CLOUDFLARE

WHITEPAPER

SaaS-Anwendungen jetzt einfacher schützen

Wie sich Nutzer und Daten mit einem Zero Trust-Ansatz schützen lassen

Inhaltsverzeichnis

Einleitung

Im heutigen Kontext dezentraler Umgebungen können Unternehmen mit Software as a Service (SaaS)-Anwendungen ihre Mitarbeitenden und Auftragnehmenden auf der ganzen Welt flexibler unterstützen. Zu den bekanntesten SaaS-Anwendungssuites gehören derzeit die Bereiche Kommunikation (E-Mail-Versand, Chat-Plattformen), Produktivität (Dokumente, Tabellenkalkulationen) und Zusammenarbeit (Online-Speicher). Die Firma Gartner prognostiziert, dass bis zum Jahr 2025 85 % der Unternehmen ihr Geschäft nach dem Cloud-First-Prinzip betreiben werden – mit SaaS als bevorzugtem Bereitstellungsweg für Zugriffsverwaltung[1].

Zwar können Unternehmen mit SaaS-Anwendungen flexibler bleiben, doch die Verlagerung in die Cloud ist mit Sicherheits- und Performance-Risiken verbunden, insbesondere wenn Unternehmen mit mehreren unabhängigen Einzellösungen jonglieren. Sicherheits-, Netzwerk- und IT-Teams müssen Dutzende, wenn nicht gar Hunderte dieser Anwendungen implementieren und verwalten. Sie stehen oft unter Zeitdruck und behalten nur schwer den Überblick über das gesamte Unternehmen. Außerdem kämpfen sie mit Sicherheits- und Konnektivitätslücken, deren Ursache Dienste sind, die von vornherein nicht aufeinander abgestimmt waren.

Viele Unternehmen wollen die Sicherheitsprodukte in ihrer SaaS-Landschaft daher besser konsolidieren. So sollen die Effizienz erhöht, die Verwaltung und Implementierung vereinfacht sowie ein einheitlicher Support sichergestellt werden.

Gartner prognostiziert, dass bis 2025 80 % der Unternehmen auf Lösungen eines einzigen Anbieters umsteigen werden, bei dem also der Zugriff auf das Internet, Cloud-Dienste und private Anwendungen über eine einzige Security Services Edge (SSE)-Plattform erfolgt[2].

Der Übergang zu einer vereinfachten SaaS-Sicherheit beginnt mit einer Reihe wichtiger Überlegungen. Mitarbeitende kommunizieren und arbeiten heute anders als früher. Sie brauchen ein einfaches und skalierbares Sicherheitskonzept, das neuen Risiken immer einen Schritt voraus ist. Es muss die Zahl der von SaaS-Anwendungen ausgehenden Sicherheitsvorfälle reduzieren und zusätzlich noch die Überwachung und Prävention von Bedrohungen durch firmeneigene Sicherheitsteams erleichtern.

Im nächsten Abschnitt erfahren Sie, wie Sie mit einer Zero Trust-Plattform, in der die Funktionen von Cloud Access Security Broker (CASB) und Cloud Email Security (CES) integriert sind, Datenverlust, Phishing, Ransomware, Schatten-IT und laterale Bewegungen in Ihrem Unternehmen unterbinden.

[1] Gartner, „Forecast Analysis: Information Security and Risk Management, Worldwide.“ Analysten: Shailendra Upadhyay, Mark Driver, Christian Canales, Ruggero Contu, Lawrence Pingree, Elizabeth Kim, John A. Wheeler, Nat Smith, Rahul Yadav, Swati Rakheja, Dave Messett, Mark Wah, Shawn Eftink. 12. August 2021. Gartner. [2] Gartner, „Predicts 2022: Consolidated Security Platforms Are the Future.“ Analysten: Charlie Winckless, Joerg Fritsch, Peter Firstbrook, Neil MacDonald, Brian Lowans. 1. Dezember 2021. Gartner.

Die Entwicklung von CASB

Umfassende SaaS-Sicherheit erfordert die Kombination mehrerer wichtiger Verfahren. Sicherheitsteams müssen einen Überblick über ihre gesamte SaaS-Landschaft erhalten, Bedrohungen leicht überwachen und bekämpfen sowie den Zugang zu vertraulichen Daten und Systemen absichern können. Einer der wichtigsten Bestandteile jeder SaaS-Sicherheitsstrategie ist ein Cloud Access Security Broker (CASB). Dieser bietet Datensicherheitskontrollen über und Einblick in die Dienste und Anwendungen eines Unternehmens, die in der Cloud gehostet werden.

