Lookout®

Leitfaden für CISOs zur Sicherung von Remote-Mitarbeitern

10 Use Cases für Datentransparenz, Datenschutz und Compliance in einer mobilen SaaS-Umgebung

Whitepaper

Inhalt

Hinweis

Veröffentlichungen von Lookout dienen ausschließlich allgemeinen Informationszwecken. Die Informationen in dieser Veröffentlichung werden ohne Gewähr bereitgestellt. Jegliche weiteren Entwicklungen oder Forschungsergebnisse nach Veröffentlichungsdatum sind in diesem Bericht nicht berücksichtigt.

Die letzten Wochen haben einen völlig neuen Trend gezeigt: Branchen aller Sektoren führen Richtlinien für die Remote-Arbeit globaler Mitarbeiter ein, um sich auf die neue Normalität vorzubereiten und die Geschäfte am Laufen zu halten. Die plötzliche Zunahme an Remote-Mitarbeitern ist fraglos eine Belastung für bestehende Netzwerkinfrastrukturen und führt bei vielen zu mangelnder Konnektivität und Sicherheit. Organisationen müssen Datenschutz- und Compliance-Vorgaben in dieser neuen Remote-Arbeitsumgebung irgendwie einhalten und setzen daher eine Cloud-First-Strategie ein. Diese soll Geschäftskontinuität und Hochverfügbarkeit von Servern und Anwendungen sicherstellen. Allerdings verbinden sich Remote-Mitarbeiter über nicht verwaltete Geräte direkt mit dem Internet und arbeiten in SaaS-Anwendungen an ihren alltäglichen Aufgaben. Das erhöht wiederum wesentlich das Risiko von Datensicherheitsverletzungen, Compliance-Verstößen und Verlust vertraulicher Informationen.

„IT-Teams benötigen Einblicke in die Daten und Aktivitäten von Remote-Mitarbeitern, um sensible und personenbezogene Daten zu schützen."

Salah Nassar,
Vice President of Marketing,
Lookout

Diese einzigartigen Herausforderungen im Zusammenhang mit digitalen Transformationen und Home-Office lassen sich nur mit einer zukunftssicheren Technologie mit umfassenden Sicherheitsfunktionen bewältigen, die Daten vom Gerät bis zur Cloud und umgekehrt verfolgen. Cloud Access Security Broker (CASB) wurden speziell dafür entwickelt, Unternehmensdaten in einer mobilen Cloud-Umgebung zu schützen. So können Unternehmen Cloud-Anwendungen und -Dienste nahtlos einsetzen. Ein CASB liefert erweiterte Lösungen für Transparenz, Datenschutz, Bedrohungsabwehr und Kontrollen für umfassenden Compliance-Support – für erfolgreiche und sichere Cloud-Bereitstellungen. Die Lookout CASB-Plattform ergänzt traditionelle CASB-Funktionen durch leistungsstarke benutzer- und datenorientierte Kontrollen zur Richtliniendurchsetzung. Diese dienen als sicherer Puffer zwischen Cloud-Anbietern und deren Kunden. CASB fungiert als Security Gatekeeper, um Daten zu schützen und Benutzer von Cloud-Bedrohungen und den damit verbundenen Risiken für Unternehmensnetzwerke zu isolieren.

„Lookout ebnet den Weg zu einem neuen Zeitalter der sicheren Multi-Cloud-Nutzung. CASB ist die einzige Lösung, die innovative Funktionen mit leistungsstarkem Datenschutz kombiniert und dabei Benutzer, Geräte und Daten in jeder Cloud komplett schützt. Wir sind überzeugt, dass die Positionierung von Lookout als „Visionär" im Gartner Magic Quadrant unser Verständnis und unseren innovativen Ansatz für den Cloud Security-Markt bestätigt."

Pravin Kothari,
Lookout EVP,
Product and Strategy, SASE

Dieser Leitfaden gibt einen Einblick in die wichtigsten CASB-Use Cases zur Sicherung von Remote-Arbeitsumgebungen, um Geschäftskontinuität und eine hohe Investitionsrentabilität für CASB-Benutzer zu ermöglichen. Die Top Threats Working Group der Cloud Security Alliance hat einen umfassenden Report über die Top-Bedrohungen des Cloud Computing veröffentlicht und die aktuellsten, von Experten bewerteten Erkenntnisse über Cloud-Sicherheitsrisiken ermittelt. Dazu gehören Hijacking von Cloud-Konten, Cloud-Datensicherheitsverletzungen, unsichere APIs, falsche Konfiguration und Administrationsfehler, Missbrauch von Systemschwachstellen sowie mehr potenziell böswillige Insider, Advanced Persistent Threats und vieles mehr. Alle diese genau definierten Bedrohungen werden in den CASB Use Cases direkt angesprochen und durch den Einsatz von Lookout CASB verhindert.

