Leitfaden für Käufer:

Mehr Sicherheit mit Next-Generation CASB

Inhalt

Rasante Zunahme der SaaS-Anwendungen in Unternehmen

SaaS-Anwendungen verändern die Arbeitsweise in Unternehmen und durch die Pandemie hat sich ihre Verbreitung zusätzlich beschleunigt.

Moderne Unternehmen versuchen, möglichst schnell äußerst effizient und produktiv zu werden, um mit den Entwicklungen Schritt zu halten und ihren Wettbewerbsvorteil auszubauen. Dazu nutzen sie Software-as-a-Service-Anwendungen (SaaS), die einfach, intelligent, überall verfügbar und anwenderfreundlich sind.

Vor diesem Hintergrund ist es kaum verwunderlich, dass der Markt für cloudbasierte SaaS-Lösungen, zum Beispiel von Salesforce, HubSpot, Google Apps, Zoom und anderen Anbietern, weiterhin wächst. SaaS ist der erste cloudbasierte Service, der sich umfassend durchgesetzt hat. Laut Gartner wird SaaS auch weiterhin der größte Posten in den IT-Budgets weltweit bleiben.

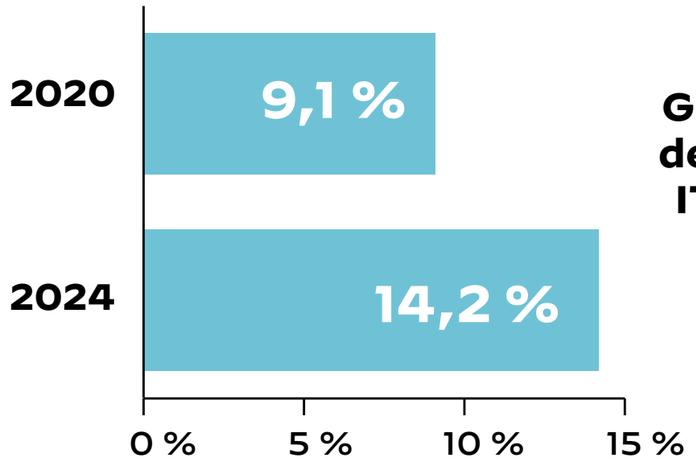
Gartner schätzte, dass die Ausgaben von Endbenutzern für Public-Cloud-Services, die 2020 bereits 270 Milliarden US-Dollar betrugen, 2021 noch einmal um **23,1 Prozent** wachsen und damit **332,3 Milliarden US-Dollar** erreichen würden. SaaS-Unternehmensanwendungen sind in diesem Zusammenhang immer noch das größte Marktsegment und werden 2022 vermutlich auf **145,3 Milliarden US-Dollar** ansteigen.

50 %

Zunahme der Gesamtausgaben für SaaS-Produkte pro Unternehmen im Jahr 2020

30 %

Zunahme der genehmigten Apps pro Unternehmen im Jahr 2020 im Vergleich zum Vorjahr



Geschätzte Zunahme des Cloud-Anteils der IT-Gesamtausgaben weltweit bis 2024

Die Cloud wird auch in Zukunft ein dynamischer und innovativer Markt bleiben. Unternehmen werden neue Technologien wie Container, Virtualisierung und Edge-Computing zur Verfügung stehen, da diese verstärkt eingesetzt und damit zum Mainstream werden.

Quellen:

- Blissfully SaaS Trends Annual Report, 2020
- „Gartner Forecasts Worldwide Public Cloud End-User Spending to Grow 23% in 2021“

Die unkoordinierte Nutzung zahlreicher SaaS-Anwendungen verursacht Chaos

Da SaaS-Anwendungen in zahlreichen unterschiedlichen Abteilungen eingeführt wurden, herrscht nun Chaos, das Unternehmen nur schwer wieder in den Griff bekommen.

SaaS bietet enorme Vorteile für Unternehmen aller Größen und daher setzen inzwischen fast alle Abteilungen auf entsprechende Anwendungen. Neben IT- und Sicherheitsteams gehören dazu zum Beispiel Entwickler- und Produktteams, der Kundenservice, DevOps und die Personal-, Finanz-, Marketing- und Vertriebsabteilung.

Je mehr SaaS-Anwendungen implementiert werden, desto unübersichtlicher werden jedoch auch die Zuständigkeiten und die Verwaltung. Anfänglich war es meist die Aufgabe der IT-Teams, die Technologie für das gesamte Unternehmen auszuwählen, und sie kümmerten sich auch um die damit verbundenen Herausforderungen, wie Budgetierung, Anschaffung, Implementierung, Sicherheit und Außerbetriebnahme.

Die zunehmende Dezentralisierung von SaaS hat die IT-Teams überrascht und macht es ihnen fast unmöglich, die verwendeten SaaS-Apps zu erfassen, zu verwalten und zu schützen. Im Durchschnitt sind Hunderte genehmigter Anwendungen in Unternehmen im Einsatz und es gibt Tausende Aufrufe von Mitarbeitern, die gesichert werden müssen.