Grundlagen der SaaS-Sicherheit: CASB

Mit CASB als SaaS können IT- und Sicherheitsteams alle Dateneinstellungen und Nutzeraktivitäten von einem einzigen Dashboard aus überblicken. Die Funktionen variieren je nach Anbieter, decken aber in der Regel Folgendes ab[3]:

- **Datenschutz:** CASB schützen vertrauliche Daten und verhindern, dass sie die vom Unternehmen kontrollierten Systeme verlassen.
- **Zugriffskontrolle:** CASB helfen dabei, zu steuern, was Nutzer in den vom Unternehmen kontrollierten Anwendungen sehen und tun können. Teilweise bieten sie auch Funktionen zur Identitätsüberprüfung, mit denen sichergestellt werden kann, dass Nutzer tatsächlich sind, wer sie vorgeben zu sein.
- **Aufspüren von Schatten-IT:** CASB helfen bei der Erkennung nicht autorisierter Systeme und Dienste (gemeinhin als „Schatten-IT“ bezeichnet), die Mitarbeitende für geschäftliche Zwecke nutzen. Wenn Sie diese Systeme katalogisieren, können sie bisher unbekannte Sicherheitsrisiken aufspüren und bekämpfen.
- **Schutz vor Bedrohungen:** CASB setzen Verfahren wie Malware-Erkennung, Sandboxing und Paketinspektion ein, um Datenlecks und externe Angriffe zu verhindern.
- **Statusverwaltung:** CASB liefern Sicherheitsteams Analysedaten zum Nutzerverhalten und Kontrolle über den Anwendungsstatus, sodass Bewegungen und Bedrohungen in einer SaaS-Umgebung leicht überwacht und verfolgt werden können.
- **Compliance:** CASB helfen Unternehmen bei der Einhaltung gesetzlicher Vorschriften (z.B. SOC 2, HIPAA, DSGVO), indem sie Fehlkonfigurationen aufdecken und damit verbundene Strafen und Bußgelder für Compliance-Verstöße vermeiden.

[3] Dies stellt keine erschöpfende Auflistung der Funktionen dar, die in einem CASB-Angebot enthalten sein können.

Aktuelle CASB-Herausforderungen

Mit der zunehmenden Verbreitung von SaaS wächst auch die Angriffsfläche, die Unternehmen schützen müssen. Die wertvollen Daten befinden sich nicht mehr in einer einzigen Datenbank, sondern in Anwendungen, die von Drittanbietern verwaltet werden (z. B. Dropbox, Google Drive usw.) – unabhängig davon, ob Sie diese für die Nutzung im Unternehmen mit einer Sandbox versehen haben oder nicht.

CASB helfen zwar beim Schutz von Unternehmensdaten und Nutzern innerhalb von SaaS-Anwendungen, stellen aber immer noch keine perfekte Absicherung gegen Bedrohungen dar. Da bei SaaS-Anwendungen eine größere Menge an wertvollen Daten verarbeitet wird, nehmen Angreifer diese Applikationen zunehmend ins Visier – unter anderem, um diese Daten zu erbeuten. Auch einfache Fehlkonfigurationen und Nutzerfehler können diesen Angriffen Tür und Tor öffnen:

Gartner prognostiziert, dass bis 2025 mehr als 99 % der Sicherheitsverletzungen in der Cloud ihren Ursprung in vermeidbaren Fehlkonfigurationen oder Nutzerfehlern haben werden[4].

Viele CASB sind immer noch unzureichend, wenn es darum geht, Fehlkonfigurationen von Nutzern und moderne SaaS-Angriffe vorherzusehen und zu beheben. Einige Provider bieten daher inzwischen Cloud- oder SaaS Security Posture Management Services (CSPM oder SSPM[5]) an. Damit können Konfigurations- und Compliance-Fehler über die Steuerungsschnittstelle verfolgt werden. Dies ist jedoch nicht überall der Fall, sodass viele Unternehmen nicht über die erforderlichen Erkennungs- und Abhilfemöglichkeiten verfügen.

Darüber hinaus gelingt es einigen CASB-Angeboten nicht, Datenschutzverletzungen vorzubeugen. Dies führt zu erhöhten Behebungskosten und Datenverlusten, da die Sicherheitsteams gegenüber den Angreifern immmer im Rückstand sind.

[4] Gartner, „Hype Cycle for Cloud Security, 2021“. Analysten: Tom Croll, Jay Heiser. 27. Juli 2021. Gartner.
[5] Diese Dienste und Funktionen werden oft zusätzlich zu, häufiger aber als Teil von CASB-Lösungen angeboten und gewährleisten sowohl Inline- als auch API-basierten Schutz für Anwendungen.

Das Problem bei der Implementierung und Integration von CASB

Während SaaS-Anbieter die Fähigkeiten ihrer integrierten Sicherheitsangebote ausbauen, bleiben zwei große Hürden bestehen: Integration und Transparenz. Zwar machen diese Anbieter Daten zugänglich und leicht nutzbar, doch die Unternehmen müssen die Sicherheitsfunktionen immer noch so bündeln, dass sie leicht zu verwalten sind. Für Unternehmen, die mehrere Einzellösungen einsetzen, erschwert sich das Tracking von Bedrohungen über verschiedene Plattformen hinweg, wenn diese Lösungen nicht für die Integration untereinander konzipiert sind oder unterschiedliche Transparenzstufen bieten.

