Lookout®

WHITEPAPER

Schutz von persönlichen Daten und Privatsphäre in SAP SuccessFactors

Neue sicherheitsspezifische Herausforderungen durch dynamische SaaS- und Cloud-Umgebungen

Lookout CASB unterstützt alle SAP SuccessFactors-Module

- Employee Central
- Performance and Goals
- Succession and Development
- Learning
- Reports
- Compensation
- Analytics
- Open Data Protocol (OData) APIs
- Workflows
- Email

Datenschutz und Maximieren von Human Capital Management

SAP SuccessFactors hat den Markt für Human Capital Management (HCM) revolutioniert und bietet Tausenden Unternehmen weltweit alles von grundlegendem Human Resources Management bis hin zu erweiterten Mitarbeiteranalysen.

Als eine Vielzahl von Unternehmen in die Cloud migrierte, um die Vorteile des Software as a Service (SaaS)-Bereitstellungsmodells zu nutzen, wurde die Lösung noch beliebter. Dadurch kamen jedoch Sicherheitsbedenken bezüglich des Schutzes der Vertraulichkeit von Mitarbeiterinformationen und der Compliance mit Datenschutzrichtlinien auf.

Die sicherheitsspezifischen Herausforderungen sind gewaltig: Apps werden heute vollkommen ortsunabhängig eingesetzt. Mitarbeiter arbeiten remote mithilfe von Geräten und Netzwerken, die Sie nicht kontrollieren. Es gibt keine festen Perimeter in der Cloud. Daten müssen überall verfügbar sein.

Durch die Einführung internationaler Gesetze zu Datenaufbewahrung und -schutz wurden die Herausforderungen noch größer. Laut der Anwaltskanzlei Morrison and Foerster haben 133 Rechtsordnungen weltweit Datenschutzgesetze erlassen (Stand Januar 2021).

Daher müssen Unternehmen, die in SuccessFactors investieren, alle Daten schützen – von mobilen Endgeräten bis hin zu in der Cloud gehostete SaaS. Zudem müssen sie Unternehmensrisiken durch den Schutz personenbezogener Daten, geschützter Gesundheitsdaten und anderer vertraulicher Informationen in Übereinstimmung mit Datenschutzrichtlinien reduzieren.

Lookout® CASB – ein Grundstein unserer integrierten Plattform für Sicherheit vom Endgerät bis in die Cloud – ermöglicht genau das. Wir bieten Ihnen umfassende Transparenz hinsichtlich Ihrer gesamten Sicherheitsinfrastruktur sowie dynamische Zugriffskontrollen, Datenschutz, Erkennung von Cyberbedrohungen und Compliance-Management.

Mit Lookout CASB können Sie sich darauf verlassen, dass die Privatsphäre von Mitarbeiterdaten an allen Fronten geschützt ist – von Personalwesen, Abrechnung, Recruiting, Mitarbeiterplanung bis hin zu anderen strategischen HCM-Unternehmensprozessen.

SuccessFactors-Checkliste für Datensicherheit

- ✓ Erweitern der Transparenz auf die SAP SuccessFactors-Cloud-Nutzung
- ✓ Bereitstellen von Zero-Trust-Zugriff über sämtliche Geräte und Standorte
- ✓ Durchsetzen erweiterter Datenschutzrichtlinien zur Erkennung, Klassifizierung und zum Schutz sensibler Daten
- ✓ Anwenden von Zero-Trust-Verschlüsselung mit 100 % Eigentumsrecht an Verschlüsselungsschlüsseln
- ✓ Schützen von heruntergeladenen Daten mit Enterprise Digital Rights Management
- ✓ Überwachen von Benutzeraktivitäten zur Identifizierung von abweichendem Verhalten und Bedrohungen
- ✓ Unterstützen komplexer, globaler Compliance-Anforderungen zur Gewährleistung von Datenschutz

Bereitstellen von Zero-Trust-Access über sämtliche Geräte und Standorte

> In 79 % der Unternehmen kam es in den letzten zwei Jahren zu einer identitätsbezogenen Datensicherheitsverletzung und 99 % glauben, dass diese vermeidbar gewesen wäre.
>
> Identity Defined Security Alliance, Mai 2020

Vor der Einbindung von Personalprozessen in SuccessFactors müssen Benutzeridentitäten überprüft werden. Erst dann wird Zugriff gewährt. Die weitverbreitete Verwendung privater Geräte für die Arbeit macht deutlich, wie wichtig identitäts- und kontextbasierter Zugriff auf Apps ist.