SaaS-Ausgaben und -Nutzungsstatistiken nach Marktsegment für das Jahr 2020

SaaS-Statistiken (pro Unternehmen)	Insgesamt	Großunternehmen	Mittelständische Unternehmen	Kleine Unternehmen
Ausgaben	Anstieg um 50 %	4,16 Mio. $	2,47 Mio. $	202.000 $
Einzelne SaaS-Apps	137	288	185	182
App-Aufrufe von Mitarbeitern	–	21.580	4.406	624
Fluktuation bei SaaS-Apps	30 %	46 %	29 %	35 %
Anzahl der doppelten Apps	3,6	7,6	5,8	2,3
Anzahl der nicht verwendeten App-Subscriptions	2,6 (Anstieg um 100 %)	7,1	4,3	1,4
Anzahl der Rechnungsempfänger pro Unternehmen	–	98	32	10

Quelle:

- Blissfully

Die Schatten-IT: weitverbreitet und gefährlicher, als viele vermuten

Datensicherheit ist nur möglich, wenn Unternehmen die Nutzung nicht genehmigter SaaS-Apps überwachen und unter Kontrolle bringen.

Nutzen Mitarbeiter verschiedener Teams für ihre Arbeit und für private Zwecke lieber eigene SaaS-Lösungen, entsteht schnell eine sogenannte **Schatten-IT**, die in der Regel aus nicht genehmigten SaaS-Anwendungen und anderen Cloud-Services besteht. Ein weiteres großes Risiko sind Mitarbeiter, die zu Hause in nicht gesicherten Netzwerken arbeiten. Viele Mitarbeiter umgehen das Unternehmens-VPN, um diese Apps direkt aufzurufen, und andere greifen auf persönlichen, nicht verwalteten Geräten auf Unternehmensressourcen zu. Dadurch wird es wesentlich schwieriger, die Schatten-IT aufzudecken und zu verhindern.

Die Schatten-IT beeinträchtigt die Kontrolle der IT-Teams über die Datensicherheit

Das IT-Team hat keine Kontrolle darüber, ob sensible und vertrauliche Unternehmensdaten über die Tausenden Cloud-Services und -Anwendungen verbreitet werden, die weder geprüft noch genehmigt wurden. Nicht verwaltete Datenrepositorys außerhalb der Sicherheitsmaßnahmen des Unternehmens vergrößern die Angriffsfläche in einem nicht abschätzbaren Ausmaß.

Die Schatten-IT verstößt gegen die Complianceanforderungen für Unternehmensdaten

Da die Schatten-IT nicht vom IT-Team verwaltet wird, hat es meist auch keinen Überblick über potenzielle Complianceverstöße der nicht genehmigten Apps und der Daten, die damit übertragen oder darin gespeichert werden. Aus diesem Grund müssen zusätzliche Auditpunkte eingerichtet und der Compliancenachweis ausgeweitet werden.

In der Schatten-IT halten sich Mitarbeiter nicht an Best Practices für die Sicherheit

Die meisten Mitarbeiter haben zwar keine bösen Absichten, wenn sie Anwendungen der Schatten-IT nutzen, aber diese Apps stellen dennoch ein großes Risiko für die Cybersicherheit des Unternehmens dar, denn sie vergrößern die Gefahr von Datenlecks und schädlichen Insideraktivitäten und können als Einfallstore für Malware und andere Bedrohungen dienen.

Gartner schätzt, dass die Schatten-IT 30 bis 40 Prozent der IT-Gesamtausgaben in großen Unternehmen ausmacht. Das bedeutet, dass fast die Hälfte des IT-Budgets für Technologie aufgewendet wird, die nicht von der IT-Abteilung genehmigt wurde. Außerdem wird 2022 ein Drittel der erfolgreichen Angriffe auf Unternehmen die Schatten-IT ausnutzen.

Quelle:

- „Don't Let Shadow IT Put Your Business At Risk", Smarter with Gartner

Drei entscheidende Fragen für Unternehmen

Weltweit stellt die zunehmende Cloud-Nutzung Entscheidungsträger in Unternehmen aller Größen vor enorme Herausforderungen in Bezug auf die Cloud-Sicherheit.

Anwendungen

Welche Apps werden von Mitarbeitern wie genutzt?

Unternehmen, in denen die Anzahl der mobilen Mitarbeiter stark zugenommen hat, setzen auf eine ehrgeizige Multi-Cloud-SaaS-Strategie. Doch da das Nutzungsverhalten der mobilen Mitarbeiter in Bezug auf SaaS-Anwendungen kaum überprüft wird, sind die Vertraulichkeit und der Datenschutz sensibler Informationen nicht gewährleistet und die Risikogefahr steigt.

Daten

Wie können wir sensible Daten in der Cloud schützen?

Einige Datentypen müssen vielen unterschiedlichen Benutzern zur Verfügung stehen, aber der Zugriff auf sensible Daten sollte auf eine kleine Gruppe beschränkt werden. Aufgrund der diversen Anforderungen an die Datennutzung in den verschiedenen Teams wird der Datenschutz zu einer wahren Herausforderung.