USE CASE 1

Vollständige Transparenz der im Unternehmen genutzten Cloud-Anwendungen

Schwachstelle

Das durchschnittliche Unternehmen kann Hunderte Cloud-Anwendungen unterschiedlicher Größe verwenden. Wir schätzen aber, dass das typische IT-Team keinen Überblick über alle genutzten Anwendungen hat. Sie müssen komplett über die ganze Cloud-Nutzung informiert sein, um Unternehmensrichtlinien und Datenschutzgesetze einzuhalten, Informationstechnologie und rechtliche Ressourcen effizient zu nutzen und sicherzustellen, dass die Unternehmenssicherheit nicht durch übersehene Freigaben und Sicherheitslücken gefährdet ist.

Beispiel für Schwachstelle

Eine Gesundheitseinrichtung hat eine Home-Office-Richtlinie aufgestellt, aber das IT-Team kann nicht alle Benutzer verfolgen, die sich direkt mit der Cloud verbinden und sensible PHI-Daten über SaaS-Apps freigeben. Der mangelnde Einblick in die genehmigte und nicht genehmigte Cloud-Nutzung kann zu Datenlecks und einer HIPAA-Verletzung für die Einrichtung führen.

Kosten, wenn nicht gelöst

Wenn Sie es versäumen, alle genutzten Clouds zu identifizieren, kann das hohe Kosten mit sich bringen. Die Nutzung nicht genehmigter Clouds setzt das Unternehmen dem Risiko einer unautorisierten Offenlegung oder des Verlusts sensibler, proprietärer und regulierter Daten aus. Wenn Unternehmensmitarbeiter Daten in nicht genehmigte Clouds verschieben, können sie das Unternehmen unwissentlich einer Compliance-Verletzung aussetzen. Diese kann wiederum zu hohen Geldstrafen, Rufschädigung und mehr führen.

CASB – Lösung und Vorteile

CASB Shadow IT Discovery streamt Protokolle von jedem Netzwerkgerät und ermöglicht die automatisierte Erkennung aller verwendeten Clouds. Shadow IT Discovery liefert einen klaren Einblick in das Unternehmensrisiko. Dazu werden über 20.000 Cloud-Anwendungen gescannt und über 60 Attribute analysiert, um die Cloud-Apps mit dem größten Risiko eines Verlusts sensibler Daten zu identifizieren und zu klassifizieren.

CASB nutzt auch Deep Application Intelligence (umfassende Anwendungseinblicke), um nicht nur hoch- und heruntergeladene Daten, sondern alle wesentlichen Anwendungsaktivitäten zu schützen. CASB erkennt verschiedene genutzte Anwendungsinstanzen und unterscheidet zwischen diesen, um die externe Zusammenarbeit zu verwalten und offene Freigaben zu verhindern. So werden Dateien und Ordner in Echtzeit gesichert.

„TRANSPARENZ ist für Cloud-Sicherheit und Compliance entscheidend. Die IT- und Sicherheitsteams müssen alle von einer Organisation genutzten Cloud-Dienste identifizieren können. Sie müssen die Risiken der von der Organisation genutzten Clouds verstehen und ein vollständiges Audit-Log der Benutzeraktivitäten erhalten, um forensische Untersuchungen zu unterstützen. All das muss ohne Kompromisse möglich sein."

Sundaram Lakshmanan,
Chief Technology Officer, Lookout

USE CASE 2

Einblick in historische Cloud-Daten

Schwachstelle

Zur Erfüllung geschäftlicher Anforderungen setzen Unternehmen zunehmend auf SaaS- und IaaS-Clouds. Daher können sensible Daten in mehreren Apps, Datenbanken und persönlichen Geräten aufbewahrt werden. Ohne angemessene Transparenz riskieren Unternehmen Compliance-Verstöße, Sicherheitsschwachstellen und Datenlecks. Unternehmen müssen sich unbedingt einen Überblick über alle archivierten oder historischen Daten verschaffen, die schon seit Jahren in ihrer Cloud aufbewahrt werden.

Beispiel für Schwachstelle

Ein Unternehmen, das im US-Bundesstaat Kalifornien tätig ist, möchte sicherstellen, dass seine Geschäftsabläufe mit den CCPA-Vorschriften übereinstimmen. Es hat die Sicherheit seiner Cloud-Anwendung mit einer Cloud-Datenschutzlösung aufgerüstet, die alle Kundendatensätze in Echtzeit verschlüsselt. Allerdings hat es nicht die historischen Daten auditiert, die seit Jahren in der Cloud gehostet werden. Ein kurzer Scan dieser Daten hat mehrere Compliance- und Datenschutzverletzungen aufgedeckt.

