Sicher durch den SaaS-Dschungel

Mit dem einzigen integrierten CASB, der die steigende Anzahl der SaaS-Apps automatisch im Griff behält

Inhalt

Einleitung

Im Kielwasser des rasanten technologischen Fortschritts der letzten zehn Jahre haben zahlreiche Unternehmen damit begonnen, ihre Anwendungen und Daten aus internen Rechenzentren in die Cloud zu migrieren. Besonders beliebt sind derzeit SaaS-Anwendungen (Software as a Service) wie Microsoft Office 365®, Box und Salesforce sowie Public-Cloud-Angebote wie Google Cloud Platform (GCP®), Amazon Web Services (AWS®) und Microsoft Azure®. Von diesem Schritt versprechen sich die Verantwortlichen zum einen eine verbesserte digitale Zusammenarbeit zwischen ihren auf Standorte in aller Welt verteilten Benutzern, zum anderen signifikante Kostensenkungen durch die Ablösung der konventionellen On-Premises-Lösungen.

Der Umstieg auf die Cloud und cloudbasierte Technologien bietet zweifellos gewaltige Vorteile, bringt jedoch auch neue Sicherheitsrisiken mit sich:

- **Schatten-IT:** Über das Internet können Mitarbeiter direkt und unter Umgehung des Unternehmensnetzwerks auf diverse SaaS-Anwendungen zugreifen, ohne dass die IT-Abteilung dies mitbekommt. Das erschwert eine effektive Kontrolle der Nutzung von Cloud-Anwendungen und der damit verbundenen Risiken.
- **Ausweitung des Netzwerkperimeters:** Wenn die IT-Infrastruktur um Cloud-Umgebungen und -Anwendungen erweitert wird und die Zahl der externen Benutzer und Datenbestände steigt, genügt es nicht länger, den Perimeter des unternehmensinternen Netzwerks zu schützen.
- **Zunehmender Datenaustausch über das Web:** Moderne Unternehmen erfassen, speichern und nutzen riesige Bestände an teils extrem vertraulichen und sensiblen Daten, die auf immer mehr SaaS-Anwendungen, öffentlichen Cloud-Umgebungen, internen Rechenzentren und Mobilgeräten von Benutzern verteilt sind.
- **Geteilte Zuständigkeiten für Sicherheit und Compliance:** Cloud-Anbieter und ihre Kunden sind jeweils für bestimmte Aspekte der Sicherheit und Compliance zuständig. Das bedeutet, dass Kundenunternehmen die Verantwortung für die Umsetzung von Sicherheits- und Complianceanforderungen nicht komplett an die Anbieter abgeben können.

Generell ist zu beobachten, dass IT-Teams infolge der fortschreitenden Migration in die Cloud zunehmend schlechter überblicken können, welchen Aktivitäten Benutzer im Internet nachgehen, welche Mitarbeiter auf welche Ressourcen zugreifen, wo sensible Daten gespeichert und wie sie gesichert sind und wie sich die Sicherheitslage des Unternehmens insgesamt darstellt.

Dieses E-Book bietet einen Überblick über die Herausforderungen, die mit dem Umstieg auf die Cloud verbunden sind, und präsentiert Best Practices zur Stärkung der Sicherheit der Anwendungen, Daten und Benutzer moderner Unternehmen.

Herausforderungen beim Umstieg auf SaaS-Anwendungen

SaaS-Anwendungen erfreuen sich wegen ihrer flächendeckenden Verfügbarkeit, hohen Benutzerfreundlichkeit und geringen Kosten seit Jahren einer starken Beliebtheit.

