Lookout®

Lookout-Komplettschutz für ServiceNow®

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 Report nicht berücksichtigt.

Inhalt

„Im Oktober 2017 hat Gartner die 11 führenden CASB-Lösungen im Hinblick auf verschiedene Merkmale bewertet, darunter Architektur, Datensicherheit, Bedrohungsschutz, UEBA, Compliance/Risiko und Unternehmensintegration. Die Lookout CASB-Plattform hat in allen bewerteten Bereichen die Höchstpunktzahl von 100 % erreicht. Wir bieten Benutzern von ServiceNow eine einzigartige Kombination aus höchster Datensicherheit, leistungsstarker End-to-End-Verschlüsselung und umfassendem Bedrohungsschutz. Dieser Schutz kann auch auf jede andere Kombinationen aus Cloud-Anwendungen im Unternehmen ausgeweitet werden."

Pravin Kothari
Lookout EVP, Product and Strategy, SASE

Zusammenfassung

Dieses Dokument bietet einen Überblick über die Merkmale und Funktionen der Cloud Access Security Broker (CASB)-Plattform von Lookout und deren beispiellosen Sicherheits- und Compliance-Vorteile für Kunden der ServiceNow®-Cloud. Dabei werden der Umfang und die Vielseitigkeit der Sicherheitsfunktionen und deren positive Auswirkungen auf die Datensicherheit und Compliance für alle Kunden von ServiceNow-Lösungen genau untersucht.

CipherCloud richtet sich an Kunden, die bestimmte Compliance-Anforderungen im Hinblick auf Datensicherheit, Datenschutz und Datenaufbewahrungsort in der ServiceNow-Cloud erfüllen müssen. In letzter Zeit wurden vermehrt Datenlecks bei Cloud-Diensten öffentlich. Das verdeutlicht noch einmal, wie wichtig es ist, sensible Daten zu schützen, um das Cybersicherheitsrisiko zu mindern.

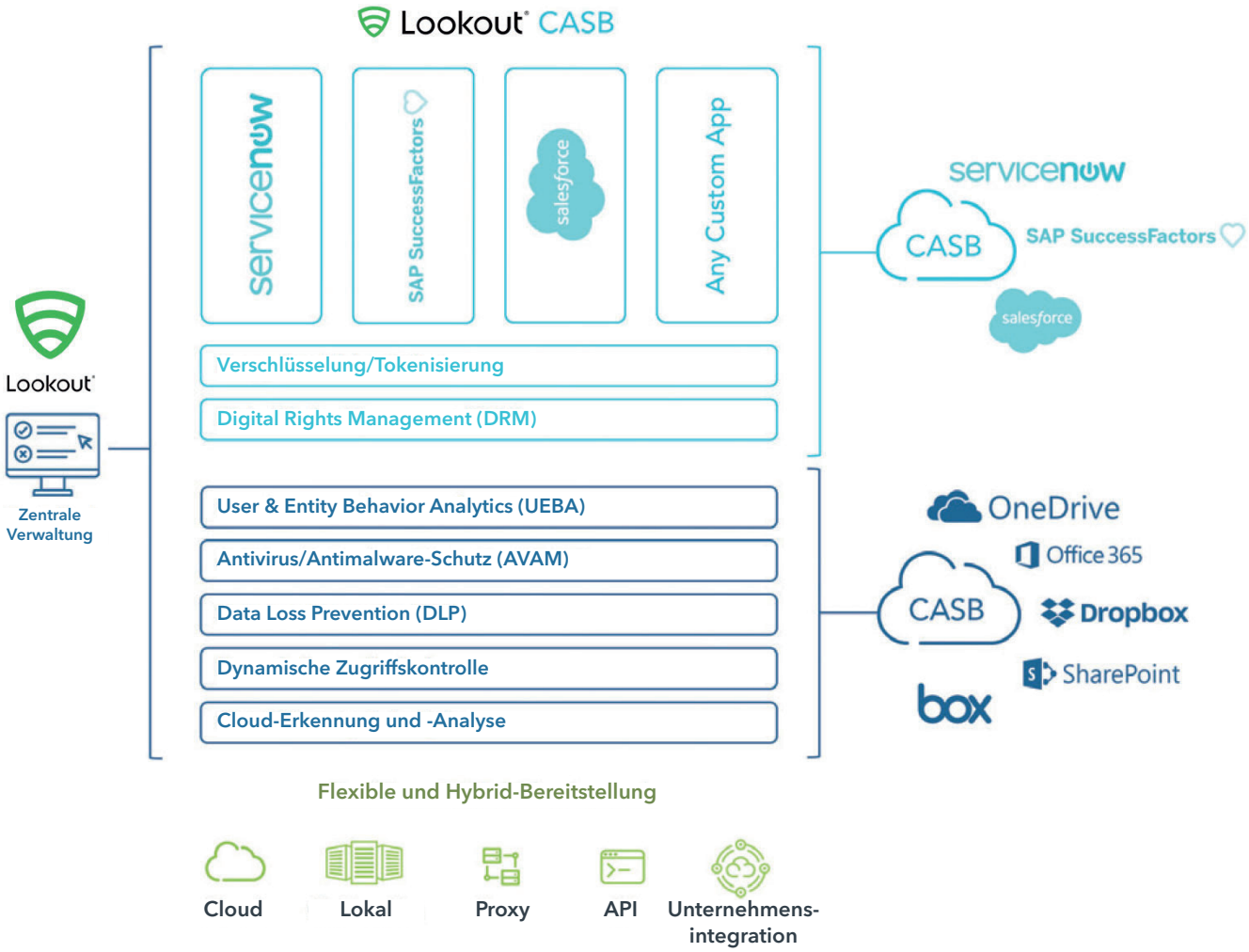
CipherCloud bietet zahlreiche Transparenz-, Datenschutz-, Bedrohungsschutz- und Compliance-Funktionen, die zusammengenommen eine optimale Lösung für den Komplettschutz Ihrer ServiceNow-Clouds bereitstellen. Die CipherCloud-Plattform ist nicht nur für Benutzer von ServiceNow, sondern auch für andere Clouds in derselben Plattform verfügbar.