Kosten, wenn nicht gelöst

Wenn Sie es versäumen, alle sensiblen Inhalte in den Clouds zu identifizieren, kann das hohe Kosten mit sich bringen. Ein DSGVO- oder CCPA-Verstoß kann enorme finanzielle Auswirkungen auf das Unternehmen haben. Darüber hinaus müssen Sie bei aktiven Cyberangriffen schnell reagieren und zum Schutz gefährdeter Daten und Ressourcen die Aktivitäten der Cyberangriffe nachvollziehen können.

CASB+ – Lösung und Vorteile

Mit CASB+ Cloud Data Discovery (CDD) können Organisationen bereits in führenden SaaS-Anwendungen gespeicherte Daten erkennen und klassifizieren. Bei den ersten CASB-Versionen lag der Schwerpunkt auf den Daten, die in die Cloud hochgeladen wurden. Sie boten aber keinen Einblick in die Daten, die bereits in der Cloud gespeichert waren. Mit Cloud Data Discovery können Organisationen historische Daten über mehrere Cloud-Apps hinweg scannen – direkt von Informationen auf Feldebene in strukturierten Clouds, wie ServiceNow und Salesforce, sowie unstrukturierten Daten und Dateien in Collaboration-Apps, wie Office 365, Slack und Box.

USE CASE 3

Automatische Erkennung und Beseitigung von bösartigem Benutzerverhalten

Schwachstelle

Überwachen Sie unbedingt die Benutzeraktivitäten in der mobilen Cloud-Umgebung. So können Sie ungewöhnliche Mitarbeiteraktivitäten erkennen und darauf reagieren, wenn sie auf bösartiges Verhalten oder kompromittierte Anmeldedaten und einen aktiven Cyberangriff hinweisen.

Beispiel für Schwachstelle

Eine Mitarbeiterin meldet sich um 03:00 Uhr nachts von einem Privatgerät bei ihrem Konto an. Sie arbeitet seit drei Jahren im Unternehmen und hat sich selbst bei Heimarbeit noch nie in diesem Zeitraum angemeldet. Oder ein Mitarbeiter aus Chicago, Illinois, meldet sich von zu Hause an und versucht nur zwei Stunden später, sich von Peking anzumelden.

Kosten, wenn nicht gelöst

Externe Bedrohungen und bösartiges Mitarbeiterverhalten können zu erheblichen finanziellen Verlusten, Rufschädigung, Markenschädigung und Geldstrafen aufgrund von Compliance-Verletzungen führen.

CASB – Lösung und Vorteile

Lookout CASB umfasst fortschrittliche Benutzerverhaltensanalysen und Bedrohungsschutzfunktionen. Damit können Sie Ihre genehmigten Clouds und eigens entwickelten cloudbasierten Anwendungen sichern und vor nicht identifizierten und bösartigen Benutzern schützen.

Die CASB-Funktion der Benutzer- und Entitätsverhaltensanalysen (User and Entity Behavior Analytics, UEBA) überwacht die Benutzeraktivitäten mit maschinellem Lernen, einschließlich Tageszeit der Aktivität, versuchte Massendatei-Downloads und andere abweichende Verhaltensweisen. UEBA kann Echtzeitentscheidungen treffen, um ungewöhnliche Aktivitäten, die von normalen Mustern abweichen, zu kennzeichnen oder zu blockieren. CASB UEBA erfasst über 60 Attribute für jede Benutzeraktivität und generiert detaillierte Audit-Logs für forensische Analysen.

CASB Incident Insights erfasst jede Geräte-, Benutzer- und Anwendungsaktivität in der Cloud und liefert Drilldown-Berichte bis hin zu den letzten Details und Beziehungen.

USE CASE 4

Identifizierung und Schutz vor unautorisiertem Kontozugriff

Schwachstelle

Cloudbasierte Zusammenarbeit und Dateifreigabe nehmen rasant zu. Daher müssen Sie sicherstellen, dass nur die richtigen Benutzer auf SaaS-Anwendungen zugreifen, in denen sensible oder kritische Daten gespeichert sind.

Beispiel für Schwachstelle

Ein Cloud-Konto wird kompromittiert, weil Benutzeranmeldedaten gestohlen wurden, oder ein verifizierter Benutzer wird zu einem bösartigen Insider und stiehlt Unternehmensdaten.