Dies erhöht die Komplexität der Anwendungsumgebung, sodass selbst einfache Angriffe schwieriger vorherzusehen und zu bekämpfen sind – Angreifer müssen schließlich nur Lücken zwischen den Sicherheitsplattformen erkennen, um Angriffe unentdeckt ausführen zu können. Unternehmen können mit einem CASB von einem einzigen Ort aus auf Sicherheitsprodukte zugreifen und erhalten so einen umfassenderen Überblick und bessere Möglichkeiten, bei der Bekämpfung von Bedrohungen alle ihre Sicherheitstools einzusetzen.

Dennoch sind CASB nur ein Teil einer größeren SaaS-Sicherheitsstrategie. Zur Abdeckung der gesamten SaaS-Landschaft müssen Unternehmen die CASB-Funktionen mit anderen Zero Trust-Technologien verknüpfen, ohne damit unnötige zusätzliche Komplexität zu erzeugen oder Sicherheitsteams zu zwingen, jedes Tool manuell zu konfigurieren und zu pflegen. SaaS lässt sich nicht im großen Maßstab einfach manuell kontrollieren. Vielmehr ist zur Ergänzung von SaaS-Verwaltungsplattformen und CASB-Tools eine Automatisierung erforderlich. Nur so können Unternehmen eine breite Palette von Bedrohungen wirksam bekämpfen, ohne einen Burnout ihres Teams oder Fehlkonfigurationen und Nutzerfehler zu riskieren.

Die Weiterentwicklung der E-Mail-Sicherheit

Wie die meisten SaaS-Dienste hat sich auch die E-Mail-Kommunikation zu einer wichtigen Geschäftsanwendung für Unternehmen jeder Größe entwickelt. Mit der Verlagerung in die Cloud und der Verbreitung von Remote-Arbeit wenden sich immer mehr Unternehmen den cloudbasierten E-Mail-Lösungen von Microsoft 365 und Google Workspace zu – laut Gartner sogar 70 % aller Firmen weltweit[6].

E-Mail ist heute deshalb die am weitesten verbreitete SaaS-Anwendung und stellt eine der größten Angriffsflächen dar, die Phishing, Malware, Spoofing, die Kompromittierung von Geschäfts-E-Mails (Business Email Compromise – BEC) und andere moderne Bedrohungen anziehen.

Doch der Schutz vor E-Mail-Angriffen kann für Sicherheitsteams eine mühsame und überwältigende Aufgabe sein, zumal die Angreifer immer raffiniertere Taktiken gegenüber ahnungslosen Mitarbeitenden einsetzen. Um Nutzer und Daten vor diesen Bedrohungen zu schützen, sollten Sicherheitsverantwortliche die Integration von E-Mail in ihre SaaS-Sicherheitsplattform in Betracht ziehen. Sie sorgen auf diese Weise für größere Transparenz und bieten einen robusteren und einfacheren Schutz.

Grundlagen der SaaS-Sicherheit: E-Mail-Sicherheit

Moderne E-Mail-Sicherheit umfasst eine Reihe von Tools, Prozessen und Techniken zum Schutz von E-Mail-Konten und -Inhalten vor heimtückischen Angriffen und unberechtigtem Zugriff. Zu den gebräuchlichsten Arten von E-Mail-Sicherheitstechnologien gehören:

- **Secure Email Gateways (SEG):** SEG verarbeiten und filtern den SMTP-Traffic und verlangen von Unternehmen, dass sie ihren MX-Eintrag ändern, um auf ihren Mail Transfer Agent zu verweisen.
- **Cloudbasierte E-Mail-Sicherheit (Cloud Email Security – CES):** Bei CES werden E-Mail-Inhalte (über API-Zugang zu cloudbasierten E-Mail-Anbietern) analysiert, ohne dass der MX-Eintrag geändert werden muss. (Hinweis: Gartner bezeichnet diese Kategorie als „ICES“ oder „integriertes CES.“)
- **Domain-based Message Authentication Reporting and Conformance (DMARC):** Bei DMARC erfolgt die Authentifizierung von E-Mails, indem die Einträge für das Sender Policy Framework (SPF) und DomainKeys Identified Mail (DKIM) einer Domain überprüft werden. Innerhalb dieses Systems werden E-Mails, die SPF- oder DKIM-Prüfungen nicht bestehen, als Spam markiert oder daran gehindert, den beabsichtigten Empfänger zu erreichen.
- **E-Mail-Datenschutz (Email Data Protection – EDP):** EDP-Lösungen verwenden Verschlüsselung, um versehentlichen Datenverlust und unbefugten Zugriff auf E-Mail-Inhalte zu verhindern.