Mit Lookout CASB können Sie granulare kontextbasierte Richtlinien für Zero-Trust-Zugriff auf Daten definieren, die in SuccessFactors gehostet werden. Richtlinien werden durch eine Kombination aus kontextuellen Faktoren und Step-up-Authentifizierung durchgesetzt, bei der Mitarbeiter aufgefordert werden, zur Gewährleistung von Richtlinien-Compliance zusätzliche Anmeldedaten anzugeben.

Zu den von Lookout CASB verwendeten kontextuellen Faktoren gehören Benutzeridentität, Benutzergruppe, Standort, IP-Adresse, Geräte, Betriebssysteme, Baselines für Benutzerverhalten, Geräte-Compliance und Risiken für geistiges Eigentum.

Zusätzliche Funktionen

- **Integration in Mobile Device Management (MDM) und Enterprise Mobility Management (EMM):** Lookout CASB setzt Gerätezugriffsbeschränkungen nach Erkennung und Klassifizierung von Endgeräten als verwaltetet oder nicht verwaltet durch. Dadurch können Benutzer keine Gehaltsabrechnungen und andere vertrauliche Daten auf nicht verwaltete Geräte herunterladen.
- **Integration in Identitätsanbieter:** Im Reverse-Proxy-Modus lässt sich Lookout CASB in Microsoft Azure AD, Okta, Ping und Thales integrieren, um Zero-Trust von Geräten und Standorten auf autorisierte Cloud-Apps durchzusetzen. Dank Identitätsprüfung in Verbindung mit Single Sign-On und Mehrfaktorauthentifizierung (Multifactor Authentication, MFA) profitieren Sie von granularen Zugriffskontrollen für Anmeldeaktivitäten bei SaaS-Apps.
- **Vermeidung von nicht autorisiertem Zugriff:** Lookout CASB erkennt und sperrt verdächtige Anmeldezeiten und -standorte. Die Lösung erkennt beispielsweise, wenn ein Benutzer sich nur zwei Stunden nach der Authentifizierung aus Nordamerika von einem Standort auf der anderen Seite des Atlantiks anmeldet.

Schützen von Daten durch Erkennung und Klassifizierung

Zur Steigerung der Produktivität von HCM-Prozessen müssen Sie zunächst die personenbezogenen Daten und andere vertrauliche Informationen schützen, die in SuccessFactors hochgeladen und für angeschlossene Drittanbieter-Apps freigegeben werden. Dadurch gewährleisten Sie sichere Verbindungen für Mitarbeiter, Geschäftspartner und Auftragnehmer, die verwaltete und nicht verwaltete Geräte von verschiedensten Standorten aus verwenden.

Mit Cloud-basierter Data Loss Prevention (DLP) aus Lookout CASB profitieren Sie von den leistungsstärksten Datenschutzfunktionen und Zugriffskontrollen, die für SuccessFactors verfügbar sind. Wir gewährleisten kontinuierlich die Integrität und Zuverlässigkeit von Daten bei der Verarbeitung und Speicherung über alle SAP-Module für SuccessFactors hinweg.

Lookout-Datenschutz für SuccessFactors

Zentrale DLP-Richtlinien-Engine: Die erweiterte DLP-Lösung von Lookout CASB weitet Datenschutz und Zugriffskontrollen auf SuccessFactors in der Cloud aus. Sie können granulare Richtlinien erstellen, mit denen sich sensible Daten in Echtzeit auf zugewiesene Klassifikation, Regeldurchsetzung, Verschlüsselung, Maskierung, Wasserzeichen, Quarantäne oder Löschung überprüfen lassen.

Optionen für die Richtlinienerstellung: Es stehen unter anderem folgende Optionen zur Verfügung: Zulassen oder Unterbinden von Uploads, Protokollierung, Benachrichtigung, Ablehnung, Schutz von Massendatenimports, Step-Up-Authentifizierung, Anwenden von Datenklassifizierungsbezeichnungen, Datenverschlüsselung

zum Schutz von Daten während Downloads, Benutzer-Compliance-Coaching, Dokumentenhervorhebung, Redigierung, Wasserzeichenerstellung, dauerhafte Löschung und Behebung durch Benutzer.

Datenschutz auf Feld- und Dateiebene: Lookout CASB schützt SuccessFactors-Daten auf Feldebene (strukturiert) und unbekannte Dateien oder Notizen (unstrukturiert). Zu den geschützten Feldern gehören persönliche Mitarbeiterdatensätze sowie Namen, Adressen, Telefonnummern, E-Mail-Adressen und Sozialversicherungsnummern. Es können auch benutzerdefinierte Felder zur Verschlüsselung von branchenspezifischen Daten, wie beispielsweise Militär-IDs, geschützt werden.