Gartner schätzt, dass der Markt für Public-Cloud-Services, der 2020 bereits ein Volumen von 257,5 Milliarden USD erreichte, 2021 noch einmal um 18,4 Prozent wachsen und einen Umsatz von 304,9 Milliarden USD verzeichnen wird. Ferner prognostiziert Gartner, dass allein der weltweite Umsatz für Cloud-Anwendungsservices (SaaS) im Jahr 2021 auf über 117 Millionen USD ansteigen wird.[1]

Allerdings sollte dabei nicht vergessen werden, dass einfach zu bedienende Anwendungen nicht automatisch sicher sind. Nicht ohne Grund sehen sich viele Unternehmen beim Umstieg auf SaaS-Anwendungen mit komplexen Herausforderungen konfrontiert:

- IT-Teams müssen neben der Nutzung der genehmigten SaaS-Anwendungen auch die (privaten und beruflichen) Mitarbeiteraktivitäten in tolerierten und nicht genehmigten Apps kontrollieren.
- Die cloudbasierte Speicherung und Verarbeitung von teils äußerst sensiblen Geschäfts- und Kundendaten stellt ein Sicherheitsrisiko dar, da sich diese Daten in der Cloud und bei der Übertragung zwischen diversen Cloud-Anwendungen und Benutzern nicht leicht effektiv schützen lassen.

In Anbetracht dessen ist es wenig überraschend, dass die Kontrolle der Schatten-IT und der Schutz der Unternehmensdaten ganz oben auf der Liste der Sicherheitsherausforderungen moderner Unternehmen stehen. Wie eine von der ESG durchgeführte Studie zeigt, befürchten 35 Prozent der befragten Sicherheitsexperten vor allem, dass sich Mitarbeiter ohne Zustimmung und Kontrolle der IT-Abteilung bei Cloud-Anwendungen und -Services registrieren, während 30 Prozent die flächendeckende Identifizierung und Klassifizierung personenbezogener Daten im Rahmen der Umsetzung gesetzlicher Datenschutzvorgaben als größtes Problem ansehen.[2]

Die Cloud kennt keine Grenzen

- Direkter Zugang zur Cloud
- Schatten-IT
- Datenaustausch über externe Plattformen

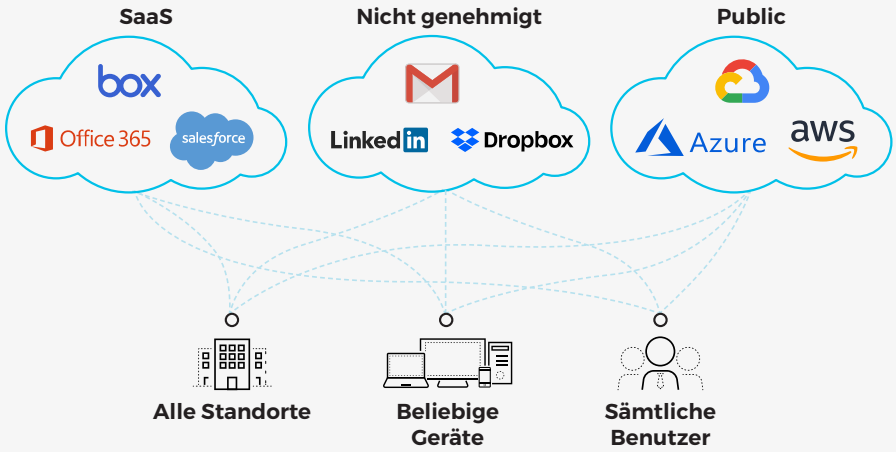


Abbildung 1: Standortübergreifende Cloud-Nutzung in modernen Unternehmen

1. „Gartner Forecasts Worldwide Public Cloud End-User Spending to Grow 18% in 2021", Gartner, 17. November 2020. https://www.gartner.com/en/newsroom/press-releases/2020-11-17-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-grow-18-percent-in-2021.
2. „ESG Master Survey Results: Trends in Data Security", ESG, 28. Januar 2019, https://www.esg-global.com/research/esg-master-survey-results-trends-in-cloud-data-security