Benutzer

Wie können wir den Zugriff auf SaaS-Apps kontrollieren und Benutzer vor Bedrohungen schützen?

Cloud-Serviceanbieter stellen meist auch einige Sicherheits- und Compliancefunktionen bereit, doch das bedeutet nicht, dass sich Enterprise-Kunden nicht mehr um den Schutz der Daten, Benutzer und Apps vor Bedrohungen kümmern müssen. Der sensible Punkt dabei ist die Frage, wer für die Sicherheit in der Cloud zuständig ist – der Kunde oder der Serviceanbieter?

SaaS-Sicherheitsprobleme, die CISOs schlaflose Nächte bereiten

Obwohl SaaS einen Mehrwert bietet, verzichten viele Unternehmen aus Sorge vor Sicherheitsproblemen bisher auf den Wechsel von On-Premises-Rechenzentren zu SaaS-Lösungen.

Zwar beschleunigen innovative SaaS-Lösungen das Unternehmenswachstum erheblich, aber sie bringen auch diverse Probleme mit sich. Wenn es um die Sicherheit und den Schutz von SaaS-Anwendungen geht, müssen sich die CISOs mit zahlreichen Unwägbarkeiten abfinden. Cloudbasierte SaaS-Lösungen sorgen für Unbehagen, da CISOs ein gewisses Maß an Kontrolle und Transparenz an den SaaS-Anbieter abtreten müssen. Dieser Schritt fällt ihnen besonders schwer, wenn davon vor allem Daten betroffen sind. Außerdem müssen sich CISOs damit abfinden, dass es je nach App unterschiedliche Sicherheitsgrade gibt und einige sogar überhaupt nicht geschützt sind, sodass die SaaS-Sicherheitsstrategie inkonsistent wird.

Die größten Sicherheitsprobleme bei SaaS-Anwendungen

Schatten-IT

Nicht autorisierte Apps, die ohne Wissen und Genehmigung des IT-Teams genutzt und verwaltet werden

Offenlegung von Daten

Die versehentliche Offenlegung von Daten und das Risiko des Datendiebstahls

Benutzerverhalten

Fahrlässige Weitergabe von Daten, Insider mit böswilligen Absichten und keine Möglichkeiten für IT-Teams, das Benutzerverhalten zu kontrollieren

Mangelnde Transparenz

Kein Überblick über die von den Apps gespeicherten oder übermittelten Daten – von sensiblen Informationen bis zu schädlichen Dateien

Bedrohungen und Malware

Komplexe Bedrohungen und Malware, die SaaS-Anwendungen, Benutzer und Daten gefährden

Compliancevorschriften

Das IT-Team kann die Compliancevorschriften in den SaaS-Umgebungen nicht umsetzen.

Größte SaaS-Bedrohungen aus Sicht der CISOs

Malwareinfektionen **77 %**

Datenverlust oder -diebstahl **72 %**

Diebstahl von Anmeldedaten oder Kontomanipulation **69 %**

Datenlecks in der Cloud **45 %**

Angriff auf das Unternehmensnetzwerk über die Cloud **35 %**

Anfälligste SaaS-Anwendungen

Apps für das Hosten und Übertragen von Dateien **72 %**

Cloudbasierte E-Mail-Apps **57 %**

Instant-Messaging-Apps **52 %**

Apps für die Kommunikation und Zusammenarbeit **42 %**

Videokonferenzen **35 %**

Projektmanagement **23 %**

Quelle:

- Cybersecurity Insiders, The CISO Cloud SaaS Security Report, 2020

Grenzen der konventionellen CASB-Ansätze

Sie weisen mehr Probleme als Potenzial auf. Um mit der rasanten Zunahme an SaaS-Anwendungen mithalten zu können, müssen Unternehmen ihre CASB-Strategie weiterentwickeln.

CASB sind zweifellos eine wichtige Komponente der Sicherheitsstrategie von Unternehmen und speziell für den Schutz cloudbasierter Anwendungen und der verarbeiteten sensiblen Daten. Doch die erste Generation der CASB-Lösungen weist einige grundlegende Nachteile auf, die behoben werden müssen.

1 **Kein vollständiger Überblick über Apps:** CASB der ersten Generation sind auf HTTP/S ausgerichtet und übersehen daher mehr als die Hälfte des Datenverkehrs von nicht webbasierten Anwendungen. Außerdem nutzen sie für die App-Erkennung immer noch ausschließlich statische Datenbanken mit Anwendungssignaturen und die rückwirkende Identifizierung über Anfragen. Doch mit diesem Ansatz lassen sich neue SaaS-Apps weder rechtzeitig identifizieren noch blockieren, um Risiken vorzubeugen. Diese CASB stellen auch keine APIs für die sicheren, modernen Apps für die Zusammenarbeit bereit, die von mobilen Mitarbeitern genutzt werden.

2 **Unzureichender Datenschutz:** Ihre Datenschutzmaßnahmen sind nicht auf die Menge an sensiblen Daten und deren rasanten Verbreitung ausgelegt. Die DLP-Funktionen (Data Loss Prevention) basieren überwiegend auf regulären Ausdrücken und traditionellem Datenfingerprinting und sind daher langsam und nicht sehr genau. Das größte Problem ist allerdings, dass sie Datenlecks in modernen Apps für die Zusammenarbeit, wie Slack, Teams und Zoom, nicht erkennen können, da diese neue Kommunikationsmethoden mit kurzen und nicht strukturieren Nachrichten verwenden.

