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
- Gölge BT'yi belirleyin

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

Die neuen Workforce-Modelle von heute verlangen, dass Benutzer überall einen schnellen, aber kontrollierten Zugriff auf Geschäftsdaten haben. Dies bedeutet, dass die Mitarbeiter Zugriff auf Daten in Cloud-Apps wie Microsoft 365, Google Workspace, Slack, Jira und Salesforce benötigen, und zwar von jedem beliebigen Gerät oder Standort aus. Bei mehr als 250 SaaS-Anwendungen für ein durchschnittliches Unternehmen können Transparenz und Kontrolle leicht 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 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

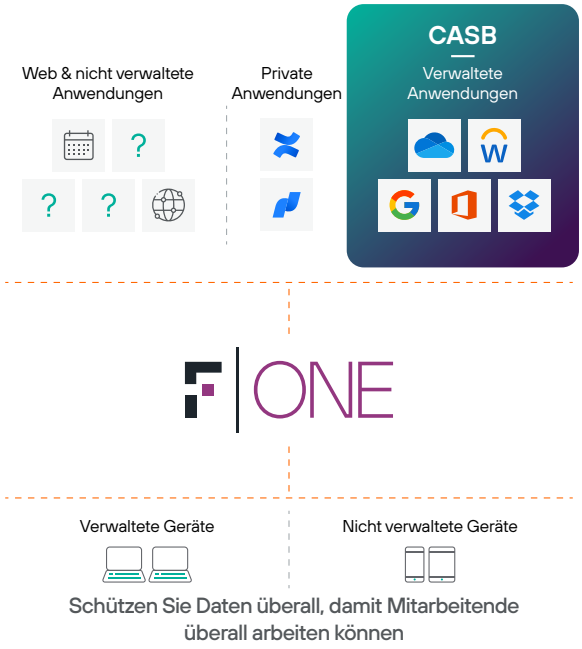
Forcepoint ONE CASB, Bitdefender ve CrowdStrike Trellix kötü amaçlı yazılım motorlarını kullanarak, kullanıcılarla SaaS uygulaması arasında aktarılmakta olan verilerdeki kötü amaçlı yazılımları tespit edip engelleyebilir. Ayrıca, popüler SaaS ve IaaS depolama çözümlerindeki dosyalarda bulunan kötü amaçlı yazılımları da tespit edip bu dosyaları karantinaya alabilir.

Gölge BT'yi belirleyin

Forcepoint ONE CASB, gölge BT'yi açığa çıkarır ve birden fazla özniteliği analiz ederek onaylanmamış uygulamalar için bir risk skoru oluşturur. Bu sayede BT ekipleri, kuruluşlarındaki SaaS kullanımı hakkında daha derin bir anlayışa sahip olabilir ve gerekli güvenlik kontrollerini uygulamaya koyabilir. CASB, ağ günlüklerini kullanarak veya Forcepoint ONE Secure Web Gateway telemetrisiyle kullanımdaki yönetilmeyen SaaS uygulamalarını tespit ederek, onaylı ve onaylanmamış SaaS uygulamalarına tutarlı güvenlik politikalarının uygulanmasını sağlayarak iş verilerini kullanıldığı her yerde güvende tutar.

CASB in Forcepoint ONE maximiert Betriebszeit, Verfügbarkeit und Produktivität

Unsere CASB-Lösung ist Teil von Forcepoint ONE, unserer Hyperscaler-basierten Cloud-Plattform mit über 300 Points-of-Presence (PoPs), globalem Zugriff und einer nachgewiesenen Betriebszeit von 99,99 %, um Cloud-Apps nahtlos zu schützen und die Benutzerproduktivität aufrechtzuerhalten. Andere Lösungen leiten den Netzwerkverkehr zu und von Cloud-Anwendungen in private Datencenter um, statt 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

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

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.	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 das Scannen von Cloud-Anbietern auf riskante Konfigurationen Cloud Security Posture Management (CSPM) und SaaS Security Posture Management (SSPM) nach Bedarf.

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.

forcepoint.com/contact

[FP-Forcepoint ONE CASB-Solution-Brief-DE] 12Sept2024