



WHITEPAPER

# Enabling Safe Adoption of SAP Cloud and SuccessFactors for GDPR

Addressing personal data and data privacy challenges  
while accelerating cloud transformation



SAP SuccessFactors 

## Lookout CASB support SAP SuccessFactors modules including:

- Employee Central
- Performance and Goals
- Succession and Development
- Learning
- Reports
- Compensation
- Succession and Development
- Analytics
- OData
- Workflows
- Email

## Optimizing data privacy and protection while maximizing human capital management

SAP SuccessFactors has revolutionized the Human Capital Management (HCM) market, providing everything from core human resources management to advanced workforce analytics for thousands of enterprises across the globe. Further expedited by the increased adoption of cloud applications during 2020, SuccessFactors has become even more widely engaged by organizations seeking to embrace Digital Transformation.

At the same time, this rapid adoption of SuccessFactors has also heightened related security considerations as organizations strive to effectively protect employees' personal data while complying with global data privacy regulations. The challenges facing today's practitioners as they tackle broadening utilization of cloud applications and growth of the remote workforce, along with deepening internal and external security requirements, are increasingly severe.

To that end, the General Data Protection Regulation (GDPR) – the European Union's overriding data protection and privacy mandate – has set a practical baseline around the globe for the observance of more stringent security and privacy requirements. Other regions have followed suit with similarly assertive data protection regulations such as the California Consumer Privacy Act (CCPA) and the Personal Data Protection Commission (PDPC) regulation in Singapore.

As a result, organizations using SuccessFactors to handle their workers PII and PHI, along with other forms of highly sensitive internal business information require a range of data-centric cloud security capabilities designed specifically to navigate these complexities.

Lookout's advanced cloud security and data protection platform provides the in-depth visibility, access control, data protection, threat protection, and compliance management capabilities required by today's SAP SuccessFactors practitioners. Using Lookout CASB, organizations can remain confident that employee data is protected across all fronts – spanning HR, payroll, recruiting, workforce planning, and other strategic HCM business processes.

## SAP SuccessFactors data security checklist:

- ✓ Extend visibility into SAP SuccessFactors cloud usage
- ✓ Enable Zero Trust access from any device and location
- ✓ Enforce advanced data protection policies to detect, classify and secure sensitive data apply
- ✓ Zero Trust encryption with 100% ownership of encryption keys
- ✓ Secure downloaded data with enterprise digital rights management
- ✓ Monitor user activity to identify anomalous behavior and threats
- ✓ Support complex global compliance requirements to ensure data privacy





# 87% of cloud professionals feel that a lack of cloud visibility is obscuring security threats to

– ‘The State of Cloud Monitoring’  
Report, Keysight

## Extend visibility into SAP SuccessFactors cloud usage

Maintaining centralized, end-to-end visibility into SuccessFactors applications activity is critical in meeting today's cloud security and compliance requirements. IT and security operations center teams must identify all connected users and devices uploading or accessing critical information in the SuccessFactors cloud while understanding any risks associated with each connected entity, enabling them to respond to potential threats.

Lookout CASB extends deep visibility into SAP SuccessFactors HCM modules, providing granular control over user activities and collaboration that involves sensitive HR-related data, including payroll and employee performance reports. This visibility offers detailed insight into user behavior and application usage, ensuring that data is protected from unauthorized access, whether malicious or accidental, and thereby reducing the potential for any damage caused by related data breaches or compliance violations.

### Key elements of Lookout CASB visualization and analysis include:

- **Detailed user activity monitoring:** Lookout CASB provides granular visibility into all user activity in SuccessFactors cloud to identify and report anomalous user activity with machine-learning powered User and Entity Behavior Analytics (UEBA). This analysis is further captured in CIO/CISO reports for forensic investigation, audits and risk analysis.
- **Insights investigate:** A context-rich set of tools for incident analysis and management, allowing security teams to analyze all activities in the cloud and drill down into incidents involving policy violations and numerous contributing factors through the highly intuitive and interactive “Incidents Insights” dashboard.

**Unauthorized access through misuse of employee credentials and improper access controls (42%) is the single biggest perceived vulnerability to cloud security.**

— 2019 Cloud Security Report,  
Cybersecurity Insiders

## Enable Zero Trust access from any device and location

As Human Resources processes and other business functions connect to SAP SuccessFactors across the globe, organizations require assurance that user identity is verified before granting access to confidential HCM data in SAP SuccessFactors. The expanding use of personal devices for accessing and downloading information further underscores the necessity for identity and context-aware application controls.

Lookout Adaptive Access Controls (AAC) define highly granular, context-aware policies to deliver “Zero Trust” access to data hosted in SAP SuccessFactors. This capability allows organizations to manage access to SAP SuccessFactors from any user, any device, and any location, with step-up authentication or user coaching upon detection of any detected policy violation. Lookout AAC addresses an extensive range of contextual information including location, user, user group, IP Address, device/OS type, user behavior, device compliance, and IP risk, among others.