3 **Schwache Sicherheitsmaßnahmen:** Sicherheit war in älteren CASB leider eine reine Formsache. Die meisten Anbieter konnten kritische Bedrohungen, unbekannte Malware und Datenlecks kaum verhindern und boten in der Regel nur Sandboxing-Tools von Drittanbietern zur Bedrohungserkennung. Außerdem bietet der Inline-Proxy-Ansatz nur einen Überblick über HTTP/S-Datenverkehr, sodass Kunden nicht umfassend geschützt sind.

4 **Inkonsistente Sicherheitsrichtlinien:** Die isolierten CASB-Lösungen zwingen Unternehmen, unterschiedliche Bereitstellungsmethoden und Technologien für Hauptsitz, Filialen und mobile Mitarbeiter zu implementieren. Doch dadurch wird die Sicherheitsstrategie uneinheitlich und kann Lücken aufweisen. Da diese CASB nicht mit der restlichen Sicherheitsinfrastruktur eines Unternehmens verbunden sind, müssen für sie auch Netzwerkänderungen vorgenommen und eine komplexe Architektur eingerichtet werden. Dadurch wird die Verwaltung in einem hybriden Arbeitsmodell ineffizient und aufwendig.

Jetzt ist der richtige Zeitpunkt für den Wechsel zu Next-Generation CASB. Sie werden in die vorhandene Sicherheitsinfrastruktur integriert und bieten den notwendigen Überblick und die erforderliche Kontrolle über alle Anwendungen, Benutzer und Daten. So behalten Sie auch die steigende Anzahl der SaaS-Anwendungen im Griff.

5 unverzichtbare Merkmale eines Next-Generation CASB

1 Der Next-Generation CASB muss cloudfähig sein und die rasante Zunahme an SaaS-Anwendungen bewältigen können

Nur mit einem umfassenden Überblick über die SaaS-Umgebung können Sie sich ein Bild von der Cloud- und Datensicherheit machen. Wenn cloudbasierte Lösungen außerhalb des Zuständigkeitsbereichs des IT-Teams genutzt werden, besteht die Gefahr, dass die Unternehmensrichtlinien für Governance und Risikominimierung nicht mehr befolgt werden. Ein Next-Generation CASB sollte automatisch alle genehmigten und nicht genehmigten Apps erkennen und schützen, einschließlich SaaS-Apps für die Zusammenarbeit, um mit der rasanten Zunahme an SaaS-Anwendungen Schritt zu halten.

Außerdem sollte er den gesamten Datenverkehr sowie alle Ports und Protokolle scannen, automatisch neue Apps erfassen und zahlreiche APIs für SaaS-Apps unterstützen, einschließlich moderner Apps für die Zusammenarbeit wie Slack® und Teams. Er muss genaue und anpassbare Risikobewertungen und -attribute für alle Apps bereitstellen, um das Benutzerverhalten zu überwachen und riskante Aktivitäten zu verhindern, bevor die Apps manipuliert werden können. Ein umfassender Echtzeitüberblick über SaaS-Anwendungen und Risikobewertungen helfen dem IT-Team, neue SaaS-Apps automatisch zu erkennen, risikobasierte Kontrollen für bekannte und unbekannte Apps einzurichten und die Datenausschleusung zu verhindern.

Achten Sie für einen cloudfähigen CASB auf die folgenden Funktionen:

- ✓ Umfassende Sicherheitsmaßnahmen für alle SaaS-Apps, einschließlich zahlreicher API-basierter Sicherheitsfunktionen für eine größere Kontrolle über genehmigte SaaS-Anwendungen
- ✓ Fortlaufende App-Erkennung durch eine Anwendungs-ID-basierte Cloud-Engine für Apps der Schatten-IT
- ✓ Automatisierte Risikoklassifizierung mit über 30 Attributen zur Identifizierung der Risiken für das Unternehmen
- ✓ Funktionen für das zeitgleiche Tagging mehrerer Anwendungen, um Apps durch Kennzeichnung des Status und anpassbarer Tags besser klassifizieren zu können
- ✓ Integrierte Inlinekontrollen und -richtlinien, die problemlos auf allen Geräten und für alle Benutzer angewendet werden können

2 Der Next-Generation CASB muss eine einfache Bereitstellung und eine schlanke Architektur bieten

In modernen, heterogenen Unternehmen mit mehreren Standorten und mobilen Benutzern erweist sich der Ansatz konventioneller CASB-Lösungen zunehmend als schwer skalierbar, teuer und daher langfristig nicht vertretbar. Die Bereitstellung von Standard-CASB ist schwierig, da sie ein unnötiges Cloud-Gateway (meist einen Proxy) dazwischenschalten und eine komplexe Weiterleitung des Datenverkehrs von Datenloggern wie Netzwerkfirewalls und PAC-Agenten (Proxy Auto-Configuration) erfordern. Außerdem benötigen sie einen Active Directory Connector, um Richtlinien nach Benutzer-ID oder Active Directory-Gruppe durchsetzen zu können. Gibt es mehrere Standorte, muss diese Infrastruktur an jedem dupliziert werden. Da immer mehr Mitarbeiter mobil sind, müssen zusätzliche Endpunkte mit PAC-Dateien oder weiteren VPN-Agenten bereitgestellt werden, um deren Datenverkehr über den cloudbasierten Proxy zu leiten. In manchen Fällen ist eine Proxy-Architektur unverzichtbar, aber für alle anderen ist sie äußerst umständlich einzurichten und sollte nicht die einzige Lösung sein.