---

[6] Gartner, „Market Guide for Email Security.“ Analysten: Mark Harris, Peter Firstbrook, Ravisha Chugh, Mario de Boer. 7. Oktober 2021. Gartner.

Die aktuellen Herausforderungen der E-Mail-Sicherheit

Ursprünglich wurden E-Mails über Softwareplattformen vor Ort bereitgestellt, doch inzwischen erfolgt die Bereitstellung zunehmend über cloudbasierte Systeme. Viele Unternehmen haben sich für Produktivitätssuites mit vielen Funktionen wie Microsoft 365 und Google Workspace entschieden, die es Nutzern ermöglichen, effektiver zu arbeiten und zu kooperieren.

Da es E-Mails schon seit langem gibt, kennen selbst ungeübte Nutzer einige der häufigsten Bedrohungen, die ihnen bei dieser Technologie begegnen können – darunter verdächtige Nachrichten, schädliche Links und mehr. Die Angreifer haben daher ihre Strategien weiterentwickelt, um die Unterscheidung zwischen legitimen und böswilligen Nachrichten zu erschweren. Diese gemischten Bedrohungen nutzen mehrere Kommunikationskanäle, um legitim zu erscheinen (z. B. Vishing, Smishing usw.), und verleiten Nutzer oft erfolgreich dazu, sensible Informationen preiszugeben.

Die zunehmende E-Mail-Nutzung macht Unternehmen auch angreifbar: Sobald ein Angreifer Zugriff auf das E-Mail-Konto einer Person hat, ist es für ihn oft ein Leichtes, sich lateral innerhalb eines Unternehmens zu bewegen und vertrauliche Daten zu kompromittieren oder zu stehlen. Cloudbasierte E-Mail-Anbieter stellen zwar in begrenztem Umfang integrierte Sicherheitsfunktionen zur Bekämpfung gängiger Bedrohungen wie Spam, Malware und Phishing bereit, sind aber notorisch schlecht gegen Angriffe von kompromittierten internen Absendern gerüstet, die sich lateral von Posteingang zu Posteingang bewegen.

Um diese Bedrohungen zu bekämpfen, entwickeln sich auch die E-Mail-Sicherheitslösungen weiter. Native cloudbasierte E-Mail-Plattformen bieten ein Grundniveau an integrierten Sicherheitsfunktionen, die gängige Spam- und Malware-Angriffe bewältigen können.

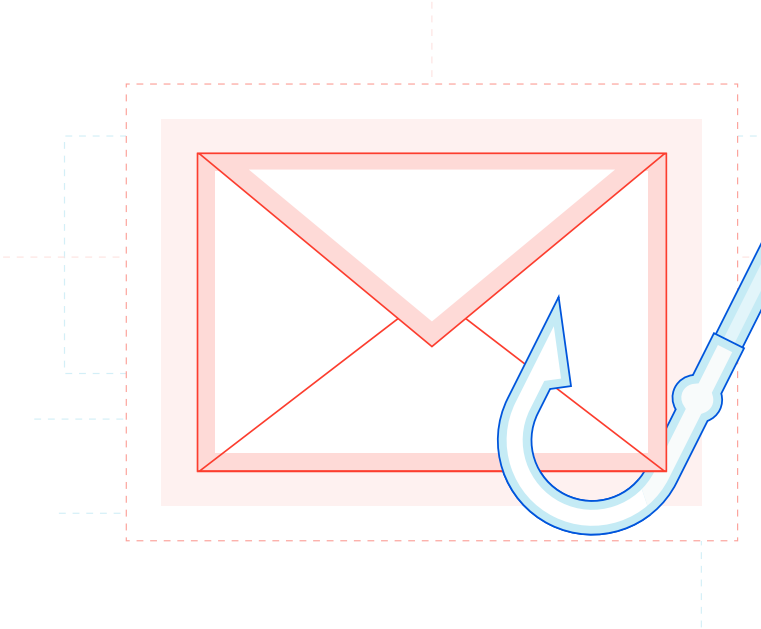
Gartner geht davon aus, dass sich 2023 mindestens 40 % aller Firmen auf diesen integrierten Schutz verlassen werden, anstatt separate Tools wie SEG zu verwenden[7].

Viele Unternehmen entscheiden sich für eine Vereinfachung ihres E-Mail-Sicherheitssystems, indem sie auf das SEG verzichten und stattdessen nach Sicherheitsangeboten suchen, die fortgeschrittene Phishing- und BEC-Angriffe unterbinden und sich über APIs eng in ihre cloudbasierte E-Mail-Umgebung integrieren lassen. Gartner schätzt, dass 2023 20 % der Anti-Phishing-Lösungen über eine API-Integration mit E-Mail-Plattformen bereitgestellt werden[8].

[7] Gartner, „Market Guide for Email Security." Analysten: Mark Harris, Peter Firstbrook, Ravisha Chugh, Mario de Boer. 7. Oktober 2021. Gartner. [8] Gartner, „Market Guide for Email Security."