Steigende Anforderungen in puncto Datensicherheit und Compliance

Das Thema Datensicherheit erlangt zusätzliche Relevanz, wenn Unternehmensdaten in weitverzweigten internen und externen Netzwerken übertragen, über SaaS-Anwendungen zugänglich gemacht und von Benutzern mit unterschiedlichen Zugriffsrechten (oder ohne Zugriffsrechte) abgerufen werden. Denn Unternehmensinfrastrukturen, die diverse SaaS-Anwendungen und Cloud-Services von Drittanbietern sowie zahlreiche für alle Mitarbeiter zugängliche Ressourcen und Verbindungspunkte zum Internet umfassen, erschweren IT-Teams die Identifizierung, Überwachung und Sicherung der sensiblen und gesetzlich geschützten Datenbestände und Übertragungspfade. Unter diesen Bedingungen entstehen Sicherheitslücken, die wiederum das Risiko von Datenlecks und Complianceverstößen steigern.

Das ist umso gravierender, da viele Unternehmen standort- oder branchenspezifischen Datensicherheitsgesetzen und -richtlinien unterliegen, wie beispielswiese der EU-Datenschutz-Grundverordnung (DSGVO), dem Health Insurance Portability and Accountability Act (HIPAA), dem Payment Card Industry Data Security Standard (PCI DSS) oder dem California Consumer Privacy Act (CCPA).

Bei Nichteinhaltung dieser Vorgaben drohen nicht nur Datenverluste und Sicherheitsverletzungen, sondern auch hohe Kosten durch empfindliche Bußgelder, Sammelklagen und Imageschäden mit begleitenden Umsatzeinbußen.

3,92 Mio. USD

durchschnittliche Kosten eines Datenlecks (2019)[3]

36%

Umsatzeinbußen durch verlorenes Kundenvertrauen nach einem Sicherheitsvorfall[3]

11,45 Mio. USD

durchschnittliche jährliche Kosten durch Insidervorfälle (pro Unternehmen, 2020)[4]

644.000 USD

durchschnittliche Kosten pro Vorfall[4]

20 Mio. € oder 4%

des weltweiten Jahresumsatzes des Unternehmens (je nachdem, welcher Betrag größer ist) als maximales Einzelbußgeld bei Nichteinhaltung von DSGVO-Vorgaben[5]

3. „2019 Cost of a Data Breach Report", Ponemon Institute, Juli 2019, https://www.ibm.com/security/data-breach
4. „2020 Cost of Insider Threats Global Report", Ponemon Institute, Januar 2020, https://www.observeit.com/cost-of-insider-threats
5. „Understanding GDPR Fines", GDPR Associates, abgerufen am 22. April 2020, https://www.gdpr.associates/what-is-gdpr/understanding-gdpr-fines

Umfassendes Monitoring als Voraussetzung für starke Sicherheit

Um Ihr Unternehmen, Ihre Daten und Ihre Mitarbeiter bei der Migration in die Cloud effektiv schützen zu können, müssen Sie genau wissen,

- **welche Cloud-Anwendungen Ihre Mitarbeiter wie oft nutzen** und welche Risiken mit jeder App verbunden sind – damit Sie gezielte Schritte zur Eindämmung der Schatten-IT in Ihrem Unternehmen einleiten können;
- **welche Benutzer und Geräte auf die genehmigten SaaS-Anwendungen Ihres Unternehmens zugreifen dürfen** – damit Sie sicherstellen können, dass nur vertrauenswürdige Personen oder Geräte Zugang zu geschäftskritischen Apps wie Microsoft Office 365®, G Suite®, Salesforce oder Box erhalten;
- **welche sensiblen Daten in welchen Cloud-Umgebungen gespeichert sind** bzw. in die Cloud übertragen oder aus der Cloud abgerufen werden;
- **wie diese Daten genutzt und für wen sie in SaaS-Anwendungen freigegeben werden** und ob dies unter Einhaltung der Sicherheitsrichtlinien Ihres Unternehmens erfolgt;
- **welche Compliancerisiken Ihr Unternehmen bei der Nutzung cloudbasierter Anwendungen und Datenspeicher berücksichtigen muss** und wie sie sich minimieren lassen; und
- **welchen Bedrohungen Ihre genehmigten Anwendungen ausgesetzt sind,** welche Benutzeraktivitäten das größte Risiko bergen und wie die Gefahr langfristig minimiert werden kann.