Kosten, wenn nicht gelöst

Benutzeranmeldeinformationen sind der Schlüssel und Ihre Daten die Kronjuwelen. Wenn eines dieser beiden Elemente kompromittiert ist, hat das schwerwiegende Folgen und kann unter anderem zu Gerichtsverfahren, hohen Bußgeldern und Rufschädigung führen.

CASB – Lösung und Vorteile

Lookout CASB bietet End-to-End-Sicherheit für Benutzer und Daten von jedem Gerät an jedem Standort zu allen vertrauenswürdigen Cloud-Anwendungen. Damit ergreifen Unternehmen den ersten Schritt zu „Zero Trust"-Cloud-Sicherheit.

CASB lässt sich in IDaaS-Lösungen wie Okta integrieren, um die Benutzeridentität zu prüfen und den Zugriff mit Single Sign-On (SSO) und Mehrfaktorauthentifizierung (MFA) zu kontrollieren.

Lookout CASB Adaptive Access Control ergänzt die Integration in IDaaS und führt eine kontinuierliche Risikobewertung der verifizierten Benutzeranmeldungen von beliebigen Standorten oder Geräten bei Cloud-Anwendungen aus. Dadurch werden kontextbezogene Zugriffe ermöglicht und die Benutzeraktivitäten durchgängig mit einem Zero-Trust-Datensicherheitsansatz geschützt. CASB überwacht das Benutzerverhalten mit UEBA und kann basierend auf dem Risiko des Benutzerverhaltens Zugriffsberechtigungen entziehen oder eine erneute Anmeldung mit Step-up-Authentifizierung anfordern. So schützen Sie jede Benutzeraktion von Anmeldung bis Abmeldung.

USE CASE 5

Identifizierung und Sicherung der Kommunikation im Ruhezustand und bei der Übertragung

„DATENSCHUTZ mit durchgängiger Zero-Trust-Verschlüsselung ist mittlerweile unerlässlich, um Daten in der Cloud zu schützen. Daten müssen im Ruhezustand in der Cloud, bei der Übertragung über das Netzwerk, über APIs und mit anderen Mitteln sowie bei der Verwendung geschützt werden. Zu guter Letzt dürfen Ihre Datenverschlüsselungsschlüssel unter keinen Umständen an Externe weitergegeben werden. Diese Grundlagen sind jetzt wesentliche Bestandteile aktueller Best Practices."

Mahesh Rachakonda,
Vice President Product & Solution Engineering, Lookout

Schwachstelle

Unternehmen speichern viele Typen sensibler und eingeschränkter Daten, darunter geistiges Eigentum, Finanzdaten, von Compliance-Vorschriften als sensibel eingestufte Daten usw. Wenn die Sicherheitskontrollen für Daten nicht ausreichen, sind Datenlecks, Diebstahl von geistigem Eigentum und Compliance-Verstöße möglich. Organisationen müssen vollständige Transparenz und Kontrolle über sensible Daten bei der Übertragung oder im Ruhezustand einrichten – insbesondere für Mitarbeiter- und Kundendatensätze, die in CRM-, HRM- und ITES-Clouds wie Salesforce und ServiceNow gehostet werden, oder bei Zusammenarbeit über cloudbasierte E-Mail-Dienste und Informationsaustausch über mehrere SaaS-Anwendungen wie Office 365, Box, Google Drive und Slack.

Beispiel für Schwachstelle

Sensible Inhalte müssen mit Datenschutzkontrollen (Verschlüsselung, Maskierung, Klassifizierung) gesichert werden, bevor sie in die Cloud hochgeladen werden. Ein Remote-Mitarbeiter hat sich von zu Hause aus beim Box-Unternehmenskonto angemeldet und versehentlich mehrere Dokumente mit lesbaren Sozialversicherungsnummern hochgeladen. Mitarbeiter können sensible Inhalte von der Cloud herunterladen und per E-Mail an externe Personen senden. Dadurch entsteht eine zusätzliche Compliance-Verletzung, da diese Daten nicht ohne Schutz durch Anonymisierung in die Cloud hochgeladen werden dürfen.

Kosten, wenn nicht gelöst

Wenn diese Daten nicht verschlüsselt sind und eine Datensicherheitsverletzung auftritt, ist das Unternehmen Bußgeldern im Zusammenhang mit Compliance-Verletzung, Meldepflicht, Risiken der Ruf- und Markenschädigung und mehr ausgesetzt.