Ein Next-Generation CASB sollte alle zwischengeschalteten Komponenten überflüssig machen und das IT-Team entlasten, da die zusätzlichen Infrastrukturinvestitionen entfallen. Sicherheitsteams können dann die Abläufe vereinfachen, indem die SASE- und die CASB-Lösung zusammen auf einer Plattform für Sicherheit, zuverlässige Netzwerkverbindungen und Datenschutz in allen Umgebungen sorgen. Außerdem sollte der CASB in die vorhandene Next-Generation Firewall eingebunden werden können, um eine umfassende und integrierte SaaS-Sicherheitsinfrastruktur und -kontrolle zu ermöglichen.

Achten Sie für eine einfache Bereitstellung und Nutzung auf die folgenden Funktionen:

- ✓ Vollständig in der Cloud verwaltete Lösung mit flexiblen Bereitstellungsoptionen zur einfachen Unterstützung eines hybriden Arbeitsmodells
- ✓ Ein Dashboard für einen umfassenden Überblick über alle Richtlinien für die Cloud-Anwendungen
- ✓ Einfache Konfiguration dank optimierter Arbeitsabläufe und ML-gestützter Automatisierung
- ✓ Native Integrationen für einen automatischen Überblick über den aktuellen Status der Schatten-IT
- ✓ Vorkonfigurierte Integrationen mit Funktionen für den Schutz vor Datenverlust und Bedrohungen sowie Inlinekontrollen zur Durchsetzung von Richtlinien. Keine zusätzlichen PAC-Dateien oder Proxys zur Bereitstellung erforderlich.

3 Der Next-Generation CASB muss sowohl bekannte als auch unbekannte Bedrohungen proaktiv und zuverlässig erkennen

Da SaaS-Apps so vielfältig sind, entstehen heterogene Umgebungen mit Hunderten Apps von verschiedenen Cloud-Anbietern – und damit zahlreichen potenziellen Angriffspunkten. Für zuverlässige SaaS-Sicherheitsmaßnahmen benötigen Sie aussagekräftige Informationen zur Erkennung und Abwehr relevanter Bedrohungen. Bei dem Next-Generation CASB sollte es sich um eine bewährte Lösung handeln, die Zero-Day-Bedrohungen mithilfe von nativ integrierten Inline-ML-Modellen verhindern kann – auch ohne Tools von Drittanbietern. Er sollte neue und unbekannte Bedrohungen sofort durch umgehungsresistente Signaturen abwehren und die neuen Informationen in Sekundenschnelle weltweit weitergeben. Auf diese Weise werden die Sicherheitsmaßnahmen schneller verbreitet als die Infektionen. Die CASB-Lösung sollte über eine traditionelle Malwareanalyse hinausgehen und Daten einer Threat-Intelligence-Engine abrufen können, die per Crowdsourcing erfasst wurden. So lassen sich Bedrohungen schnell und einfach mit Inlinesicherheitsfunktionen für Zero-Day-Angriffe in Echtzeit abwehren. Dieser neue Ansatz sorgt für ein hohes Sicherheitsniveau und eine zuverlässige Abwehr ungewöhnlicher SaaS-Bedrohungen im gesamten Netzwerk. So spart das IT-Team Zeit und Aufwand.

Achten Sie für eine zuverlässige Abwehr von Bedrohungen auf die folgenden Funktionen:

- ✓ Fortlaufender Schutz vor Malware und Bedrohungen dank einer cloudbasierten Analyse- und Präventions-Engine, die unbekannte dateibasierte Bedrohungen erkennen und abwehren kann
- ✓ Abläufe zur automatisierten Behebung von Sicherheitsvorfällen
- ✓ Überwachung der Benutzeraktivitäten und Einleitung entsprechender Maßnahmen, sofern notwendig

4 Die CASB-Lösung muss über äußerst präzise Erkennungstechniken für einen umfassenden Datenschutz und die Erfüllung der Complianceanforderungen verfügen