### Additional features include:

- **Integration with MDM/EMM solutions:** Lookout CASB enforces device-level access restrictions upon retrieving and classifying the endpoint device type(managed/unmanaged). For example, blocking users from downloading salary reports on unmanaged devices.
- **Integration with identity providers:** Operating in reverse-proxy mode, Lookout CASB combines with IDaaS solutions, such as Microsoft Azure Active Directory, Okta, Ping and Thales, to deliver Zero Trust identity protection from any device, any location, to all trusted cloud applications. This allows for user identity authentication with Single Sign-On (SSO) and Multi-Factor Authentication (MFA), enabling fine grained access control for login activities over SaaS applications.
- **Preventing time travel:** Lookout Adaptive Access Controls detects and blocks suspicious login times and locations. For example, identifying an attempted log-in from overseas only two hours after the user authenticated from North America.

## Biggest cloud security concerns



**64%**

Data Loss/  
Leakage



**62%**

Data privacy/  
Confidentiality

2019 Cloud Security Report,  
Cybersecurity Insiders

## Enforce advanced data protection policies to detect, classify and secure sensitive data

With the growing usage of SAP SuccessFactors cloud to address the complex set of HCM requirements, organizations demand integrated data protection capabilities that can effectively defend confidential PII data uploaded to SuccessFactors, and shared across multiple connected third-party applications. Furthermore, these requirements must extend and adapt to support employees, business partners, and contractors using both managed and unmanaged devices, from any location.

Lookout's industry-leading cloud Data Loss Prevention (DLP) capabilities extend enterprise data security controls to SAP SuccessFactors and enable the use of centralized policies to monitor, classify and protect sensitive data residing in the application.

### To protect SAP SuccessFactors data, Lookout Data Protection offers:

- **Centralized DLP policy engine:** Lookout CASB delivers advanced Data Loss Prevention (DLP) capabilities that extends the enterprise data security controls to the cloud and defines centralized policies to monitor, classify and protect sensitive data across all modules of SAP SuccessFactors – while in motion or at rest. With Lookout, users can define highly granular and customizable policies to scan and protect sensitive information in real-time through data classification, rules enforcement, encryption, masking, watermarking, quarantining, or deletion.
- **Extensive policy creation options:** The extensive data protection controls for real-time data protection include upload allow/deny, logging, notification, denial, protecting bulk data imports, step-up authentication, application of data classification labels, encryption of files to protect data during downloads, user coaching, document highlighting, redaction, watermarking, permanent deletion, and/or user remediation.
- **Field and file-level data protection:** Lookout's unique data protection capabilities for Success Factors encompasses known field-level data (structured) and unknown files or notes (unstructured). SAP SuccessFactors fields protected by Lookout include personal employee records such as name, address, phone number, e-mail address and social security number, among others.
- **Data classification:** Lookout CASB classifies sensitive data for full visibility into and protection across the cloud applications, users, and devices – securing employee records and other protected information from unintended data exposure. Lookout integrates with Microsoft Information Protection (MIP) and TITUS to extend data classification and governance to any document in any cloud.



On average, **17%** of all sensitive files in an organization, containing credit card information, health records or personal information subject to regulations like GDPR, HIPAA and PCI, are accessible to all the employees.

– 2019 Data Risk Report, Varonis

## Apply Zero Trust encryption with exclusive key control

Although SaaS providers offer data protection at-rest (i.e., data in storage), they often fail to secure data in-use or data in-transit, creating the potential to leave clear-text data in SaaS applications vulnerable to potential breaches. Additionally, many cloud apps' key management policies and processes may not comply with data protection laws such as GDPR, HIPAA or CCPA – partly due to the control over encryption keys residing with SaaS providers, and not their customers.

Lookout Zero Trust encryption for SAP SuccessFactors offers the most compelling approach to data protection, helping organizations have tighter control over various HCM modules within applications. Lookout CASB uses AES 256-bit encryption to protect personally identifiable information (PII) elements in SAP SuccessFactors, ensuring the unencrypted data never leaves the customer's network. Involved encryption keys are retained exclusively by the customer, preventing unauthorized users, cloud provider system administrators, and outsiders from accessing that data without permission.

Lookout's data protection encompasses known field-level data (structured) and unknown files or notes (unstructured). SAP SuccessFactors fields protected by Lookout include personal employee records such as name, address, phone number, e-mail address, social security number, IP address, device/OS type, user behavior, device compliance, and IP risk, among others.

