neben CASB schützt die allumfassende Plattform Forcepoint ONE den Zugriff auf Unternehmensinformationen von jeder Website und privaten Anwendung aus:

- → **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 Richtlinien für angemessene Nutzung auf verwalteten Geräten an beliebigen Standorten durch.
- → **Private Anwendungen:** ZTNA schützt und vereinfacht den Zugriff auf private Anwendungen ohne die mit VPNs verbundenen Komplikationen und Risiken.
- → **Zusätzliche Funktionen** wie RBI oder die Überprüfung von Cloud-Anbietern auf problematische Konfigurationen (CSPM) sind bei Bedarf verfügbar.

Weitere Informationen erhalten Sie im Lösungsüberblick von Forcepoint ONE.

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

Lassen Sie uns mit einer Demo beginnen.