



CipherCloud®

Lookout Total Protection for ServiceNow®



Notice

Lookout publications are made available solely for general information purposes. The information contained in this publication is provided on an “as is” basis. Any additional developments or research since the date of publication will not be reflected in this report.

Contents

Notice	2
Executive Summary	4
CASB Functionality for ServiceNow.....	5
CASB Capabilities for ServiceNow	7
Visibility.....	7
Data Security	7
Data Protection	7
Data Loss Prevention (DLP)	8
Digital Rights Management (DRM)	8
Threat Protection.....	9
User Entity and Behavior Analytics (UEBA)	9
Adaptive Access Control	9
Antivirus / Antimalware Protection.....	9
Support for Global Compliance Requirements	10
Lookout Connectors Protect Data in All Your SaaS Applications	11
Lookout AnyApp for all of your Custom Applications.....	11
Flexible Delivery Models Speed Deployment	12
Leverage Existing Infrastructure	13
Lookout CASB Benefits	14
Lookout CASB Differentiation.....	15
The Largest Multinationals in the World Use Lookout	16
About Lookout.....	16

“In October of 2017, Gartner Group evaluated the 11 leading CASB vendor solutions across a mix of features including architecture, data security, threat protection, UEBA, compliance/risk, and enterprise integration. The Lookout CASB platform received a perfect score of 100% in all areas evaluated. We are uniquely positioned to bring the strongest data security, powerful end-to-end encryption, and comprehensive threat protection for ServiceNow users. We can also extend this to any other mix of cloud applications within the enterprise.”

Pravin Kothari

Lookout EVP, Product and Strategy, SASE

Executive Summary

The goal of this document is to share an overview as to how the Lookout cloud access security broker (CASB) platform’s features and capabilities provide unparalleled security and compliance capabilities to ServiceNow® cloud customers. We will take a close look at the depth and breadth of security capabilities, and how they positively impact both data security and compliance for any customer utilizing ServiceNow solutions.

CipherCloud is intended for customers that must meet specific compliance and are concerned with data security, data privacy, and data residency requirements within their ServiceNow cloud. Given recent publicity highlighting cloud services that have been the center of a data breach, the emphasis on and importance of protecting sensitive data to limit cybersecurity risk and exposure has increased greatly.

CipherCloud enables a wide range of visibility, data protection, threat protection, and compliance capabilities, that, combined, offer the best solution to provide total protection for your ServiceNow clouds. The CipherCloud platform provides this value not only for the users of ServiceNow but also for other clouds which may be integrated with the same platform.

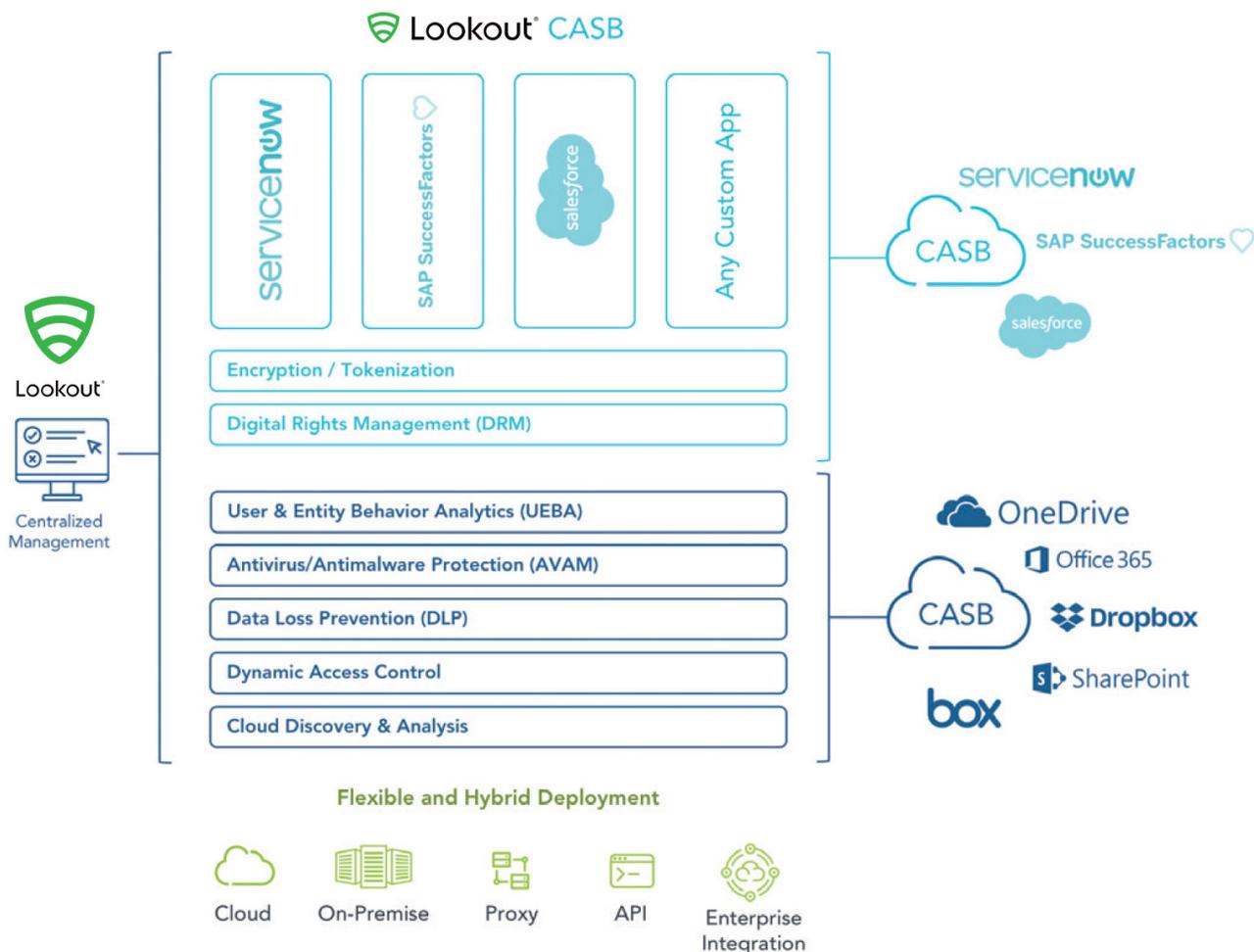
The features in CipherCloud are implemented through strong policy-driven controls which can support varying requirements for strong access control, sensitive content protection, threat prevention, and much more. Visibility controls are also important, as organizations must understand and tightly manage their exposure to the multiplicity of cloud services being used by their employees.