Welche Apps werden von Mitarbeitern wie genutzt?

Wie können wir sensible Daten in der Cloud schützen?

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

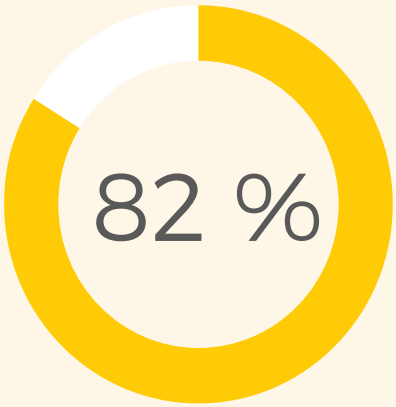
Konventionelle Lösungen haben ausgedient

Viele Unternehmen setzen bei der Migration in die Cloud auf

- **native Sicherheitsfeatures** ihrer SaaS-Anwendungen und Cloud-Plattformen, die sich jedoch von Anbieter zu Anbieter und von App zu App unterscheiden und nur grundlegenden Schutz bieten;
- **Cloud Access Security Broker (CASBs)**, die speziell für Datensicherheit, Schutz und Compliance über mehrere SaaS-Anwendungen hinweg konzipiert sind.

  CASB-Tools haben jedoch ihre Grenzen:

  - Sie können mit dem starken Wachstum von SaaS nicht mithalten, weil sie weder über eine automatisierte Klassifizierungs-Engine noch über ausreichend intelligente Funktionen verfügen, um neue Anwendungen zuverlässig zu identifizieren.
  - Sie bieten nur grundlegende Sicherheitsfunktionen für die Cloud. Außerdem bietet ihr Datensicherheitsansatz nicht den Umfang und die Tiefe einer DLP der Enterprise-Klasse.
  - Ihre Bereitstellung ist komplex und ihre zusammengesetzte Architektur verursacht hohe Gesamtbetriebskosten. Da sie nicht eng in andere Sicherheitstools integriert sind, erfordern sie eine komplizierte Umleitung des Datenverkehrs von der Firewall und sind auf PAC-Dateien angewiesen.

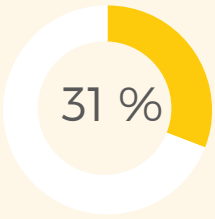


der befragten Sicherheitsexperten geben an, dass sich konventionelle Sicherheitslösungen für Cloud-Umgebungen gar nicht eignen oder nur einen begrenzten Funktionsumfang bieten.[6]

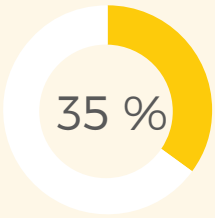
6. „2020 Cloud Security Report", Cybersecurity Insiders, August 2020.

- **Web-Proxys** lassen sich wegen ihrer mangelnden Interoperabilität kaum aufeinander sowie auf die vorhandenen Firewalls abstimmen. Außerdem scannen Proxys nicht den gesamten Datenverkehr.
- **Punktlösungen von verschiedenen Anbietern**, wie beispielsweise eigenständige Cloud Access Security Broker (CASBs), sichere Internetgateways (SWGs) und cloudfähige DLP-Tools (Data Loss Protection), sind voneinander isoliert und nicht mit der bestehenden On-Premises-Sicherheitsinfrastruktur des Unternehmens integriert.