Die Schwierigkeiten bei der Implementierung und Integration von E-Mail-Sicherheit

Diese integrierten Funktionen geben Unternehmen zwar eine gewisse Sicherheit, reichen aber zur Abwehr moderner E-Mail-Bedrohungen bei weitem nicht aus. Ganze Kategorien von Angriffen – etwa Spear-Phishing und BEC – erfordern spezielle Sicherheitsplattformen, die von E-Mail-Dienstleistern nicht angeboten werden. Hinzu kommt, dass veraltete E-Mail-Sicherheitslösungen nicht auf die Skalierung, die Bewältigung von cloudnativen Herausforderungen oder das Abfangen von sehr gezielten Angriffen ausgelegt sind.



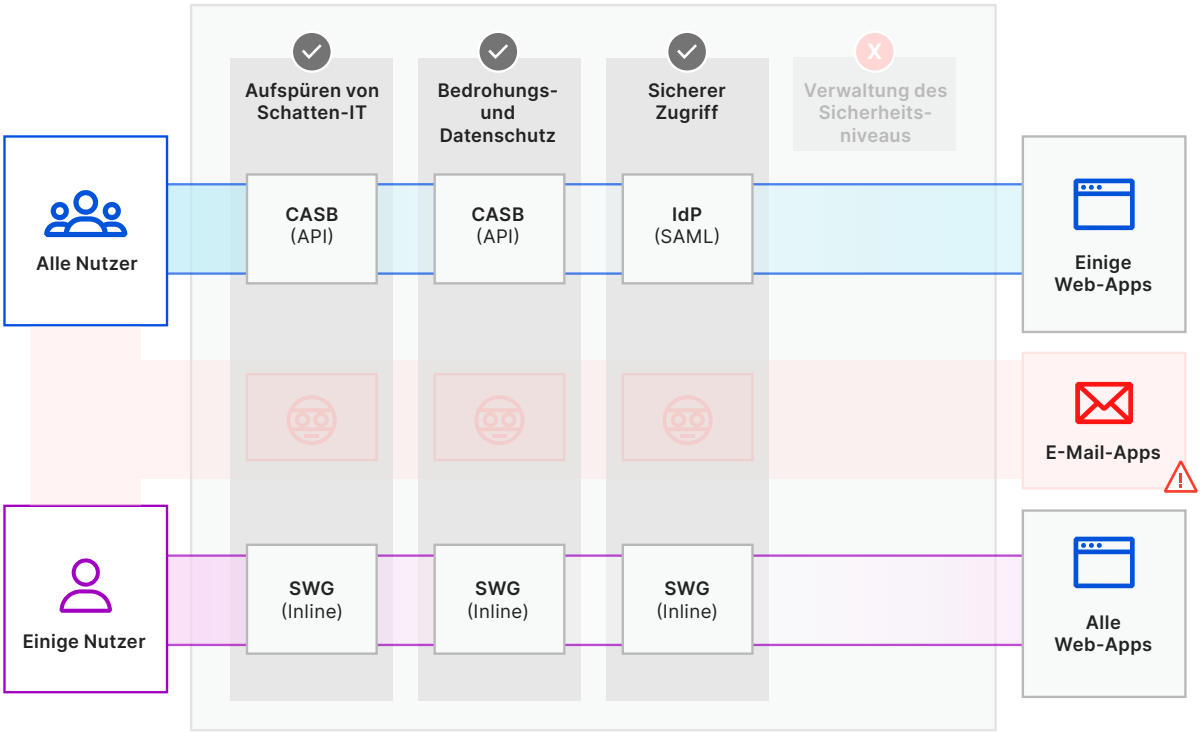
Selbst wenn Sicherheitsteams E-Mail-Sicherheitstools für moderne Bedrohungen ausfindig machen, können sie auf zusätzliche Probleme stoßen: komplexe Konfigurationsanforderungen, zeitaufwändige Bereitstellungsprozesse und mühsame Richtlinienpflege. Zum Beispiel lassen sich SEG-Produkte bekanntermaßen nur schwer gegen E-Mail-Angriffe einsetzen, da es nicht machbar (oder skalierbar) ist, eine immer länger werdende Liste von Richtlinien zu pflegen, um jede Angriffsvariante zu neutralisieren. Für das Erkennen raffinierter Angriffe müssen Algorithmen in einem Umfang eingesetzt werden, den nur cloudnative Dienste bewältigen können.

Um die E-Mail-Systeme von Unternehmen vor diesen Angriffen zu schützen – ohne die Sicherheitsteams zu überlasten, mehrere veraltete Hardwareprodukte miteinander zu kombinieren oder sich darauf zu verlassen, dass die Mitarbeitenden jede böswillige Nachricht abfangen – benötigen Unternehmen einen Zero Trust-Ansatz, der cloudnative E-Mail-Sicherheitsfunktionen integriert und den der E-Mail-Kommunikation gewährten impliziten Vertrauensvorschuss reduziert.