CASB – Lösung und Vorteile

Lookout CASB Data Loss Prevention (DLP) umfasst detaillierte Richtlinienkontrollen, um eingeschränkten und sensiblen Inhalt in Echtzeit zu identifizieren. CASB DLP ermöglicht Multi-Cloud-Schutz mit einer einheitlichen DLP-Schnittstelle, um Daten über zahlreiche SaaS- und IaaS-Clouds und sogar eigens entwickelte Anwendungen hinweg zu schützen. Sie können CASB auch in Ihre vorhandenen DLP-Produkte integrieren, damit Sie Richtlinien konsistent im ganzen Unternehmen anwenden und Ihre Sicherheitsinvestition so weiter schützen können.

Zum Schutz von E-Mail-Daten bietet Lookout die erste sichere E-Mail-Gateway-Lösung der Branche. Diese ist in CASB integriert, sodass E-Mails von jedem Clientgerät (Desktop, Mobilgerät, Browser) über ein sicheres dediziertes Gateway weitergeleitet werden können. Gleichzeitig werden DLP-Richtlinien für die E-Mails durchgesetzt, bevor diese an die Empfänger zugestellt werden. Der Schutz von E-Mail-Daten umfasst die Maskierung sensibler Inhalte in Betreff und Hauptteil, Datenrechteverwaltung und Verschlüsselung von Anhängen.

USE CASE 6

Sicherung der Offline-Zusammenarbeit

Schwachstelle

Datenschutzfunktionen für sensible Inhalte müssen beim Herunterladen von der Cloud beibehalten werden. Verwaltung von Informationsrechten (Information Rights Management, IRM) wurde ursprünglich zum Schutz urheberrechtlich geschützter Materialien in lizenzierter Verteilung entwickelt. Damit können Unternehmen und Regierungsbehörden den Zugriff auf digitale Dokumente steuern, die urheberrechtlich geschütztes Material, geistiges Eigentum, Betriebsgeheimnisse und andere sensible und vertrauliche Daten enthalten können. Ein IRM-Unternehmenssystem dient dazu, unautorisierte Zugriffe sowie das Weitergeben und die weitere Verteilung dieser digitalen Daten zu verhindern.

Beispiel für Schwachstelle

Ein Remote-Mitarbeiter lädt ein sensibles Dokument von einer Ihrer Clouds in sein Mobilgerät herunter und sendet es per E-Mail an einen externen Partner. Ohne angemessene Datenschutztools in der Cloud können Sie nicht verhindern, dass Remote-Mitarbeiter geistiges Eigentum herunterladen und offline weitergeben.

Kosten, wenn nicht gelöst

Wenn Daten für eine nicht autorisierte Partei offengelegt werden, kann das zu finanziellen Verlusten, Ruf- und Markenschädigung, Compliance-Bußgeldern und mehr führen.

CASB – Lösung und Vorteile

Das umfassende Datensicherheitsportfolio von Lookout beinhaltet natives IRM für die Sicherung des Offline-Datenzugriffs. CASB IRM definiert Richtlinien, um zentralisierten Datenschutz und Verschlüsselungskontrollen auf die Daten anzuwenden, die von Cloud-Anwendungen auf die Geräte von Benutzern heruntergeladen werden. Dabei wird unter anderem festgelegt, welche Geräte auf die Daten zugreifen dürfen (beispielsweise, dass Benutzer nicht mit persönlichen Geräten auf sensible Daten zugreifen können). Falls heruntergeladene Daten vor missbräuchlicher Verwendung geschützt werden müssen (damit z. B. ehemalige Mitarbeiter keine Kundendaten an den neuen Arbeitgeber übermitteln), können Administratoren den Zugriff auf die Daten wieder zurückziehen, selbst wenn diese heruntergeladen und auf ein anderes Gerät kopiert wurden. Durch das Entziehen von Schlüsseln in Echtzeit können Sie Daten selbst auf verlorenen und gestohlenen Geräten schützen. Lookout CASB lässt sich auch in IRM-Pakete von größeren Drittanbietern integrieren, wie Microsoft.

USE CASE 7

Datenschutz bei einer Sicherheitsverletzung

Schwachstelle

Viele Cloud-Dienstanbieter unterstützen grundlegende Datenschutzfunktionen. Diese sind allerdings auf die Anwendungsebene beschränkt und können keine sensiblen Daten auf detaillierter Ebene kontrollieren und verschlüsseln. Darüber hinaus verlangen diese Cloud-Anbieter Kopien Ihrer Datenverschlüsselungsschlüssel. Aufgrund dieser Sicherheitseinschränkungen sind Ihre Daten leider Fehlkonfigurationen, administrativen Fehlern oder Aktivitäten bösartiger Insider bei den Cloud-Anbietern ausgesetzt. Zu guter Letzt wird dabei auch noch die Offenlegung Ihrer Daten für diese Cloud-Anbieter ohne Ihr Wissen oder Ihre Zustimmung erzwungen.