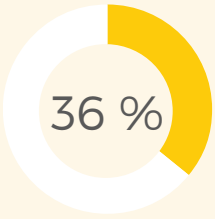
Hier müssen die Verantwortlichen möglicherweise feststellen, dass sich die Einführung und Bereitstellung dieser Lösungen sowie ihre Integration mit den anderen Komponenten der vorhandenen Sicherheitsinfrastruktur so kompliziert gestaltet, dass das gewünschte Maß an Schutz und Überwachung nicht erreicht werden kann. Denn ein auf voneinander isolierten Komponenten basierender Ansatz behindert die effektive Verwaltung der Sicherheitsmaßnahmen, reißt neue Sicherheitslücken und erschwert die anwendungsübergreifende Implementierung von Sicherheits- und Compliancevorgaben.



sind der Meinung, dass Sicherheit nicht mit dem Tempo der Veränderungen von Anwendungen mithalten kann.[7]



denken, dass die Risiken der Datensicherheit, wie Datenverluste und -lecks, die Einführung der Cloud behindern.[8]



haben Schwierigkeiten, konsistente Sicherheitsrichtlinien für Cloud- und On-Premises-Umgebungen festzulegen.[9]

7–9. „2020 Cloud Security Report", Cybersecurity Insiders, August 2020.

Die sichere Einführung von SaaS-Anwendungen

Für den sicheren Umstieg auf die Cloud benötigen moderne Unternehmen **eine zentrale, konsistente Lösung zum Schutz ihrer …**

Benutzer **Anwendungen** **Daten** **Geschäftsprozesse**

Zudem benötigen sie leistungsstarke Funktionen zur:

Überwachung des gesamten Datenverkehrs, damit die Verantwortlichen stets genau darüber im Bilde sind, welche Anwendungen und Cloud-Umgebungen von ihren Mitarbeitern für welche Aktivitäten genutzt werden, welche nicht genehmigten Apps (Schatten-IT) zum Einsatz kommen und wie groß die damit entstehenden Risiken sind;

Kontrolle des Zugriffs auf Unternehmensanwendungen durch die Implementierung von Mechanismen zur Benutzerauthentifizierung und zur flächendeckenden Durchsetzung von Unternehmensrichtlinien;

Implementierung standortunabhängiger Sicherheitsmaßnahmen, die sämtliche Daten, Anwendungen und Benutzer in allen Netzwerken und Cloud-Umgebungen schützen, ohne dass dafür eine komplexe Infrastruktur aus diversen Punktlösungen eingerichtet werden muss.

Stärkung der Datensicherheit durch die Identifizierung, Erfassung und Sicherung aller sensiblen und gesetzlich geschützten Daten, die von allen Benutzern über das Netzwerk übertragen werden und in den Cloud-Umgebungen des Unternehmens gespeichert sind

Abwehr komplexer Bedrohungen in der Cloud in Echtzeit und mit hoher Zuverlässigkeit, ohne dass Sicherheitstools von Drittanbietern eingesetzt werden müssen

Risikominimierung und Umsetzung von Compliancevorgaben durch die automatische Identifizierung und Schließung von Schwachstellen und öffentlichen Links zu SaaS-Anwendungen sowie durch die konsistente Implementierung richtlinienkonformer Maßnahmen zum Schutz von Cloud-Umgebungen und sensiblen Datenbeständen

Eine moderne Sicherheitsstrategie für das SaaS-Zeitalter

Der sichere Umstieg auf die Cloud erfordert unter anderem effektive Maßnahmen zum Schutz der Datenspeicherung und -nutzung. Deshalb muss jeder erfolgreiche SaaS-Sicherheitsansatz die folgenden Komponenten umfassen:

Automatische Funktionen zur Datenerfassung und -klassifizierung, mit denen sich die Übertragung und Speicherung von personenbezogenen Daten, geistigem Eigentum und anderen sensiblen oder gesetzlich geschützten Informationen in der Cloud mit hoher Genauigkeit überwachen lassen

Moderne Datensicherheitstools, die Daten bei der Übertragung und Speicherung schützen und Datenlecks sowie fahrlässige, riskante oder schädliche Aktivitäten der Benutzer automatisch unterbinden, indem sie Warnmeldungen ausgeben, Dateien verschlüsseln, Freigaben deaktivieren, digitale Rechte durchsetzen und unsichere Übertragungsprozesse stoppen