Die meisten CASB-Lösungen bieten grundlegende Sicherheitsfunktionen für Datenschutz und Compliance, die auf Cloud-Umgebungen beschränkt sind. Enterprise-DLP-Lösungen (Data Loss Prevention), die im Unternehmen bereitgestellt werden, nutzen zwar moderne Techniken und komplexe Funktionen, aber sie verursachen Inkonsistenzen zwischen On-Premises- und Cloud-Umgebungen. Ein Next-Generation CASB sollte zuverlässige, konsistente und umfassende Datenschutz- und Compliancefunktionen für das gesamte Unternehmen bieten, in Cloud-Umgebungen und On-Premises-Netzwerken. Er sollte alle gespeicherten oder übermittelten Daten in SaaS-Anwendungen (inline oder extern über APIs) erkennen, klassifizieren und schützen, um sicherzustellen, dass Richtlinien- und Complianceverstöße sowie Datenlecks korrekt behoben werden. Vor allem muss ein Next-Generation CASB auch neue Datenmodelle moderner Apps für die Zusammenarbeit wie Slack, Teams und Zoom verarbeiten können, in denen kurze und unstrukturierte Nachrichten sowie Screenshots verwendet werden. Mithilfe einer effektiven Cloud-Detection-Engine, beschreibenden Datenprofilen, präzisem Abgleich von Daten, Bilderkennung, natürlicher Sprachverarbeitung und KI-Modellen sollten sensible Daten erkannt werden, sowohl strukturierte als auch unstrukturierte und sowohl im Speicher als auch während der Übertragung.

Achten Sie für umfassenden Datenschutz und zuverlässige Compliance auf die folgenden Funktionen:

- ✓ Enterprise Data Loss Prevention für Daten im Speicher und während der Übertragung, einschließlich der Erkennung sensibler Daten in SaaS-Anwendungen, Offenlegung von Daten über vorkonfigurierte EDM-, OCR- und Datenprofile sowie Verhinderung der Datenausschleusung
- ✓ Datensicherheit für geschäftskritische Apps für die Zusammenarbeit wie Slack, Teams, Zoom, Jira und Confluence und die Möglichkeit, mithilfe von Deep-Learning-Prozessen, natürlicher Sprachverarbeitung und KI-Modellen sensible Daten auch in unstrukturierten Benutzerkonversationen automatisch und in Echtzeit zu erkennen
- ✓ Vorkonfigurierte Complianceberichte, unter anderem ein in Echtzeit erstellter DSGVO-Bericht für gespeicherte Daten, ein bei Bedarf erstellter Bericht zur Risikoeinschätzung für gespeicherte Daten und ein bei Bedarf erstellter SaaS Security-Bericht zu Schatten-IT-Anwendungen

5

Die CASB-Lösung sollte integrierte und konsistente Sicherheitsfunktionen für alle Standorte bereitstellen

CASB sind nicht mit der zentralen Infrastruktur eines Unternehmens verbunden und können daher keine konsistenten Sicherheitsfunktionen für alle Umgebungen (Cloud, On-Premises-Netzwerke und Remotebenutzer) bereitstellen. Dadurch steigt die Arbeitslast der Sicherheitsteams, die die Risiken, Richtlinien und Kontrollfunktionen in den verschiedenen Umgebungen abstimmen müssen. Ein Next-Generation CASB sollte eine integrierte Lösung sein, um ein sicheres hybrides Arbeitsmodell zu ermöglichen sowie alle Daten im Speicher und während der Übertragung und alle genutzten Anwendungen zu schützen. Eine solche Lösung vermeidet die Komplexität von Punktlösungen und schützt konsistent alle gespeicherten und übertragenen Daten in cloudbasierten Apps und im physischen Netzwerk. Der neue multimodale CASB sorgt für die Sicherheit genehmigter und nicht genehmigter Apps und des gesamten Datenverkehrs (webbasiert und nicht webbasiert) und bietet in einer einheitlichen cloudbasierten Konsole einen umfassenden Überblick. Er muss nicht genehmigte SaaS-Apps erkennen und Risiken verwalten können sowie zahlreiche API-basierte Sicherheitsfunktionen umfassen, um genehmigte Apps in der Cloud zu scannen und alle Benutzer-, Ordner- und Dateiaktivitäten im Speicher erkennen, untersuchen und beheben zu können.

Achten Sie für einen integrierten multimodalen CASB auf die folgenden Funktionen:

- ✓ Detaillierte Inlinekontrollen für alle Anwendungen, Benutzer und Geräte
- ✓ Datensicherheits- und Compliancemaßnahmen für alle SaaS-Apps, Netzwerke und Benutzer – ohne zusätzliche Tools von Drittanbietern
- ✓ Funktionen zur Abwehr von Bedrohungen für alle Apps, Netzwerke und Geräte mit WildFire – ohne zusätzliche Tools von Drittanbietern
- ✓ Nutzung der vorhandenen Sicherheitsinfrastruktur. Keine Änderungen an der Architektur, PAC-Dateien oder sonstige VPN-Agenten erforderlich.

