Lookout®

Warum brauchen Unternehmen einen CASB?

Whitepaper

Warum brauchen Unternehmen einen CASB?

Wenn Ihr Unternehmen in der Cloud arbeitet, ist ein Cloud Access Security Broker (CASB) unerlässlich. Tatsächlich stuft das weltweit führende Forschungs- und Beratungsunternehmen Gartner, Inc. CASB in seiner Liste der 10 wichtigsten Informationssicherheitstechnologien für Unternehmen von heute als Nummer 1 ein.

Durch den umfassenden Einsatz von Cloud-Diensten und -Anwendungen sind ganz neue Angriffsziele und Bedrohungen entstanden. Nutzen Ihre Mitarbeiter Office 365 oder Salesforce? Wie sieht es mit Dropbox, Facebook, Twitter, LinkedIn, Google Drive, Evernote oder iCloud aus? Wenn ja, braucht Ihr Unternehmen einen CASB.

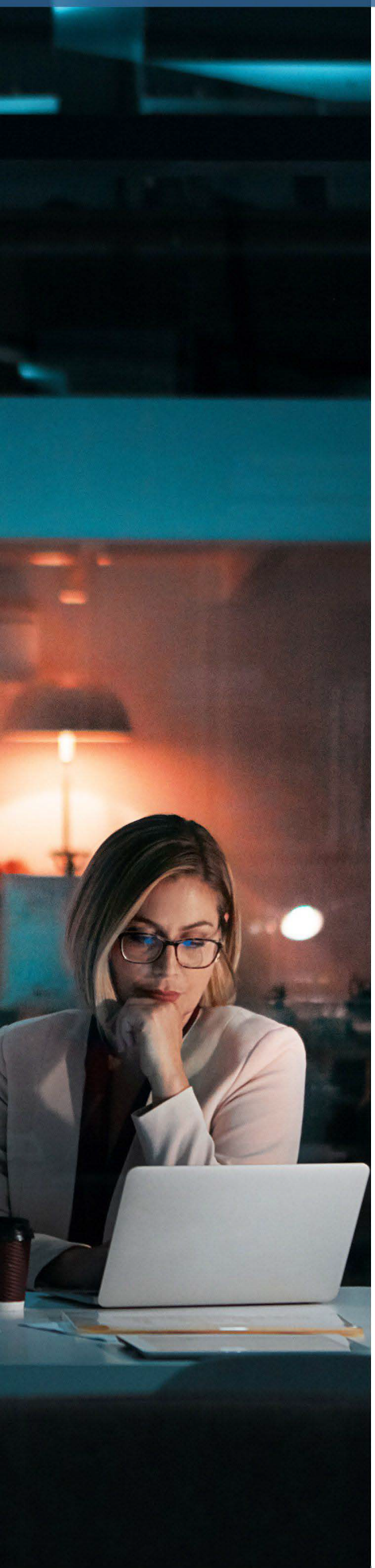
Dazu kommt der weit verbreitete Einsatz von Mobilgeräten. Unternehmen interagieren regelmäßig mit Benutzern, die sie nicht verwalten. Ihre Systeme, Anwendungen und Daten sind in regelmäßigem Kontakt mit Mobiltelefonen, Tablets und Laptops, die außerhalb Ihrer Kontrolle liegen. Tatsache ist: Etwa 86 % aller Workflows finden mittlerweile in der Cloud statt.

Gartner geht davon aus, dass in Zukunft 95 % aller Sicherheitsprobleme in der Cloud durch Anwenderfehler entstehen. Eine manuelle und an Personen orientierte Herangehensweise an die Cloud-Sicherheit wird nicht funktionieren. Eine Ergänzung um automatisierte Funktionen ist erforderlich.

Hier kommt CASB ins Spiel.