Effektive Lösungen zur Durchsetzung von Compliancevorgaben, um die Privatsphäre zu schützen und den ordnungsgemäßen Umgang mit gesetzlich geschützten, sensiblen Daten zu gewährleisten, die Freigabe von Daten einschließlich der Frage, wie und mit wem welche Daten geteilt werden, zu kontrollieren und überwachen sowie die Dokumentation von Complianceverstößen zu erleichtern und diese zu beheben

Weitere Informationen über effektive Datensicherheit in der Cloud finden Sie auf unserer Website unter:

paloaltonetworks.com/cyberpedia/what-is-cloud-data-protection

Grundpfeiler der SaaS-Sicherheit: eine leistungsstarke SASE-Lösung

Wenn Sie Ihr Unternehmen auf dem Weg in die Cloud umfassend schützen möchten, benötigen Sie eine kombinierte Netzwerk- und Sicherheitsinfrastruktur, die unter anderem für mobile Benutzer sowie cloudbasierte Anwendungen und Datenspeicher ausgelegt ist und alle Filialen und Verkaufsstellen abdeckt.

Unsere umfassende SASE-Lösung vereint Netzwerk- und Sicherheitsdienste auf einer zentralen cloudbasierten Plattform und versetzt Ihr IT-Team in die Lage, Risiken für Daten, Anwendungen und Benutzer zu minimieren, die Modernisierung Ihrer Cloud-Umgebungen und Netzwerke voranzutreiben und den Umstieg auf SaaS-Anwendungen sicher zu meistern.

Mit den SaaS-Sicherheitsfunktionen unserer SASE-Lösung können Sie Daten, Anwendungen und Benutzer in allen Netzwerken und Cloud-Umgebungen konsistent schützen. Außerdem wird der komplizierte Einsatz verschiedener Punktlösungen (wie herkömmliche CASBs und Webproxys) überflüssig, was den mit dem Umstieg auf die Cloud verbundenen Arbeits-, Ressourcen- und Investitionsaufwand drastisch reduziert.