Ein besserer Ansatz für SaaS-Sicherheit

SaaS-Anwendungen, von Kommunikationsplattformen bis hin zu E-Mail-Zustellungssystemen, machen einen großen Teil der heutigen Geschäftsabläufe aus. Aber diese Anwendungen vor immer komplexeren Bedrohungen zu schützen, kann für Sicherheitsteams ein Alptraum sein. Sie müssen sich oft mit mehreren Tools herumschlagen, die nicht für eine native Integration untereinander konzipiert sind oder die keinen Überblick über die gesamte SaaS-Landschaft eines Unternehmens bieten.

Herkömmliches SaaS-Sicherheitsmodell

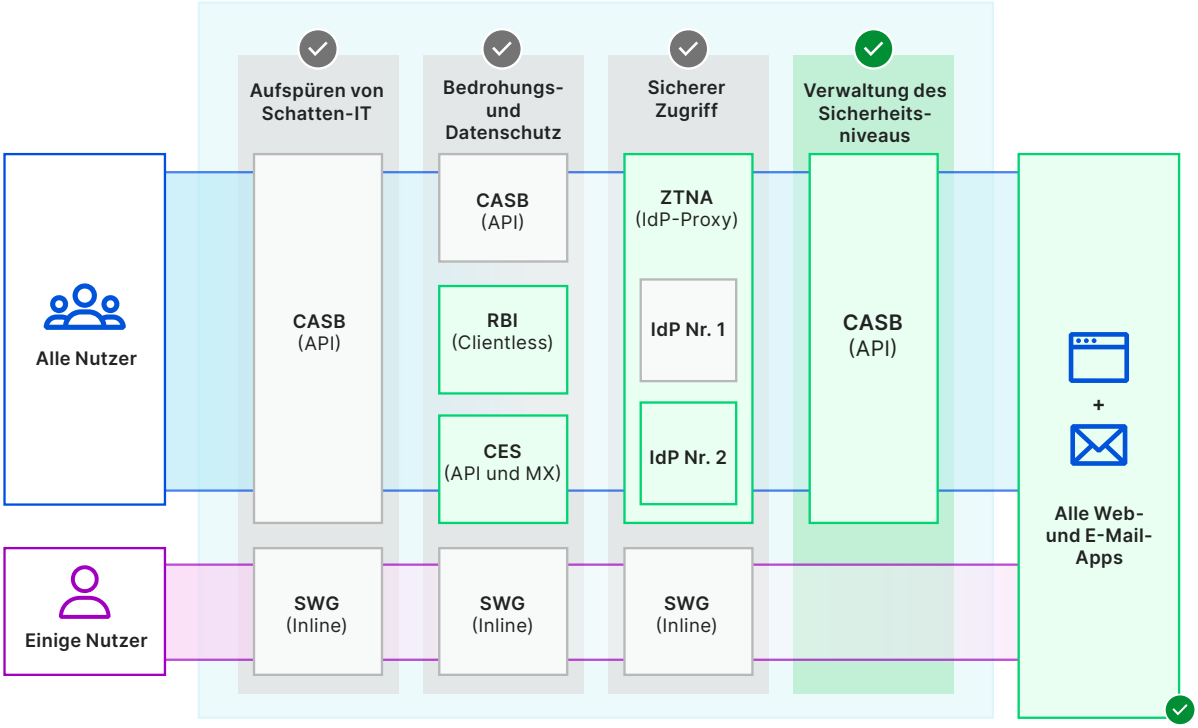


SWG = Secure Web Gateway | CASB = Cloud Access Security Broker | IdP = Identity Provider (Identitätsanbieter)

Während Anbieter immer robustere SaaS-Sicherheitstools entwickelten, mussten IT- und Sicherheitsteams diese branchenführenden Lösungen miteinander verknüpfen, um ihre Anwendungen und Daten zu schützen. Dies erforderte oft einen erheblichen Aufwand an Zeit und internen Ressourcen für die Implementierung und Verwaltung. Und während Einzellösungen in der Lage waren, Bedrohungen auf individueller Ebene zu bekämpfen, gab es keine übergreifende Plattform, die mehrere Anbieter unterstützte und Transparenz für das gesamte Unternehmen bot.

Oftmals reichten die herkömmlichen SaaS-Sicherheitsmaßnahmen nicht aus, um den Schutz auf E-Mail-Plattformen auszudehnen. Das machte Unternehmen anfällig für gezielte Angriffe, die geschäftskritische Arbeitsabläufe replizierten, sich als vertrauenswürdige Partner und Nutzer ausgaben und bestehende E-Mail-Klassifizierungssysteme und integrierte Kontrollen leicht umgingen. Und ohne native Integration zwischen diesen Lösungen – oder einen Überblick über die gesamte Bedrohungslandschaft – blieben beim Schutz von Anwendungen vor aktuellen Bedrohungen noch mehr Lücken, die die Sicherheitsteams beheben mussten.