Die Funktionen in CipherCloud werden über leistungsstarke richtliniengesteuerte Kontrollen implementiert, mit denen Sie unterschiedliche Anforderungen an strenge Zugriffskontrolle, Schutz sensibler Inhalte, Bedrohungsschutz und vieles mehr erfüllen können. Transparenzkontrollen sind ebenfalls wichtig, da Organisationen die verschiedenen von Mitarbeitern genutzten Cloud-Dienste verfolgen und das damit verbundene Risiko streng kontrollieren müssen.

CASB-Funktionalität für ServiceNow

Die Lookout CASB-Plattform bietet detaillierte Einblicke, End-to-End-Datenschutz, Advanced Threat Protection und umfangreiche Compliance-Funktionen für Benutzer der ServiceNow-Cloud. Mit der cloudnativen CASB-Plattform werden vertrauliche und sensible Daten an allen Standorten – sowohl in der Cloud als auch auf Benutzergeräten – vor unautorisiertem Zugriff und Datenfreigabe geschützt.

Außerdem können Unternehmen mit den CASB-Funktionen nicht nur die ServiceNow-Anwendung, sondern auch Multi-Cloud-Umgebungen sicher einsetzen. CASB bietet dieselben Vorteile für SaaS, PaaS und IaaS, damit Ihre Daten stets geschützt sind. Darüber hinaus ermöglicht AnyApp die Integration speziell entwickelter Cloud-Anwendungen ohne komplexe SDK- oder Anwendungsänderungen.



Die Lookout CASB-Plattform bietet detaillierte Einblicke, End-to-End-Datenschutz, Advanced Threat Protection und umfangreiche Compliance-Funktionen für Benutzer der ServiceNow-Cloud.

CASB-Funktionen für ServiceNow

Transparenz

Mit Lookout erhalten Sie einen umfassenderen Einblick in die komplette Cloud-Infrastruktur. Lookout CASB erkennt automatisch Schatten-IT und genutzte Cloud-Ressourcen im ganzen Unternehmen. So wissen das IT-, das Sicherheits- und das Compliance-Team genau, was im ganzen Unternehmen vor sich geht. Das durchschnittliche Unternehmen nutzt über 500 Clouds in verschiedenen Größenordnungen. Wir schätzen aber, dass das typische IT-Team nur einen Teil davon einsehen kann. Nach der Erkennung sollten Sie das potenzielle Risiko dieser Clouds für die Organisation beurteilen und entsprechende Maßnahmen ergreifen, um dieses zu mindern.