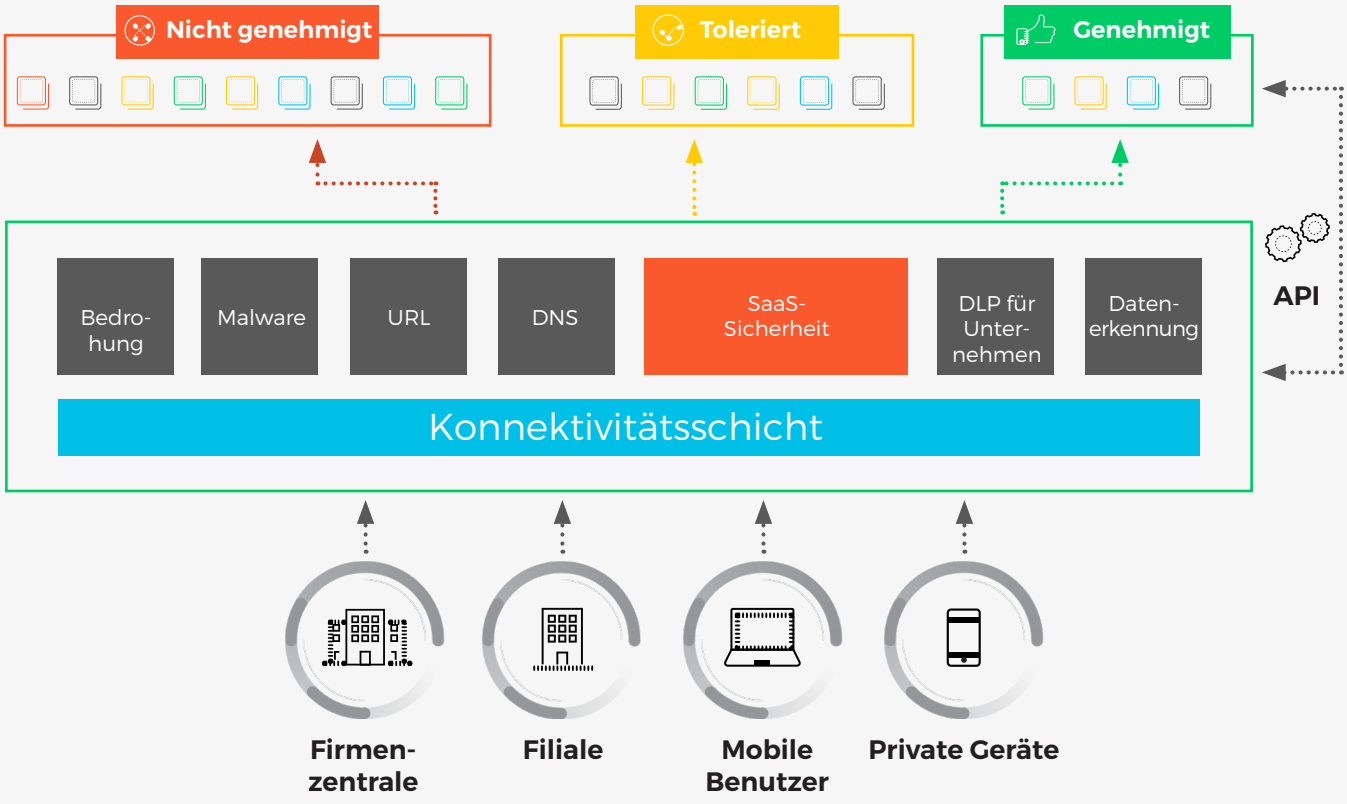


Abbildung 6: Konsistenter Schutz mit Palo Alto Networks

SaaS-Sicherheitslösungen von Palo Alto Networks

Palo Alto Networks bietet jetzt den einzigen integrierten CASB, der die stetig steigende Zahl der SaaS-Apps automatisch im Griff behält. Er ist nativ in die NGFWs von Palo Alto Networks integriert und bietet proaktive Transparenz, erstklassigen Schutz und die kürzeste Wertschöpfungszeit für alle SaaS-Anwendungen.

Er bietet Ihnen unter anderem die folgenden wichtigen Sicherheitsfeatures:

- Vollständige Transparenz, kontinuierliche Kategorisierung und detaillierte Untersuchung von Tausenden von SaaS-Anwendungen auf potenzielle Risiken. Er nutzt die Möglichkeiten der weltweiten Palo Alto Networks-Community, um den gesamten webbasierten und sonstigen Datenverkehr zu schützen und sicherzustellen, dass neue Anwendungen automatisch erkannt werden, sobald sie in zunehmendem Maße eingesetzt werden.
- DLP-Funktionen (Data Loss Prevention) der Enterprise-Klasse, mit denen Sie die Übertragung und Speicherung sensibler Daten erfassen, überwachen und schützen können, um beispielsweise Datenuploads und -freigaben in genehmigten und nicht genehmigten Anwendungen und in IaaS für alle Benutzer des Unternehmens im Griff zu behalten.
- Granulare Zugangskontrollen, die nur vertrauenswürdigen Benutzern den Zugriff auf genehmigte SaaS-Anwendungen ermöglichen und ohne Beeinträchtigung der Arbeitsprozesse für eine sichere Benutzererfahrung sorgen.
- Standortunabhängige, konsistente und automatisierte Cloud-Sicherheitsfunktionen zum Schutz Ihrer SaaS-Anwendungen und -Daten.
- Schutz vor Cyberattacken und fahrlässigen Verhaltensweisen, die möglicherweise Datensicherheitsverletzungen nach sich ziehen.
- Zuverlässige Tools für das Management und die Eindämmung von Sicherheitsvorfällen.