Moderne SaaS-Sicherheit



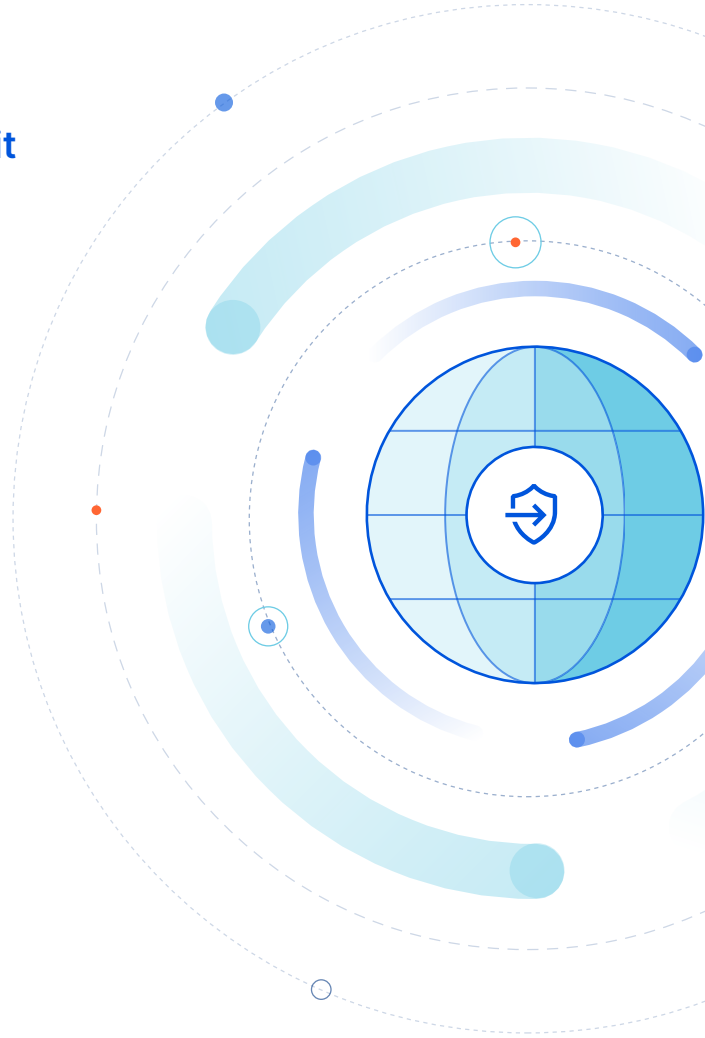
SWG = Secure Web Gateway | CASB = Cloud Access Security Broker | IdP = Identity Provider (Identitätsanbieter) | RBI = Remote Browser Isolation | CES = Cloud Email Security | ZTNA = Zero Trust Network Access

Zur Schließung der Lücken, die herkömmliche SaaS-Sicherheits- und -Verwaltungslösungen hinterlassen haben, benötigen Unternehmen eine moderne Bedrohungsabwehr. Diese muss darauf ausgelegt sein, Anwendungen und Daten von einer einzigen, Internet-nativen Plattform aus zu schützen. Eine entscheidende Komponente dieses modernen Ansatzes ist ein robustes Sicherheitsniveau. Mit dem Sicherheitsniveau sollten Sicherheitsteams besser bestimmen können, wie Nutzer auf kritische Ressourcen zugreifen. Außerdem sollten sie Einblick in und Kontrolle über externe und interne Bedrohungen erhalten.

Anstatt dass Unternehmen gegen einzelne Bedrohungen mit Einzellösungen vorgehen müssen, kann eine SaaS-Sicherheitsplattform Anwendungen scannen, um Anomalien in der Konfiguration, bei den Berechtigungen und bei der gemeinsamen Nutzung zu erkennen. Das versetzt Sicherheitsteams unter anderem in die Lage, den Anwendungszugriff zu verwalten, E-Mail-Angriffe zu bekämpfen, Insider-Bedrohungen und die riskante gemeinsame Nutzung von Daten zu unterbinden.

Dieser Ansatz bietet nicht nur einen robusteren und umfassenderen Schutz für SaaS-Anwendungen, sondern ermöglicht es Unternehmen auch, Zeit bei der Bearbeitung von Tickets zu sparen, Sicherheitsprozesse zu automatisieren und sich auf strategische Initiativen zu konzentrieren – anstatt sich um Datenverluste, Angriffe und manuelle Konfigurationen und Wartung zu sorgen.