SaaS Security von Palo Alto Networks

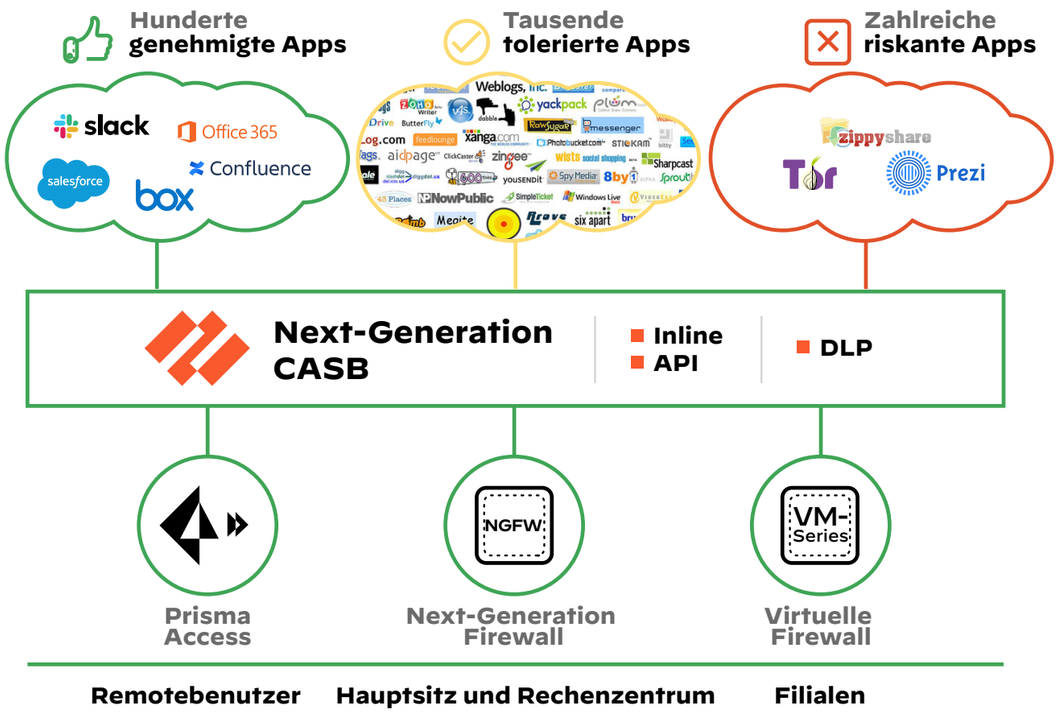
Der Next-Generation CASB, der die steigende Anzahl der SaaS-Apps bewältigt

Für den sicheren Umstieg auf die Cloud benötigen Unternehmen eine zentrale, konsistente Lösung zum Schutz ihrer Benutzer, Anwendungen und Daten in allen Umgebungen. SaaS Security kann auch die steigende Anzahl an SaaS-Apps bewältigen, da es in vorhandene Architekturen und Arbeitsabläufe eingebettet wird und die Anwendungen daher automatisch erkennt und schützt. Damit profitieren Unternehmen von einer größeren Einfachheit und Effizienz. Hier finden Sie eine Übersicht aller Vorteile von SaaS Security:

- Es ist die einzige Lösung, die neue SaaS-Apps automatisch mit unserer patentierten App-ID-Technologie erkennen und verwalten kann. App-ID nutzt Informationen der globalen Palo Alto Networks Community und maschineller Lernverfahren, um kontinuierlich nach neuen SaaS-Anwendungen zu suchen. So stellen Sie sicher, dass beliebte und weitverbreitete Apps automatisch erkannt werden.

- Im Gegensatz zu proxybasierten CASB müssen in der schlanken Architektur unseres Next-Generation CASB keine Komponenten zwischengeschaltet werden. Dadurch verkürzt sich die Amortisation um das Fünffache, da die Lösung innerhalb weniger Minuten auf unseren SASE- und Next-Generation Firewall-Plattformen gestartet werden kann. Welche Vorteile bietet unser Next-Generation CASB? Einen effizienten Betrieb, niedrigere Gesamtbetriebskosten und einen höheren ROI.

- SaaS Security kann Bedrohungen unmittelbar abwehren, da es auf Informationen von Tausenden Kunden weltweit zugreifen und umgehungsresistente Signaturen in Sekundenschnelle bereitstellen kann. So lassen sich alle Bedrohungen, einschließlich Zero-Day-Angriffen, in Echtzeit und ohne Sicherheitstools von Drittanbietern abwehren.



Der neue CASB von Palo Alto Networks für moderne Unternehmen

- Er nutzt die branchenweit umfassendste cloudbasierte **Enterprise Data Loss Prevention** für alle SaaS-Apps (sowohl inline als auch im Speicher über Out-of-Band-APIs), einschließlich moderner Apps für die Zusammenarbeit. Außerdem deckt er das gesamte Unternehmen ab, von Cloud-Umgebungen über On-Premises-Netzwerke bis zu mobilen Benutzern – also alle Orte, an denen sich Benutzer aufhalten und Daten gespeichert werden. Dadurch ist für einen umfassenden Datenschutz und konsistente Compliancemechanismen gesorgt.

- Dank vorkonfigurierter Complianceberichte und dem konsistenten Schutz von SaaS-Apps durch **Enterprise DLP**, ML-gestützte Threat Prevention und die fortlaufende Überwachung der Benutzeraktivitäten und administrativen Konfigurationen wird die Einhaltung der Compliancevorgaben diverser Verordnungen wie PCI DSS, HIPAA und DSGVO sichergestellt.