Beispiel für Schwachstelle

Viele Datenschutzgesetze geben vor, dass Ihr Unternehmen Daten schützen und anonymisieren muss. Sie haben Ihre Clouds bei der Compliance-Prüfung gescannt und dabei festgestellt, dass der Großteil des Inhalts als Klartext vorliegt. Nur wenige Cloud-Dienste verschlüsseln Daten und das auch nur im Ruhezustand in der Datenbank. Darüber hinaus verkauft ein böswilliger Insider Kopien der Cloud-Datenverschlüsselungsschlüssel, die auf einer Ihrer SaaS-Clouds gehostet sind, an einen Dritten.

Kosten, wenn nicht gelöst

Wenn diese Daten nicht geschützt sind und eine Datensicherheitsverletzung auftritt, ist das Unternehmen Bußgeldern im Zusammenhang mit Compliance-Verletzung, Meldepflicht, Risiken der Ruf- und Markenschädigung und mehr ausgesetzt.

CASB – Lösung und Vorteile Lookout bietet Zero-Trust-Verschlüsselung, die Daten vollkommen ortsunabhängig schützt – im Ruhezustand, bei der Netzwerkübertragung, in Cloud-Anwendungsschichten (API, Middleware, Arbeitsspeicher) und bei der Verwendung. Die gemäß FIPS 140-2 zertifizierten Datenschutzfunktionen von Lookout erfüllen alle globalen Compliance-Vorschriften und bieten den höchsten Schutz vor Cyberbedrohungen. Dabei wehren sie komplexe Bedrohungen und Angriffe wie API-basierte Angriffe ab, die auf verschlüsselte Daten abzielen. Darüber hinaus bleiben die Datenverschlüsselungsschlüssel bei Ihnen und werden nie an den Cloud-Anbieter weitergegeben.

Die Tokenisierungslösung von Lookout richtet sich an Länder oder Regionen mit strengen Datenspeicherungsgesetzen, bei denen bestimmte Typen sensibler Daten die Landesgrenzen selbst verschlüsselt nicht überschreiten dürfen. Die Cloud-Tokenisierung von Lookout ersetzt sensible Felder durch nach dem Zufallsprinzip generierte Token, die strukturell ähnlich sind, aber keine mathematische Korrelation zu den Originaldaten aufweisen. So können Organisationen Cloud-Anwendungen nahtlos einsetzen, aber die Datensensibilität lokal beibehalten.

„Anbieter von SaaS-Anwendungen können eine Kopie Ihrer Datenverschlüsselungsschlüssel anfordern, um ihre Optionen zur Datenbankverschlüsselung zu unterstützen. Diese sollten Sie, mit Verlaub, nie weitergeben. Dadurch sind Sie weiteren Risiken ausgesetzt, wie bösartigen Insidern beim Anbieter, Datenoffenlegung wegen Fehlkonfiguration, möglicher erzwungener Offenlegung ohne Ihr Wissen, Nichteinhaltung vieler verschiedener Vorschriften und mehr. Dank der Zero-Trust-Verschlüsselung von CipherCloud CASB+ können Sie dieses Problem umgehen.“

Pravin Kothari,
Mitgründer und CEO, Lookout

USE CASE 8

Echtzeitverwaltung von Mobilgeräten mit Kontrollen zur Endgerätesicherheit

Schwachstelle

Mobilgeräte können gestohlen, per „Jailbreak" entsperrt oder auf andere Weise nicht konform werden. Durch Jailbreaking werden Einschränkungen der Sicherheitssoftware aufgehoben, indem Hersteller- oder Netzbetreibereinschränkungen von der Plattform eines Mobilgeräts entfernt werden. In diesem Zusammenhang müssen Sie unbedingt Richtlinien implementieren, die den Gerätezugriff einschränken und das Herunterladen von Inhalten speziell blockieren. Diese Richtlinien müssen die Nutzungseinschränkung und das Herunterladen von Daten in BYOD-Geräte (Bring Your Own Device), COPE-Geräte (Corporate Owned, Personally Enabled) oder COBO-Geräte (Company Owned, Business Only) ermöglichen.

Beispiel für Schwachstelle

Ein Firmenmobilgerät ist verloren gegangen und der Administrator möchte den gesamten Zugriff auf Unternehmensdateien von diesem Gerät aussetzen. In einem anderen Beispiel ist die installierte Firewall ausgefallen oder falsch konfiguriert.