### Exclusive benefits offered by Lookout Zero Trust encryption include:

- **Hold your own keys:** Lookout key management allows customers to bring their own keys to encrypt the data. SAP SuccessFactors cloud solution does not retain control over the keys to decrypt the data or share it with any third-party application, hence preventing forced disclosure of data without the knowledge of the customer.
- **Format preservation:** Lookout's strong encryption includes field-level policies for preserving format in SAP SuccessFactors functions, partial field encryption and support for searching, sorting, reporting and charting on encrypted data. This offers best-in-class data protection to customers without sacrificing key business functionalities.

**There are undeniable risks in permitting employees' access to corporate resources from personal devices. Companies that are serious about implementing BYOD must account for the fact that users are the weakest link in the security chain.**

– Forbes

## Secure downloaded data with enterprise digital rights management

The growing use of personal devices challenges organizations to protect sensitive data as it travels outside the cloud environment, extending the need for secure of file data access.

Lookout Enterprise Digital Rights Management (E-DRM) enforces data protection controls on sensitive data in the SAP SuccessFactors cloud, enabling automatic encryption of sensitive employee data, salary reports and other related workflows during downloads on user devices to enable last-mile data protection. Customers can define E-DRM policies to permit file access and downloads on managed devices only, and restrict access to authorized users awarded permission to decrypt downloaded files using Lookout's lightweight E-DRM client.

### Lookout E-DRM benefits include:

- **Full visibility and data ownership:** Organizations have complete visibility into any data accessed and downloaded by internal and external users, including customers, vendors, and partners. Additionally, the organizations have complete control over downloaded files, regardless of where they are being shared.
- **Decryption key management:** Organizations can revoke the decryption keys and retract the user access in real-time to protect sensitive data on lost or stolen devices. This also protects data from misuse, for example blocking former employees from taking customer data to new companies.





**The average cost to recover from a cyberattack for organizations with more than \$1 billion in revenue is \$4.6 million.**

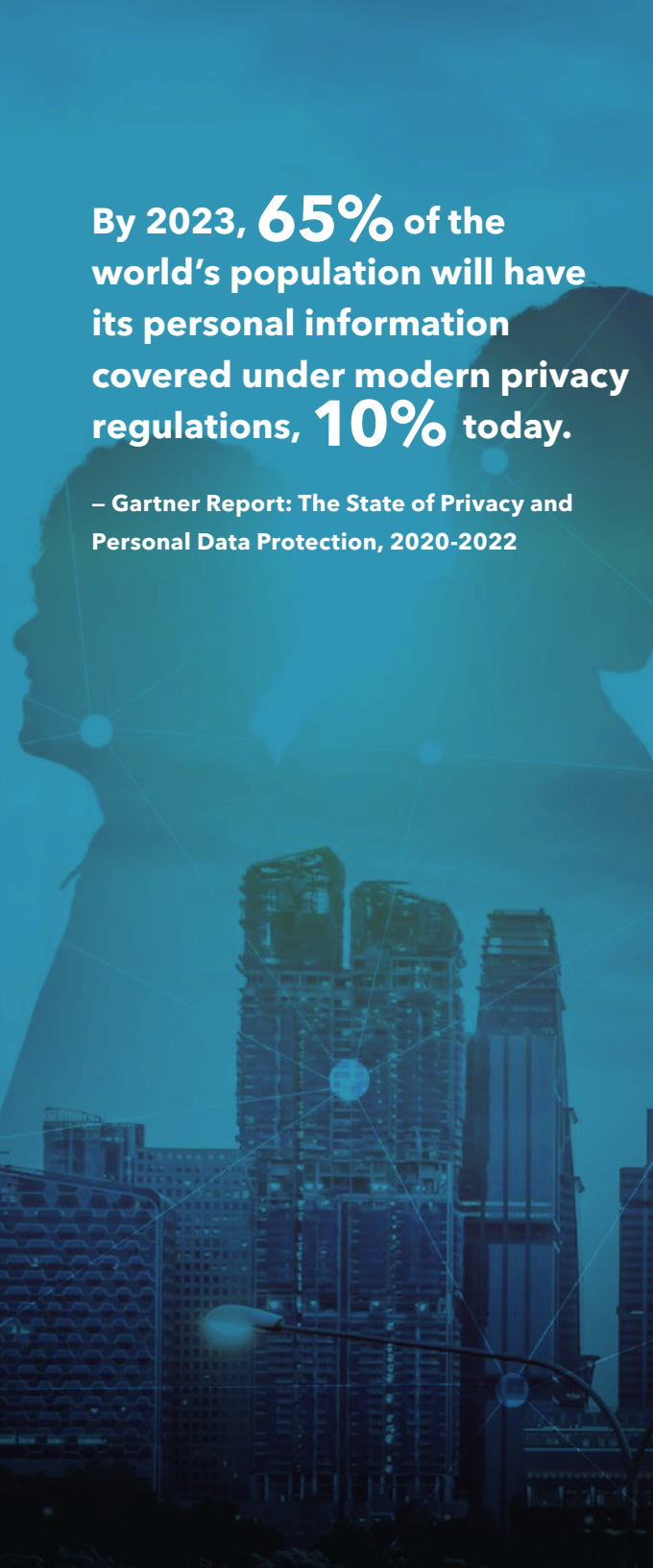
– TechBeacon

## Monitor user activity to identify anomalous behavior and threats

Increased adoption of SAP SuccessFactors creates additional exposure to malware as threats may be shared across clouds and bypass conventional anti-virus systems. Such threats inadvertently uploaded into the cloud can propagate rapidly across applications and user devices, perpetuating damage on a massive scale.