Datenklassifizierung: Lookout CASB klassifiziert Daten und bietet Transparenz und Schutz für alle SuccessFactors-Module sowie Apps, Benutzer und Geräte. Dadurch verhindern Sie, dass Mitarbeiterdatensätze und sensible Daten versehentlich offengelegt werden. Wir unterstützen außerdem die Integration in Microsoft Information Protection (MIP) und Titus, sodass sich Datenklassifizierung und -Governance auf sämtliche Dokumente in jeder Cloud ausweiten lassen.

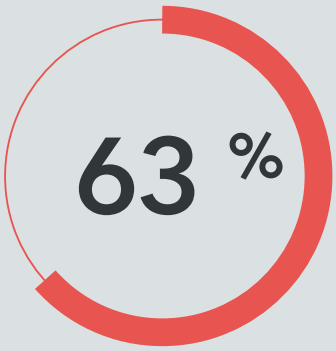
Anwenden von Zero-Trust-Verschlüsselung mit exklusiver Schlüsselkontrolle

In über 64 % der Finanzdienstleistungsunternehmen hat jeder Mitarbeiter 1.000 vertrauliche Dateien geöffnet.

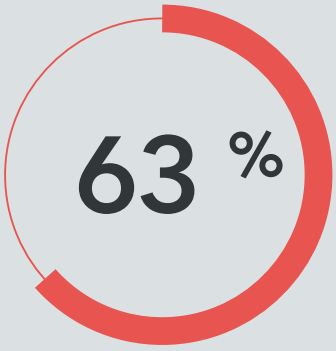
Varonis, 2021 Financial Services Data Risk Report

Einige SaaS-Anbieter schützen Daten bei der Speicherung, aber die meisten lassen Daten, die gerade verwendet oder verarbeitet werden, außen vor. Dadurch können sensible und vertrauliche Klartextinformationen in SaaS-Apps zu schwerwiegenden Datensicherheitsverletzungen führen.

Die größten Sicherheitsbedenken



Datenverlust/-lecks



Datenschutz/-vertraulichkeit

AWS Cloud Security Report 2020 for Management: Managing the Rapid Shift to Cloud

Zusätzlich halten viele Schlüsselverwaltungsrichtlinien und -prozesse in Cloud-Apps unter Umständen nicht die GDPR-, HIPAA- und CCPA-Datenschutzgesetze ein, da SaaS-Anbieter – und nicht ihre Kunden – Verschlüsselungsschlüssel verwalten.

Zero-Trust-Verschlüsselung für SuccessFactors von Lookout CASB bietet den überzeugendsten Ansatz für Datenschutz. Die Lösung stellt Funktionen für strengere Kontrolle über SuccessFactors HCM-Module innerhalb von Apps bereit und

wir verwenden 256-Bit-AES-Verschlüsselung zum Schutz von personenbezogenen Daten in SuccessFactors. Zudem können Sie sich darauf verlassen, dass nicht verschlüsselte Daten nicht Ihr Netzwerk verlassen. Sie haben die alleinige Kontrolle über gültige Verschlüsselungsschlüssel, sodass nicht autorisierte Benutzer, Systemadministratoren von Cloud-Anbietern und Außenstehende nicht ohne Berechtigung auf Daten zugreifen können.

Einzigartige Vorteile von Lookout CASB-Verschlüsselung

Alleinige Verwaltung von Schlüsseln: Mit dem Lookout CASB-Schlüsselmanagement sind Sie der alleinige Eigentümer von Schlüsseln zur Datenverschlüsselung. SuccessFactors ist nicht Eigentümer von Schlüsseln, verschlüsselt keine Daten und gibt sie auch nicht an Drittanbieter-Apps weiter, wodurch sich die nicht autorisierte Offenlegung von Daten vermeiden lässt.

Formatbeibehaltung: Bei der starken Verschlüsselung mit Lookout CASB werden Richtlinienformate auf Feldebene in SuccessFactors beibehalten. Wir bieten außerdem Teilfeldverschlüsselung beim Durchsuchen und Sortieren von Daten sowie bei Bericht- und Diagrammerstellung. Dadurch profitieren Sie von erstklassigem Datenschutz ohne die Behinderung von geschäftskritischen HCM-Prozessen.