Lookout bietet außerdem Einblick in die Aktivitäten und die Zusammenarbeit von Benutzern, die wichtige und potenziell sensible Unternehmensdaten betreffen. Einfache Kontrollen unterstützen die Zusammenarbeits-Governance und die Freigabe zwischen verschiedenen internen und externen Gruppen. Lookout CASB bietet zudem noch Kontrollen, die den Upload sensibler Daten in einen externen Ordner einschränken, Links zu Ordnern mit sensiblen Daten automatisch entfernen und den Freigabeumfang genau definieren. Zu guter Letzt werden diese detaillierten Einblicke in Aktivitätsprotokollen für Compliance-Berichte, Audits und forensische Untersuchungen erfasst.

Datensicherheit

Datenschutz

Lookout bietet erstklassige Verschlüsselung für Ihre ServiceNow-Cloud. Bei der Verschlüsselung werden sensible Daten in unlesbaren Text konvertiert. So können eventuell kompromittierte Daten nicht genutzt werden und gelten

somit nicht als Datenleck. Gemäß Best Practices der Branche für eine Vielzahl globaler Compliance-Vorschriften müssen Daten bei der Übertragung (über das Netzwerk), bei der Verwendung (auf dem Clientgerät) und im Ruhezustand (in der Datenbank) verschlüsselt werden. Die Entschlüsselungsschlüssel müssen separat gespeichert werden. Sie dürfen nie an den Cloud-Anbieter weitergegeben werden, da dies einige globale Compliance-Anforderungen verletzen könnte. Sie haben die alleinige Kontrolle über die Verschlüsselung und Schlüsselverwaltung von Lookout. So können Sie Datensicherheitsanforderungen ganz einfach und flexibel in einer skalierbaren Plattform erfüllen.

Lookout CASB ist die einzige Cloud-Sicherheitsplattform, die auch Tokenisierung als Ergänzung der Verschlüsselungsfunktion anbietet. Dabei werden die Originaldaten durch ein „Token" ersetzt, das keine Informationen aus dem Originalinhalt enthält. Im Gegensatz zur Verschlüsselung gibt es bei diesem Ansatz keine mathematische Korrelation zwischen dem Token und den Originaldaten. Die Tokenisierung wird auch als Datenmaskierung bezeichnet und häufig in Ländern oder Regionen mit strengen Datenaufbewahrungsgesetzen verwendet, in denen bestimmte Typen sensibler Daten die Landesgrenzen nicht überschreiten dürfen. Die Tokenisierung wird auch häufig zur PCI-Compliance eingesetzt und erfüllt Anforderung 3 des PCI Data Security Standard (PCI DSS).

Data Loss Prevention (DLP)

Lookout DLP identifiziert Inhalt in Echtzeit und unterstützt benutzerdefinierte und standardmäßige native ServiceNow-Objekte. Diese leistungsstarke Funktion erkennt sensible Daten sowohl in strukturierten als auch in unstrukturierten Objekten. Bei Richtlinienverletzungen setzt Lookout DLP Aktionen wie Alarme, eingeschränkte Freigabe oder automatische Verschlüsselung sensibler Dateien durch. Richtlinien können auch so eingestellt werden, dass Benutzer Zeit haben, identifizierte Probleme selbst zu beheben. Kunden können DLP-Richtlinien in vorhandene lokale DLP-Unternehmenssysteme integrieren. Der globale Datensicherheitsreport von CipherCloud hat ergeben, dass nahezu 20 % der Unternehmenskunden Tokenisierung benötigen. In bestimmten Regionen wie Europa und Asien-Pazifik war die Tokenisierung das einzige wesentliche Datentool zum Schutz vor versehentlichen Compliance-Verstößen.

Digital Rights Management (DRM)

Unsere umfassende Datensicherheit beinhaltet auch natives DRM, z. B. für sicheren Offline-Datenzugriff. Daten, die von ServiceNow auf das Gerät eines Benutzers heruntergeladen werden, können nach vordefinierten Richtlinien geschützt 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 neue Unternehmen 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. CipherCloud lässt sich auch in DRM-Pakete von größeren Drittanbietern integrieren, wie Microsoft.