Lookout addresses this manner of cybersecurity threat by aggregating and correlating related data from across enterprise network, cloud, SaaS, and mobile environments, offering complete visibility into these risks as they occur including:

- **Zero-day threat protection:** Lookout's integrated anti-virus anti-malware (AVAM) solution scans all inbound and outbound cloud content to defend against viruses, malware, and ransom-ware with industry-leading detection rates, and quarantining infected content on the fly, without adding any noticeable latency. Additionally, URL link protection and on-premise sandbox integration allow detection and remediation for even the most challenging Zero-Day threats.
- **User and Entity Behavior Analytics (UEBA):** Lookout's UEBA capability uses machine learning to monitor user activity in SAP SuccessFactors cloud, including factors such as unusual region or time of day, attempted bulk file download and other anomalous behavior. UEBA provides real-time alerts on unusual activity, and can block actions based on variation from normal patterns. Examples of such anomalies might be an abnormally large number of downloads from an individual user, an unusually high volume of login attempts from the same user, or persistent login attempts by an unauthorized account.
- **SIEM support:** Integration with multiple SIEM solutions – including HP ArcSight, IBM QRadar, Intel Security, LogRhythm, and Splunk – extend user activity log collection from on-prem to the cloud, automating incident management with centralized analysis and reporting of organization's security events.



By 2023, **65%** of the world's population will have its personal information covered under modern privacy regulations, **10%** today.

– Gartner Report: The State of Privacy and Personal Data Protection, 2020-2022

## Support complex global compliance requirements to ensure data privacy and residency

Data protection laws such as GDPR require that organizations prevent personal data from being retained in or traveling through countries that do not have data protection standards that are equivalent to the resident country. This situation creates a complex challenge for organizations that rely on cloud-based applications, as the cloud service often includes data centers spread across multiple regions to ensure availability and prevent application latency.

Lookout CASB and the supporting security solutions, that includes Cloud Encryption Gateways

### Lookout's centralized compliance and governance support ensure:

- **Absolute data residency:** Lookout encryption and key management architecture allow one global instance of a SaaS application to selectively encrypt and/or tokenize the data for each required country and meet local residency requirements. This absolute capability for data residency control ensures that identifying personal or sensitive data is not revealed outside of the country or area of sovereignty.
- **Protection from government forced disclosure:** Lookout brings a unique and powerful key management capability that is always controlled under the customer's jurisdiction. This prevents access through forced government disclosures and gives 100 percent control over data access.
- **Safe harbor from breach notification:** Data most often cannot be breached if it is encrypted and related data encryption keys reside solely with the customer. Under compliance regulations such as GDPR, organizations are not required to notify their customers or employees if a cyberattacker or malicious insider gets hold of encrypted data, protecting reputation risk and reducing the cost associated with breach.

## The largest multinationals in the world use Lookout CASB

- From large to small enterprise
- Across every region and geography
- Significant concentration in North America and EU
- Representing nearly every vertical including:
  - Banking and Financial Services
  - Healthcare and Pharmaceutical
  - Manufacturing
  - Energy
  - Technology
  - Telecommunications
  - Education
  - Government







## About Lookout

Lookout is an integrated endpoint-to-cloud security company. Our mission is to secure and empower our digital future in a privacy-focused world where mobility and cloud are essential to all we do for work and play. We enable consumers and employees to protect their data, and to securely stay connected without violating their privacy and trust. Lookout is trusted by millions of consumers, the largest enterprises and government agencies, and partners such as AT&T, Verizon, Vodafone, Microsoft, Google, and Apple. Headquartered in San Francisco, Lookout has offices in Amsterdam, Boston, London, Sydney, Tokyo, Toronto and Washington, D.C. To learn more, visit [www.lookout.com](http://www.lookout.com) and follow Lookout on its [blog](#), [LinkedIn](#), and [Twitter](#).

For more information visit  
[lookout.com](http://lookout.com)

Explore our CASB integration for SAP SuccessFactors at  
[lookout.com/products/sap-success-factors](http://lookout.com/products/sap-success-factors)

[lookout.com](http://lookout.com)