SaaS-Monitoring im gesamten Unternehmen

Kontinuierliche Erkennung und Kontrolle neuer Anwendungen mithilfe von Informationen aus einer großen, weltweiten Community

Schutz der Unternehmensdaten

Konsistente DLP und Compliance für alle SaaS-Apps, Netzwerke und Benutzer

Vorreiter bei Sicherheit

Echtzeitschutz vor Bedrohungen mit ML-basierter Angriffsabwehr ohne Tools von Drittanbietern

Einfach und kosteneffizient

Einfach bereitzustellen mit niedrigeren Gesamtbetriebskosten als vergleichbare herkömmliche CASB-Lösungen

Fazit

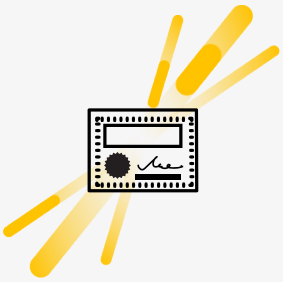
Wenn Sie den Umstieg auf die Cloud oder die Anpassung Ihrer bestehenden Cloud-Sicherheitsstrategie planen, sollten Sie unbedingt einen ganzheitlichen, auf einer modernen SASE-Lösung mit integrierten SaaS-Sicherheitsfunktionen basierenden Ansatz in Erwägung ziehen. Die cloudbasierte SASE-Lösung von Palo Alto Networks kann Ihnen dabei helfen, die Daten, Benutzer und Netzwerke Ihres Unternehmens bei der Einführung von SaaS-Anwendungen konsistent vor Cyberrisiken zu schützen. Sie ermöglicht an jedem gewünschten Standort den sicheren Zugriff auf in der Cloud bereitgestellte Anwendungen und Daten und bietet Ihnen dabei unter anderem die folgenden Vorteile:

Umfassende Transparenz für die Cloud

- Sie können jederzeit überblicken, welche Cloud-Umgebungen an welchen Standorten von welchen Mitarbeitern genutzt werden.
- Die Nutzung nicht genehmigter Apps wird automatisch erkannt, sodass Sie das damit verbundene Risiko minimieren können.
- Dank der kontinuierlichen Überwachung des Benutzerverhaltens werden verdächtige Aktivitäten umgehend aufgedeckt.

Vielschichtige und konsistente Cloud-Sicherheit

- Die Lösung unterstützt den sicheren Umstieg auf die Cloud, die Anbindung neuer Filialinfrastrukturen und die flächendeckende Einführung mobiler Arbeitsmodelle.
- Sie können bestehende Richtlinien und Kontrollen sowie Compliance- und Datensicherheitsmechanismen auf Ihre SaaS-Apps ausdehnen.
- Der Einsatz isolierter Punktlösungen erübrigt sich.



Compliance und Datenschutz in der Cloud

- Mit den leistungsstarken Kontroll- und Managementfunktionen können Sie Ihre Daten vor unbefugtem Zugriff schützen.
- Gesetzlichen Vorgaben unterliegende Daten lassen sich automatisch anwendungsübergreifend erfassen, klassifizieren und schützen.
- Sie erhalten umfassende Unterstützung bei der Umsetzung von Datenschutz- und Complianceanforderungen.

Weitere Informationen zu den SaaS-Sicherheitslösungen von Palo Alto Networks finden Sie auf unserer Website unter:

paloaltonetworks.com/network-security/saas-security

Über Palo Alto Networks

Palo Alto Networks ist ein weltweit führendes Unternehmen im Bereich der Cybersicherheit, das mit seinen bahnbrechenden Technologien die Weichen für eine cloudorientierte Zukunft stellt und die Arbeitsweise von Unternehmen und ihren Mitarbeitern von Grund auf modernisiert. Wir haben uns das Ziel gesetzt, zum bevorzugten Cybersicherheitspartner für Unternehmen zu werden und gemeinsam mit ihnen unseren digitalen Lebensstil zu schützen. 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 künstliche Intelligenz, Analyse, Automatisierung und Orchestrierung zum Einsatz. Mit einer integrierten Plattform und einem wachsenden Partnernetzwerk schützt Palo Alto Networks die Clouds, Netzwerke und Mobilgeräte Zehntausender Unternehmen und arbeitet unermüdlich für eine Welt, in der jeder Tag ein bisschen sicherer ist als der Tag zuvor. Weitere Informationen erhalten Sie unter **www.paloaltonetworks.de**.

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