Schutz vor Bedrohungen

User Entity and Behavior Analytics (UEBA)

Lookout für ServiceNow umfasst eine Advanced Threat Protection-Funktion zum Schutz Ihrer ServiceNow-Cloud. Unsere UEBA-Funktion 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.

Adaptive Zugriffskontrolle

Unsere adaptive Zugriffskontrolle kann den Zugriff (selbst für augenscheinlich autorisierte Benutzer) ebenfalls blockieren – abhängig von verwendeter Plattform, Tageszeit, Ursprungsort und anderen Faktoren, die auf Diebstahl, kompromittierte Anmeldedaten oder einen ausgefeilten Cyberangriff hinweisen können.

Antivirus/Antimalware-Schutz

Unsere Antivirus/Antimalware (AVAM)-Scans schützen vor Viren, Malware und Ransomware. Diese leistungsstarke Option trägt ebenfalls zur Sicherheit der ServiceNow-Daten bei. Dank URL-Linkschutz und einer lokalen Sandbox-Integration können wir selbst schwer zu fassende Zero-Day-Bedrohungen erkennen und beseitigen.

Lookout CASB ist die einzige Cloud-Sicherheits-plattform, die auch Tokenisierung als Ergänzung der Verschlüsselungs-funktion anbietet.

Unterstützung für globale Compliance-Anforderungen

Dank der Lookout CASB-Architektur können die größten multinationalen Unternehmen komplexe Compliance-Vorschriften wie die Europäische Datenschutz-Grundverordnung (DSGVO), HIPAA, PCI, GLBA, SOX und viele weitere Vorschriften auf der ganzen Welt einhalten. Unsere Option für die Hybrid-Bereitstellung bietet jedem Unternehmen eine integrierte, sichere Bereitstellung für die wichtigsten Cloud-Anwendungen in mehreren Ländern – mit Kontrollen und Schlüsselmanagementfunktionen, die sich entsprechend unterschiedlichster Richtlinienanforderungen konfigurieren lassen. Jedes Land hat möglicherweise unterschiedliche Compliance-Kontrollen für Datenschutz, Datensicherheit, Datenhoheit und Datenaufbewahrung. Die CASB-Plattform kann zudem jede beliebige Kombination aus von Kunden kontrollierten Schlüsseln für mehrere Anwendungen unterstützen – auch in Konfigurationen mit mehreren lokalen Schlüsselmanagementsystemen.

In zahlreichen Ländern gelten Datenschutzgesetze, gemäß denen die Verarbeitung personenbezogener Daten für Bürger innerhalb der Landesgrenzen oder in Regionen mit ausreichendem Datenschutz vorgegeben ist (z.B. EU-DSGVO). Viele Unternehmen müssen diese Anforderung hinsichtlich des Datenaufbewahrungsorts erfüllen. Weitere Informationen zu länderspezifischen Datenschutzgesetzen finden Sie im Lookout Global Compliance Resource Center.

Die meisten Cloud-Anbieter können den Datenaufbewahrungsort nicht gewährleisten, da Daten zwischen mehreren Regionen verschoben, in anderen Ländern per „Command-and-Control" aufgerufen oder von regionsübergreifenden Remote-Supportdiensten genutzt werden. Viele globale Organisationen konnten Cloud-Anwendungen nur mit zusätzlichen Sicherheitskontrollen wie Lookout CASB implementieren.

Lookout-Konnektoren schützen Daten in allen SaaS-Anwendungen

CASB stellt auch Anwendungskonnektoren für zahlreiche gängige SaaS-basierte Geschäftsanwendungen bereit, darunter SAP SuccessFactors, ServiceNow, Office365®, Adobe®, Box®, Dropbox®, SAP S/4HANA, SAP Hybrid Cloud und viele weitere. Diese Konnektoren schützen Anwendungsinhalte und erhalten dabei Anwendungsfunktionen aufrecht. Gleichzeitig erhalten Sie damit mehr Compliance-Funktionen als mit dem Angebot des SaaS-Anwendungsanbieters. Anwendungen eines PaaS-Ökosystems im Marketplace eines Anbieters werden ebenfalls von der CASB-Plattform geschützt. So erhalten Kunden größere Kontrolle über und Einblicke in die Daten, die mit diesen PaaS-Drittanbietern geteilt werden. Dank dieser Funktionen können Sie Ihre Daten mit einem konsistenten Ansatz und einer einheitlichen Frontend-Schnittstelle schützen und für Compliance in allen Ihren Cloud-Umgebungen sorgen. Unsere Konnektoren können die Sicherheit bis zum Unternehmensrand erweitern, damit alle Daten in Ihren Clouds stets geschützt sind – entweder durch Verschlüsselung oder Tokenisierung.