Ein Zero Trust-Ansatz für die SaaS-Sicherheit



Wer den richtigen Ansatz für SaaS-Sicherheit entwickeln möchte, muss die modernen SaaS- und cloudbasierten Bedrohungen aus der Vogelperspektive betrachten. Allerdings kann es Sicherheitsteams überfordern, bestehende Lösungen an die Bedürfnisse eines Unternehmens anzupassen. Anstatt Bedrohungen auf individueller Ebene zu bekämpfen – oder sich auf ein Flickwerk aus Einzeltools zu verlassen – benötigen Unternehmen eine Sicherheitsplattform, die vereinfacht und leicht zu verwalten ist. Außerdem muss sie aktuelle Bedrohungen vorhersehen und bekämpfen können.

Sowohl CASB als auch die cloudbasierte E-Mail-Sicherheitsfunktionen sind wesentliche Bestandteile einer SaaS-Sicherheitsstrategie. Sie sind jedoch so konzipiert, dass sie am besten innerhalb einer Zero Trust-Architektur funktionieren – einer Architektur, in der alle Technologien gemeinsam besser funktionieren als einzeln. Bei richtiger Implementierung hilft der Einsatz mehrerer Sicherheitsschichten auch, angrenzende Probleme abzumildern, weil dadurch Sicherheitslücken beseitigt, die Bandbreite des Sicherheitsteams geschont und die Überwachung von Bedrohungen automatisiert werden.

Wie Cloudflare SaaS-Apps schützt

Cloudflare bietet die einfachste Lösung zum Schutz Ihrer gesamten SaaS-Landschaft. Unternehmen können kontrollieren, wie ihre Nutzer auf wichtige Ressourcen zugreifen, wie sie diese Ressourcen vor externen oder internen Angriffen schützen und wie sie Risiken in Echtzeit überwachen und bekämpfen.

*Tragen Sie sich in unsere DLP-Warteliste ein

SaaS-Anwendungen mit der Zero Trust-Lösung von Cloudflare absichern

Zur Absicherung von Daten während der Übertragung platziert Cloudflare Zero Trust-Kontrollen für Zugriff (ZTNA), Gateway (SWG) und Browserisolierung (RBI) vor Cloud- und SaaS-Anwendungen, um eine Inline-CASB-Bereitstellungsarchitektur zu unterstützen und zu betreiben.

Zum Schutz von ruhenden Daten innerhalb von SaaS-Anwendungen scannen Integrationen stark genutzte Anwendungen kontinuierlich auf Sicherheitslücken und potenzielle Bedrohungen hin. Diese Integrationen lassen sich einfach konfigurieren und sind API-gesteuert.

E-Mail-Sicherheit von Cloudflare Area 1 mit Zero Trust kombinieren

Cloudflare Area 1 Email Security ist ein repräsentativer ICES-Anbieter, der Unternehmen mehr Flexibilität bietet – je nach ihren E-Mail-Sicherheitsanforderungen. Die Integration erfolgt über eine API und die Lösung fungiert als Gateway zur Verifizierung, Filterung, Inspektion und Isolierung des E-Mail-Traffics mittels MX-Eintragsänderungen.

Area 1 spürt im Internet Angriffsinfrastrukturen und Phishing-Kampagnen auf und schützt Kunden so vor Phishing-Angriffen, noch bevor diese den Posteingang der Empfänger erreichen.

Wenn Sie mehr darüber erfahren möchten, wie Cloudflare die Sicherheit von SaaS-Anwendungen unterstützt, werden Sie hier fündig: https://www.cloudflare.com/de-de/products/zero-trust.

Quellen

1. Gartner, „Forecast Analysis: Information Security and Risk Management, Worldwide.“ Analysten: Shailendra Upadhyay, Mark Driver, Christian Canales, Ruggero Contu, Lawrence Pingree, Elizabeth Kim, John A. Wheeler, Nat Smith, Rahul Yadav, Swati Rakheja, Dave Messett, Mark Wah, Shawn Eftink. 12. August 2021. Gartner.

2. Gartner, „Predicts 2022: Consolidated Security Platforms Are the Future.“ Analysten: Charlie Winckless, Joerg Fritsch, Peter Firstbrook, Neil MacDonald, Brian Lowans. 1. Dezember 2021. Gartner.

4. Gartner, „Hype Cycle for Cloud Security, 2021.“ Analysten: Tom Croll, Jay Heiser. 27. Juli 2021. Gartner.

6. Gartner, „Market Guide for Email Security.“ Analysten: Mark Harris, Peter Firstbrook, Ravisha Chugh, Mario de Boer. 7. Oktober 2021. Gartner.

7. Gartner, „Market Guide for Email Security.“ Analysten: Mark Harris, Peter Firstbrook, Ravisha Chugh, Mario de Boer. 7. Oktober 2021. Gartner.

8. Gartner, „Market Guide for Email Security.“ Analysten: Mark Harris, Peter Firstbrook, Ravisha Chugh, Mario de Boer. 7. Oktober 2021. Gartner.

+49 89 2555 2276 | enterprise@cloudflare.com | www.cloudflare.com/de-de/

REV:BDES-3303.2022JUN24