Kosten, wenn nicht gelöst

Wenn Daten an eine nicht autorisierte Partei offengelegt werden, kann das zu finanziellen Verlusten, Ruf- und Markenschädigung, Compliance-Bußgeldern und mehr führen.

CASB – Lösung und Vorteile

Die Geräteverwaltungslösung von Lookout unterstützt interne und externe Zusammenarbeit, Remote-Entzug von Schlüsseln bei verlorenen oder kompromittierten Geräten in Echtzeit sowie Dateientschlüsselung in mobilen und Endgeräte-Apps durch autorisierte Benutzer. Dazu ist die Lösung in VMWare Airwatch integriert, einer Anwendung der Unternehmensklasse für Mobile Device Management.

USE CASE 9

Bewahrung der Konfigurationsintegrität von IaaS- und SaaS-Clouds

Schwachstelle

Advanced Persistent Threats können oft in Cloud-Umgebungen eindringen und dort Daten kompromittieren. Im Netzwerk können sie den Netzwerkverkehr abhören und Fehlkonfiguration und administrative Fehler identifizieren, die den Datenzugriff ermöglichen. Um Sicherheits- und Compliance-Anforderungen zu erfüllen, müssen Sie das verhindern.

Beispiel für Schwachstelle

Remote-Arbeit ist jetzt die neue Normalität. Daher müssen Sicherheits- und Betriebsteams mehrere Sicherheitskontrollen mit 360-Grad-Kontrolle und -Transparenz für Daten und Remote-Benutzer aktivieren. Selbst ein kleiner Anwenderfehler oder eine geringfügige Sicherheitslücke kann zu einem enormen Datenleck für die gesamte Organisation führen. Es gibt viele Beispiele für Fehlkonfigurationen, die zu Datenoffenlegung und unautorisiertem Zugriff auf Cloud-Daten geführt haben. Im Oktober 2017 wurde gemeldet, dass Accenture versehentlich einen enormen Speicher privater Daten in vier ungesicherten Cloud-Servern aufbewahrt hat. So wurden hoch sensible Passwörter und geheime Entschlüsselungsschlüssel offengelegt, die dem Unternehmen und seinen Kunden erheblich hätten schaden können.

Kosten, wenn nicht gelöst

Cyberangriffe, kompromittierte Anmeldedaten und bösartiges Mitarbeiterverhalten können zu erheblichen finanziellen Verlusten, Rufschädigung, Markenschädigung und Geldstrafen aufgrund von Compliance-Verletzungen führen.

CASB – Lösung und Vorteile

Lookout Cloud Security Posture Management (CSPM) bewertet automatisch Ihre Cloud-Landschaft gemäß genau definierten Sicherheits- und Compliance-Richtlinien. Dadurch erhalten Sie einen vollständigen Einblick in Ihr Cloud-Risiko anhand von intuitiven Drilldown-Dashboards. Lookout CSPM schützt kritische Administrations- und Konfigurationskontrollen in Ihren SaaS- und IaaS-Clouds, wie Office 365, Amazon AWS, Microsoft Azure und Google Cloud Platform, durch kontinuierliche Überwachung und Echtzeit-Schutzvorrichtungen. CSPM reduziert die betriebliche Komplexität mit einer zentralisierten Lösung für alle Cloud-Dienste und die gesamte Infrastruktur, verhindert Datenverlust aufgrund von Fehlkonfigurationen und sorgt für Einhaltung der aktuellen Compliance-Richtlinien (DSGVO, CCPA, HIPAA, PCI) in einer Multi-Cloud-Infrastruktur.

USE CASE 10

Integration in bestehende Sicherheitsinfrastrukturen des Unternehmens

Schwachstelle

Viele Organisationen haben hohe Beträge in Unternehmenssicherheitslösungen wie DLPs, SIEMs, SSOs, AVAMs usw. investiert. Sie möchten diese Investitionen nicht nur im Hinblick auf den ROI schützen, sondern auch auf den Zeitaufwand für Schulung der Mitarbeiter, Aufbau der Sicherheitsinfrastruktur und Aufstellung von Richtlinien und Korrektur-Workflows zum Erfüllen der Geschäftsanforderungen.

Beispiel für Schwachstelle

Eine Organisation hat viel Geld in eine lokale DLP-Lösung mit umfassenden Sicherheitsfunktionen investiert, die den Datenverkehr am Endgerät prüft und entsprechend darauf reagiert. Die Organisation hat zwar eine Cloud-Sicherheitslösung übernommen, um ihre Ressourcen in der Cloud zu schützen, möchte aber nicht auf die Funktionen der bestehenden DLP-Lösung verzichten – obwohl die Cloud-Sicherheitslösung ebenfalls integrierten DLP-Support aufweist.