Lookout AnyApp für alle Ihre speziell entwickelten Anwendungen

Mit dem Lookout CASB-Konnektor „AnyApp" können Kunden diese leistungsstarken Datenschutzfunktionen für ihre eigenen cloudbasierten Anwendungen integrieren. So stellen Unternehmen sicher, dass Kundenanwendungen Daten auf jeder Cloud-Plattform schützen können. Mit AnyApp können Kunden Verschlüsselung, Tokenisierung, dynamische Zugriffskontrolle, DRM, UEBA, Bedrohungsschutz und viele weitere nützliche Sicherheitsfunktionen in ihre speziell entwickelten cloudbasierten Anwendungen einbinden.

Flexible Modelle für schnelle Bereitstellung

Mit unserer gehosteten Bereitstellung ist diese innerhalb weniger Stunden erledigt. Dank vereinfachter und schneller Administration können Sie unseren leistungsstarken CASB-Schutz für Ihre ServiceNow-Instanz innerhalb von Stunden einrichten – damit alle Daten über die Verschlüsselung hinaus geschützt sind. Wir unterstützen auch lokale Bereitstellungen in unseren Rechenzentren, vollständig in der Cloud gehostete Bereitstellungen sowie Hybridoptionen (lokal und gehostet) entsprechend Ihrer Compliance- und Betriebsstrategie. Unsere cloudnative CASB-Plattform vereinfacht die Bereitstellung erheblich und ergänzt die CASB-Standardfunktionen durch End-to-End-Datenschutz mit führenden SaaS-, PaaS- und IaaS-Geschäftsanwendungen.

Die Architektur der Lookout-Plattform unterstützt flexible und schnelle Bereitstellungen. Über die API-Integration unseres Cloud Security Broker (CSB) können Sie CASB-Funktionen in Anwendungen von SaaS-Anbietern einbetten und dort nutzen. Der CSB verwendet die APIs, die von den Cloud-Anbietern veröffentlicht und unterstützt werden. Das CSB-Integrationsmodell ermöglicht eine genaue Prüfung aller Benutzer, Inhalte und Zusammenarbeitsaspekte ausgewählter Clouds, um Überwachung, Kontrolle und Schutz (Verschlüsselung) zu verbessern.

Cloud Security Gateway (CSG) ist ein Inline-Proxy, der die strengsten Sicherheitsrichtlinien durchsetzt und Daten schützt. Unser Inline-Support für Anwendungen bietet umfassenden und komplett transparenten Datenschutz auf Feldebene für SaaS-Programme von Anbietern wie ServiceNow, SAP SuccessFactors, ServiceNow und viele weitere sowie für Ihre speziell entwickelten Anwendungen.

Nutzung der vorhandenen Infrastruktur

Die Lookout-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).

- Externe DLP (EDLP) integriert bestehende DLP-Unternehmenslösungen in die Lookout-Plattform. 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 Single Sign-On (SSO) können Sie Zugriffsrichtlinien für Anmeldeaktionen erstellen und anwenden. Dadurch lassen sich Anmeldeaktivitäten bei ServiceNow genauer kontrollieren. Die Lookout-Plattform unterstützt diese Funktion über eine IdP-Proxy-Entität. Aktivieren Sie dieses Feature, indem Sie den CSB-IdP-Proxy als Teil des SSO-Ablaufs in Ihrem Unternehmen einrichten.
- Antivirus/Antimalware (AVAM) liefert zusätzliche Details zur Erkennung vieler Malware-Typen, darunter Zero-Day-Bedrohungen, Viren, Spyware, Ransomware, Würmer und Bots. Dank dieser Integration werden alle zusätzlichen in ServiceNow hochgeladenen Dateien vor der Infizierung durch bösartige Inhalte geschützt, die interne ServiceNow-Benutzer betreffen können. Nach Bedarf können Sie mehrere externe Dienste konfigurieren und Richtlinien individuell auf diese anwenden.