Schützen von heruntergeladenen Daten mit Enterprise Digital Rights Management

> „Die Risiken, die entstehen, wenn wir Mitarbeiter Zugriff auf Unternehmensressourcen von privaten Geräten gewähren, sind nicht zu leugnen."
>
> Forbes

Die steigende Anzahl von Mitarbeitern, die private Mobilgeräte für die Arbeit verwenden, führt zu neuen Herausforderungen beim Schutz vertraulicher Daten außerhalb der Cloud-Umgebung. Dadurch wird auch sicherer Zugriff auf Offline-Daten immer wichtiger.

Enterprise Digital Rights Management (EDRM) in Lookout CASB wendet strenge Datenschutzkontrollen auf vertrauliche Daten in SuccessFactors an. Wir verschlüsseln automatisch persönliche Informationen über Mitarbeiter, Gehaltsabrechnungen und zugehörige Workflows während Downloads auf Benutzergeräte und sorgen so für vollständigen Datenschutz.

Sie können EDRM-Richtlinien definieren, um Dateizugriff und -Downloads nur auf verwalteten Geräten zu gestatten, und den Zugriff auf autorisierte Benutzer beschränken, die heruntergeladene Dateien mit dem Lightweight-EDRM-Client von Lookout CASB entschlüsseln dürfen.

Zusätzliche EDRM-Schutzmechanismen

Vollständige Transparenz und alleiniges Eigentumsrecht an Daten: Lookout CASB bietet Ihnen vollständige Transparenz im Hinblick auf Datenzugriff und -Download durch interne und externe Benutzer, einschließlich Kunden, Anbieter und Partner. Wir sorgen dafür, dass Sie die Kontrolle über heruntergeladene Dateien behalten – ganz gleich, wo sie freigegeben werden.

Management von Verschlüsselungsschlüsseln: Mit Lookout CASB können Sie Verschlüsselungsschlüssel zurückziehen und Benutzerzugriff in Echtzeit stoppen, um so vertrauliche Daten auf verlorenen oder gestohlenen Geräten zu schützen. Dadurch vermeiden Sie auch die missbräuchliche Verwendung von Daten, zum Beispiel Mitarbeiter, die Kundendaten mit in neue Unternehmen nehmen.

Identifizieren von abweichendem Benutzerverhalten und Cyberbedrohungen

Jede SaaS-Plattform – auch SuccessFactors – kann Malware zum Opfer fallen. Diese führt dann zu einem Cyberangriff, der sich lateral auf Ihre Cloud-Infrastruktur ausbreitet, auf andere Clouds übergreift und herkömmliche Virensysteme umgeht.

Cyberkriminelle verwenden in der Regel Command-and-Control-Taktiken, um Geräte und Apps zu kompromittieren und an persönliche und administrative Anmeldeinformationen zu gelangen. Die Angreifer erlangen immer mehr Zugriff, bis sie vertrauliche Daten und wertvolles geistiges Eigentum finden, was dann zu einer katastrophalen Datensicherheitsverletzung führt.

Lookout CASB aggregiert und korreliert zugehörige Daten aus Unternehmensnetzwerken, Clouds, SaaS- und mobilen Umgebungen und bietet auf diese Weise Schutz gegen diese Art der Cybersicherheitsbedrohung. Sie erhalten einen umfassenden Überblick über die frühesten Anzeichen von Bedrohungsverhalten, sodass Sie Angriffe schnell vermeiden und Datensicherheitsverletzungen unterbinden können.

> „Die durchschnittlichen Kosten für die Behebung eines Cyberangriffs liegen bei Unternehmen mit einem Umsatz von mehr als 1 Milliarde USD bei 4,6 Millionen USD."
>
> **TechBeacon**

Erkennen von verdächtigem Verhalten und Cyberbedrohungen

Zero-Day-Bedrohungsschutz: Die integrierte Antivirus/Antimalware (AV/AM)-Funktion in Lookout CASB scannt alle ein- und ausgehenden Cloud-Inhalte, um Viren, Malware und Ransomware mit branchenführenden Erkennungsraten abzuwehren. Infizierte Inhalte werden automatisch ohne spürbare Latenz unter Quarantäne gestellt.

Dank URL-Link-Schutz und einer lokalen Sandbox-Integration können Sie zudem die fortschrittlichsten Cyberangriffe schnell erkennen und beheben.