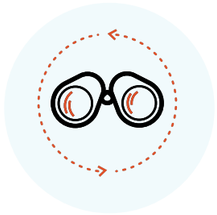
- Über eine cloudnative Implementierung kann die Lösung nativ in die Netzwerksicherheitsinfrastruktur integriert werden. Dadurch wird sie zu einer wichtigen Komponente der **SASE**-Plattform oder **Next-Generation Firewall** und kann alle genutzten Anwendungen erkennen und schützen, sowohl webbasierte als auch andere. Sie bietet einen umfassenden Datenschutz für alle Anwendungen, Netzwerke, Daten und Arbeitsabläufe sowie für alle Benutzer, unabhängig von deren Standort.

SaaS Security von Palo Alto Networks schließt eine Marktlücke und befriedigt die Nachfrage nach einer vereinfachten Version der älteren CASB. **Laut unserer Untersuchungsergebnisse kann ein solch umfassender, aber unkomplizierter Ansatz die Sicherheitsvorfälle innerhalb von drei Jahren um 45 Prozent reduzieren.**

SaaS Security deckt alle CASB-Anwendungsfälle ab

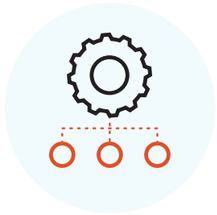
Gönnen Sie Ihrem IT-Team die Vorteile eines integrierten CASB

Falls Ihr Unternehmen Schwierigkeiten hat, die steigende Anzahl der SaaS-Anwendungen in den Griff zu bekommen, sollten Sie unseren integrierten CASB in Betracht ziehen.



Umfassender Überblick und Kontrolle über SaaS-Anwendungen in einer Konsole

- Automatische Erkennung und Kontrolle neuer Apps dank der Cloud App-ID™-Technologie
- Keine zwischengeschalteten Komponenten, niedrige Gesamtbetriebskosten
- Zahlreiche API-basierte Sicherheitsfunktionen für genehmigte Apps



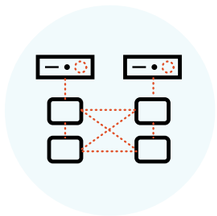
Schlanke Architektur und einfache Bereitstellung auf verschiedenen Formfaktoren

- Secure Access Service Edge (SASE)
- Hardwarefirewalls
- Softwarefirewalls

Präzise Data Loss Prevention und ML-gestützte Threat Prevention

- Schutz sensibler Daten in allen SaaS-Apps, an allen Standorten der Benutzer und allen Speicherorten der Daten
- Beschreibende Identifikatoren, präziser Abgleich von Daten, natürliche Sprachverarbeitung und Bilderkennung für eine äußerst genau Datenerfassung
- Abwehr von Bedrohungen mithilfe von Inline-ML-Modellen
- Unmittelbar verfügbare umgehungsresistente Signaturen für die Bedrohungserkennung

Eine einheitliche cloudbasierte Konsole für Inlinefunktionen, API und Enterprise DLP



Bereitstellung auf unserer umfassenden SASE-Plattform oder den Next-Generation Firewalls

Compliance mit Verordnungen wie PCI DSS, HIPAA und DSGVO durch den Schutz von SaaS-Apps

Ein integrierter CASB von Palo Alto Networks

Palo Alto Networks hat sich das Ziel gesetzt, zum bevorzugten Cybersicherheitspartner für Unternehmen zu werden und gemeinsam mit ihnen unseren digitalen Lebensstil zu schützen. Wir schützen die Clouds, Netzwerke und Mobilgeräte Zehntausender Unternehmen. Dazu gehen wir durch kontinuierliche Innovation die größten Herausforderungen rund um die Cybersicherheit an, mit denen Unternehmen derzeit konfrontiert sind. Dabei kommen die neuesten Forschungsergebnisse aus den Bereichen der künstlichen Intelligenz, Analysen, Automatisierung und Orchestrierung zum Einsatz.

Palo Alto Networks wurde 2005 gegründet und hat seinen Hauptsitz im kalifornischen Santa Clara. Zur Betreuung unserer Kunden haben wir zudem Niederlassungen auf der ganzen Welt. Weitere Informationen erhalten Sie unter:

Weitere Informationen erhalten Sie unter: www.paloaltonetworks.de

Sie möchten mehr erfahren?

Zur Demo für SaaS Security

Das sagen unsere Kunden

"Wir sind davon überzeugt, dass Palo Alto Networks uns auch in Zukunft begleiten wird. Palo Alto Networks weiß genau, welche Sicherheitsfunktionen in SaaS-Umgebungen notwendig sind, um alle kritischen Aspekte einer solchen Bereitstellung abzudecken."

Juan Carlos Alzate Garcia,
Vice President of Technology

CIUDAD CELESTE
SAMBORONDÓN

Zur Fallstudie

www.paloaltonetworks.de

Oval Tower, De Entrée 99–197
1101 HE Amsterdam, Niederlande

Zentrale: +1 408 753 4000
Vertrieb: +1 866 320 4788
Support: +1 866 898 9087