Integration in vorhandene Unternehmens-sicherheitslösungen, um getätigte Investitionen auszuschöpfen.

Vorteile von Lookout CASB

- **Schnellere Cloud-Einführung:** Erweitern Sie die Cloud-Nutzung über ServiceNow hinaus, indem Sie Hindernisse in Bezug auf Cloud-Sicherheit, Datenschutz und Compliance überwinden.
- **Größere Cloud-Transparenz:** Erkennen Sie Nutzung, Datenbewegung und Benutzeraktivitäten in ServiceNow, um Datenverlust und Compliance-Risiken zu minimieren.
- **Niedrigere Betriebskosten:** Nutzen Sie eine zentral gesteuerte, einfach bereitzustellende gehostete oder hybride Plattform für alle Cloud-Anforderungen des Unternehmens – für End-to-End-Datenschutz und minimierten Aufwand bei Compliance-Audits.
- **Minimale Sicherheitsverletzungsrisiken dank leistungsstarkem Datenschutz:** End-to-End-Datenschutz und andere wichtige Funktionen sorgen dafür, dass Daten stets in ServiceNow und anderen Cloud-Anwendungen oder -Plattformen geschützt sind. Dadurch minimieren Sie das Risiko von Datenlecks, finanziellen Verlusten, Rufschädigung und rechtlichen Konsequenzen.
- **Kontrolle und Verhinderung erzwungener Datenoffenlegung an Dritte:** CASB verfügt über eine einzigartige und leistungsstarke Schlüsselmanagementfunktion, die stets in der Kontrolle des Kunden liegt.
- **Verbesserte Governance der Zusammenarbeit:** CASB liefert eine Komplettlösung für die Freigabe von Daten für Dritte, einschließlich voller Kontrolle über sensible Inhalte und vollständiger Überwachung und Protokollierung der Aktivitäten.
- **Verbesserung der DSGVO-Compliance – eine Lösung für globale Compliance-Anforderungen:** Die Lookout CASB-Architektur kann jede Kombination aus globalen Compliance-Anforderungen und lokalen Datenschutzgesetzen erfüllen – damit Sie cloudbasierte Anwendungen ganz einfach einsetzen können.

Unterscheidungsmerkmale von Lookout CASB

- **Transparente Workflow-Nutzung:** Lookout CASB erweitert den Datenschutz transparent und nahtlos auf die Benutzererfahrung, ohne Beeinträchtigung von Anwendungs-Workflows.
- **AnyApp-Konnektor:** Kunden können leistungsstarken CASB-Schutz für sensible Daten in ihre eigenen speziell entwickelten Cloud-Anwendungen integrieren.
- **Anwendungsspezifischer Datenschutz:** Lookout CASB bietet höchsten Datenschutz in gängigen SaaS-Anwendungen.
- **Hybrid-Architektur:** Eine zentrale Lookout-Plattform kann mehrere Anwendungs-Clouds und jede beliebige Kombination aus cloudbasierter und lokaler Schlüsselverwaltung unterstützen.
- **Unternehmensintegration:** Vollständige Integrationen in EDLP, EDRM, SIEM, IAM, SSO, EMM, NGFW und viele weitere Systeme sind verfügbar.
- **Verschlüsselung – End-to-End-Datenschutz:** Mit Verschlüsselung im Ruhezustand, bei der Übertragung und bei der Verwendung können Sie die höchsten Sicherheitsanforderungen erfüllen und gleichzeitig Benutzertransparenz für typische Anwendungsfunktionen wie Suchen, Erstellen von Berichten, Sortieren, Diagrammerstellung und mehr bereitstellen.
- **Zero-Trust-Schlüsselmanagement:** Dank vollständiger Unterstützung für HMS und mehrere lokale Schlüssel können Sie die verschiedensten Compliance-Anforderungen erfüllen.
- **Natives Gerätemanagement**: Schränken Sie authentifizierte Benutzer nach dem Gerätetyp ein, damit sie nur von festgelegten vertrauenswürdigen Plattformen auf Daten zugreifen können.
- **Sicherer Offline-Datenzugriff:** Integrierte DRM- oder EDRM-Integration ermöglicht sicheren Online- und Offline-Zugriff auf Dokumente, den Sie unmittelbar entziehen können.

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 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.