Kosten, wenn nicht gelöst

Mangelnde Integration mit lokalen Unternehmenssicherheitslösungen kann mehrere isolierte Bereitstellungen für den Schutz von Unternehmensressourcen zur Folge haben. Dadurch werden Netzwerkinfrastruktur und -verwaltung komplexer. Außerdem kann so das Risiko von Sicherheitslücken und Datenlecks erhöht werden.

CASB+ – Lösung und Vorteile

Die Lookout CASB-Plattform ermöglicht die Integration in vorhandene Sicherheitslösungen, um bereits getätigte Investitionen, darunter EDLP, SSO und Antivirus/Antimalware-Lösungen, voll auszuschöpfen. Außerdem können Kunden sie in bestehende SIEM-Lösungen integrieren und Daten von Unternehmens-Firewalls und Proxys nutzen. So erhalten sie weitere Einblicke in alle verwendeten Clouds, einschließlich nicht genehmigte SaaS-Anwendungen (Schatten-IT).

CASB lässt sich in externe DLP-Lösungen wie Symantec DLP integrieren. Damit können Organisationen vorhandene unternehmensspezifische DLP-Richtlinien beibehalten und auf Daten erweitern, die in SaaS- und Cloud-Dienste hochgeladen werden. Mit dieser Lösung können Organisationen umgebungsspezifische Richtliniendetails aufrecht erhalten und gleichzeitig von der Verschlüsselung und Richtliniendurchsetzung von Lookout profitieren.

Dank CASB-Integration mit SSO-Diensten wie Okta können Sie Zugriffsrichtlinien für Anmeldeaktionen erstellen und anwenden. Dadurch lassen sich Anmeldeaktivitäten bei SaaS- und IaaS-Anwendungen genauer kontrollieren.

CASB Antivirus/Antimalware (AVAM) unterstützt das Virenschutzprogramm Bitdefender und erkennt so viele Malware-Typen noch besser, darunter Zero-Day-Bedrohungen, Viren, Spyware, Ransomware, Würmer und Bots.

CASB-Integration in VMware Workspace ONE (AirWatch) ermöglicht die kontextbezogene Zwei-Faktor-Authentifizierung. Ein Unternehmen kann die Zwei-Faktor-Authentifizierung auslösen, wenn ein bestimmter Kontextfaktor, wie Standort, Netzwerk, Daten oder ungewöhnliches Benutzerverhalten, auftritt. CASB nutzt Azure Information Protection (AIP) für DRM und Dokumentenklassifizierung und erweitert AIP auf jedes Dokument in jeder Cloud, einschließlich exportierte Berichte mit sensiblen Informationen.

CASB+ amortisiert sich schnell

Agentenlose Architektur für schnellere Bereitstellungen

CASB unterstützt Reverse-Proxy-basierte Bereitstellungen (CASB Mobile Connect) und liefert so sichere agentenlose Konnektivität für mobile und nicht verwaltete Geräte. Dadurch können Sie CASB schnell und reibungslos bereitstellen und alle CASB-Funktionen ohne ressourcenintensive Installation von Agenten oder aufwendige Wartung nutzen.

Unterstützung für all Ihre Clouds

CASB unterstützt zahlreiche gängige SaaS-basierte Geschäftsanwendungen, darunter Office 365, Slack, Salesforce, Amazon Web Services, SAP SuccessFactors, ServiceNow, Adobe, Box, Dropbox und viele weitere. CASB schützt Anwendungsinhalte und erhält dabei Anwendungsfunktionen aufrecht. Gleichzeitig erhalten Sie damit mehr Compliance-Funktionen als mit dem Angebot des SaaS- oder IaaS-Anwendungsanbieters. So können Sie Ihre Daten mit einem konsistenten Ansatz und einer einheitlichen Frontend-Schnittstelle schützen und für Compliance in allen Ihren Cloud-Umgebungen sorgen.

Unterstützung für benutzerdefinierte Anwedungen

Mit dem Lookout CASB-Konnektor „AnyApp" können Kunden die leistungsstarken Datenschutzfunktionen für ihre eigenen cloudbasierten Anwendungen integrieren. AnyApp bindet Verschlüsselung, Tokenisierung, dynamische Zugriffskontrolle, DRM, UEBA, Bedrohungsschutz und viele weitere nützliche Sicherheitsfunktionen in die speziell entwickelten cloudbasierten Anwendungen von Kunden ein. So werden eigene Unternehmensanwendungen in jeder Cloud-Plattform geschützt.

Die weltweit größten Unternehmen nutzen Lookout CASB

- 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 verfügt über 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, LinkedIn und Twitter.