Dank maschinellem Lernen und Automatisierung liefert CASB kritische Kontrollpunkte für sichere und regelkonforme Cloud-Nutzung über mehrere Anbieter hinweg. Die Grundlage bilden hier vier wichtige Komponenten der Cloud-Sicherheit: Transparenz, Compliance, Datensicherheit und Schutz vor Bedrohungen. Risiken werden dann nicht mehr durch manuelle Prozesse festgestellt, sondern vom CASB. So sparen Sie erheblich Zeit und vermeiden Benutzerfehler.

Aufgrund einiger falscher Annahmen wird die Cloud-Sicherheit nicht immer in den Sicherheitsbudgets von Unternehmen berücksichtigt. Viele Unternehmen denken, dass ihre Cloud-Dienstanbieter alle Sicherheitsfunktionen übernehmen. Das ist aber nicht der Fall. Cloud-Dienstanbieter sind für die Sicherheit der Cloud verantwortlich, während Sie für die Sicherheit Ihrer eigenen Inhalte in der Cloud sorgen müssen. Viele glauben auch, dass die Investition in die SIEM-Sicherheit auch die Cloud-Sicherheit umfasst. Das trifft nicht unbedingt zu. Sie können aber einen CASB in ein vorhandenes SIEM-Sicherheitssystem integrieren, um den Schutz zu maximieren.



Um zu verstehen, warum ein CASB so wichtig für Unternehmen ist, sollten Sie sich einige wichtige Fragen stellen, die Ihnen helfen einzuschätzen, welche Kosten ein mangelnder Schutz von Daten verursachen kann:

Transparenz

- Wer greift auf welche Anwendungen zu?
- Wer greift auf nicht genehmigte Anwendungen zu?
- Was machen nicht verwaltete Benutzer?

Der CASB ermittelt kompromittierte Anmeldeinformationen und präparierte Sites. Er berechnet das Risiko und beurteilt die Fähigkeit des Unternehmens, Bedrohungen abzuwehren.

Compliance

- Sind meine DevOps-Funktionen regelkonform?
- Sind meine Zugriffsschlüssel regelkonform?
- Gibt es Benutzer mit zu hohen Berechtigungen in meinen Systemen?

Der CASB stellt die Einhaltung von Datenvorschriften für Ihre Branche sicher. Fast die Hälfte aller Aktivitäten mit Cloud-Anwendungen findet auf Mobilgeräten statt. Ein Drittel aller Verstöße gegen DLP-Richtlinien geschehen auf Mobilgeräten.

Datensicherheit

- Wer gibt Daten öffentlich weiter?
- Teile ich mir die Verantwortung für die Sicherheit mit meinem Cloud-Anbieter und der SIEM-Lösung?
- Weist meine DevOps-Lösung Sicherheitslücken auf?

Der CASB verschlüsselt sensible Daten im Ruhezustand und bei der Übertragung über das Netzwerk. Dabei schützt er vertrauliche Daten in genehmigten Anwendungen und verhindert Uploads geistigen Eigentums in nicht genehmigte Anwendungen.

Schutz vor Bedrohungen

- Welche Benutzer in meinen Systemen bergen ein hohes Risiko?
- Wie schnell kann ich riskante Benutzeraktivitäten unterbinden?
- Wie schnell kann ich riskante Anwendungen unterbinden?

Der CASB tauscht Bedrohungserkenntnisse mit anderen Technologien wie EDR (Endpoint Detection and Response, Erkennung und Schutz von Endgeräten) und Sandboxes aus. Er blockiert oder beseitigt Malware in genehmigten und nicht genehmigten Anwendungen und erkennt und beseitigt Ransomware.

Wenn Ihr Sicherheitsteam diese wichtigen Fragen zu den vier Grundpfeilern der Cloud-Sicherheit nicht beantworten kann, benötigen Sie einen CASB. Dieser versorgt Sie kostengünstig und effektiv mit diesen wichtigen Einblicken.

Aus unternehmerischer Sicht übersteigt der ROI eines CASB bei weitem seine Kosten. Wie viel würde eine Datensicherheitsverletzung kosten? Wie hoch ist das finanzielle Risiko, ohne einen CASB zu arbeiten? Wie hoch wären die Kosten von Compliance-Verstößen, verlorenem geistigen Eigentum oder einer Schädigung des Markenrufs bei einer Sicherheitsverletzung in der Cloud?