Benutzer- und Entitätsverhaltensanalysen: User and Entity Behavior Analytics (UEBA) in Lookout CASB nutzt ausgefeilte Algorithmen für maschinelles Lernen, um Aktivitäten in SuccessFactors zu überwachen, einschließlich ungewöhnlicher Regionen oder Tageszeiten, versuchter Massendatei-Downloads und anderer abweichender Verhaltensweisen.

> „Bis 2023 werden die persönlichen Informationen von 65 % der Weltbevölkerung modernen Datenschutzrichtlinien unterliegen (heute sind es nur 10 %)."
>
> **Gartner-Bericht: The State of Privacy and Personal Data Protection, 2020-2022**

UEBA gibt Echtzeitalarme zu abweichendem Verhalten aus, das durch einen Cyberangreifer oder bösartigen Mitarbeiter hervorgerufen wurde. In diesem Fall blockiert Lookout CASB Aktionen basierend auf Abweichungen von normalen Verhaltensmustern.

Zu diesen Abweichungen gehören eine ungewöhnlich hohe Anzahl von Downloads durch einen einzelnen Benutzer, eine ungewöhnlich hohe Anzahl von Anmeldeversuchen vom selben Benutzer oder ständige Anmeldeversuche von einem nicht autorisierten Benutzer.

SIEM-Unterstützung: Mit Lookout CASB lassen sich lokal erfasste Benutzeraktivitätsprotokolle durch die Integration in Microfocus ArcSight, IBM QRadar, Intel Security, LogRhythm und Splunk SIEMs auch auf die Cloud ausweiten. Dadurch können Sie die Automatisierung des Vorfallmanagements mit der zentralen Analyse und Berichterstellung im Hinblick auf Sicherheitsereignisse vom Endgerät bis in die Cloud kombinieren.

Gewährleistung von Richtlinien-Compliance für sichere Privatsphäre und Datenaufbewahrung

Aufgrund von Datenschutzgesetzen wie der DSGVO dürfen Daten keine Länder passieren, deren Datenschutzstandards nicht denen des Ursprungslandes entsprechen. Auch die dortige Speicherung ist untersagt.

Dadurch entstehen komplexe globale Herausforderungen für Unternehmen, die SuccessFactors und andere SaaS-App-Plattformen nutzen. Bei Cloud-Diensten kommen häufig mehrere geographisch verteilte Rechenzentren zur Gewährleistung von Hochverfügbarkeit und minimaler Latenz zum Einsatz.

Lookout CASB verwendet Cloud-Verschlüsselungs-Gateways, um für sichere, zentrale Compliance und Governance zu sorgen. Dies umfasst absolute Kontrolle über den Datenaufbewahrungsort, Schutz vor durch die Regierung erzwungener Offenlegung und Schutz vor Meldepflicht.

Zentrale Compliance und Governance

Absolute Kontrolle über den Datenaufbewahrungsort: Das Lookout CASB-Verschlüsselungs- und -Schlüsselmanagement gestattet eine globale Instanz einer SaaS-App und sorgt für die punktuelle Verschlüsselung und Tokenisierung von Daten für jedes Land zur Erfüllung von lokalen Datenaufbewahrungsanforderungen. Diese Funktion für absolute Kontrolle über den Datenaufbewahrungsort gewährleistet, dass personenbezogene und vertrauliche Daten aus SuccessFactors nicht außerhalb des entsprechenden Souveränitätsbereichs offengelegt werden.

Schutz vor durch die Regierung erzwungener Offenlegung: Lookout CASB bietet einzigartige und leistungsstarke Schlüsselverwaltungsfunktionen, die immer unter Ihrer Kontrolle und in Ihrem Zuständigkeitsbereich bleiben. Dadurch können Sie Zugriff durch die von der Regierung erzwungene Offenlegung vermeiden und behalten stets umfassende Kontrolle über Ihre Daten.

Schutz vor Meldepflicht: Wenn Daten verschlüsselt sind und die entsprechenden Datenverschlüsselungsschlüssel sich nur in Ihrem Besitz befinden, kommt es in der Regeln nicht zu Datensicherheitsverletzungen. Bei den meisten Compliance-Richtlinien sind Sie nicht dazu verpflichtet, Ihre Kunden oder Mitarbeiter zu benachrichtigen, wenn ein Cyberangreifer oder bösartiger Insider Zugang zu verschlüsselten Inhalten erhält. Dadurch sind Sie vor Reputationsschäden und den Kosten einer öffentlich bekannten Datensicherheitsverletzung geschützt.

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, D.C.

Weitere Informationen finden Sie unter www.lookout.com/de. Folgen Sie Lookout auf seinem **Blog**, **LinkedIn** und **Twitter**.