Einige Beispiele für den Business Case eines CASB:

Schützt den Markenruf und geistiges Eigentum

Was würde es Ihre Marke kosten, wenn ein böswilliger Insider oder ein Angreifer von außen Ihr geistiges Eigentum wie Betriebsgeheimnisse und Patente stiehlt? Die echten Kosten des Verlusts von geistigem Eigentum belaufen sich auf schätzungsweise 40 Millionen US-Dollar pro Vorfall. Studien zufolge verursachen Rufschädigung und Kundenabwanderung aufgrund einer Datenpanne Kosten von ungefähr 239 US-Dollar pro Stunde.

Verhindert Compliance-Verstöße

Mit einer CASB-Lösung können Unternehmen Verstöße gegen internationale Sicherheitsvorschriften wie HIPAA, PCI Data Security Standard und DSGVO und die damit verbundenen Kosten vermeiden. Ein einzelner HPA-Verstoß im Gesundheitswesen kostet schätzungsweise mehr als 1,5 Millionen US-Dollar pro Jahr.

Maximiert die Cloud-Investition

Die Kosten für die Sicherung Ihrer Daten in der Cloud sind im Vergleich zu den jährlichen Einsparungen durch den Cloud-Einsatz gering. CASB sorgt wie eine Versicherung dafür, dass Sie weiter von den geschäftlichen Vorteilen und Kosteneinsparungen des Cloud-Betriebs profitieren können.

Was spricht für die Nutzung der Cloud?

Investition in Höhe von 14,2 Mio. USD + **18 Monate** + **Fokus** = **311 Apps in der Cloud** & **Einsparungen in Höhe von 14 Mio. USD**

Cloud-Einsparungen pro Jahr > **Jährliche Kosten für einen CASB**

*Fallstudie von GE Oil & Gas

Ein Cloud Access Security Broker liefert einen vollständigen Einblick in die allgemeine Nutzung von Cloud-Anwendungen sowie Datensicherung und Governance für die ganze Cloud-Umgebung. So können Sie Ihre Daten schützen und gleichzeitig kostspielige Sicherheitsverletzungen oder Bußgelder wegen Nichteinhaltung von Vorschriften vermeiden.

Die weltweit größten Unternehmen nutzen Lookout

5 der 10 führenden US-Banken

6 der weltweit führenden Banken

3 der 10 führenden Versicherungsunternehmen

3 der 10 führenden US-Gesundheitsanbieter

3 der 10 führenden Pharmaunternehmen

2 der größten Telekommunikationsunternehmen

Regierungsbehörden in den USA, im Vereinigten Königreich sowie in Kanada, Australien und anderen Ländern

Lookout®

Über Lookout

Lookout ist ein Anbieter von integrierten Sicherheitslösungen vom Endgerät bis zur Cloud. In einer Welt, in der Datenschutz höchste Priorität hat und Mobilität und Cloud bei der Arbeit und in der Freizeit unverzichtbar geworden sind, haben wir es uns zur Aufgabe gemacht, Sie sicher in die digitale Zukunft zu führen. Wir geben Verbrauchern und Mitarbeitern die Möglichkeit, ihre Daten zu schützen und sicher miteinander in Verbindung zu bleiben, ohne ihre Privatsphäre oder ihr Vertrauen zu verletzen. Lookout wird von Millionen Anwendern, den größten Unternehmen und Behörden sowie Partnern wie AT&T, Verizon, Vodafone, Microsoft, Google und Apple genutzt. Lookout hat seinen Hauptsitz in San Francisco und Niederlassungen in Amsterdam, Boston, London, Sydney, Tokio, Toronto und Washington, DC. Weitere Informationen finden Sie unter www.lookout.com/de. Folgen Sie Lookout auf seinem Blog sowie bei LinkedIn und Twitter.