CASB Functionality for ServiceNow

The Lookout CASB platform provides deep visibility, end-to-end data protection, advanced threat protection, and comprehensive compliance capabilities to support ServiceNow cloud users. The cloud-native CASB platform ensure that confidential and sensitive data is protected at all locations - in the cloud and on users' devices - to protect from unauthorized access or data sharing.

The CASB capabilities also enable enterprises to safely use multi-cloud environments that go far beyond their ServiceNow application. The same CASB benefits can apply to any SaaS, PaaS, or IaaS so that you know your data will always be protected. The addition of the AnyApp capability allows customers to integrate custom developed cloud applications easily without any complex SDK or application modifications.



The Lookout CASB platform provides deep visibility, end-to-end data protection, advanced threat protection, and comprehensive compliance capabilities to support ServiceNow cloud users.





CASB Capabilities for ServiceNow

Visibility

Lookout extends visibility to your complete cloud infrastructure. Lookout CASB provides automated discovery of shadow IT and cloud resources being used across the entire enterprise. This enables IT, the security operations team, and compliance teams to gain complete knowledge of the true extent of the extended enterprise. The average enterprise has over 500 clouds of varying sizes, yet, in our estimate, the typical IT team has complete knowledge of only a percentage of them. Once discovered, these clouds should be evaluated on their potential risk to the organization and appropriate actions should be taken to reduce risk and exposure.

Lookout also provides visibility into user activities and collaboration that touches important and potentially sensitive corporate data. Basic controls provide strong support for collaborative governance and sharing between various internal and external groups. Lookout CASB further provides controls to limit the uploading of sensitive content to an external folder, automatically remove any links to folders containing sensitive data, and to precisely define the scope of sharing. Finally, this deep visibility is captured in activity logs to support compliance reporting, audit, and forensic investigation.

Data Security

Data Protection

Lookout provides best-in-class encryption in support of your ServiceNow cloud. Encryption enables the conversion of sensitive data into unreadable text so that in the event that the data is compromised, it is unusable and may not be

considered a breach. The industry best practice in order to meet a wide diversity of global compliance regulations is that data must be encrypted while in transit (through the network), in use (on the client device), and at rest (in the database). The decryption keys must be stored separately and never provided to your cloud vendor, or this may violate some of the global compliance requirements. Lookout's encryption and key management are solely held with you and provide the power and flexibility to address data security requirements in one scalable platform.

Lookout CASB is the only cloud security platform that also provides tokenization as an adjunct to the encryption capability. Tokenization refers to a technique that replaces the original data with a "token," which contains no information from the original content. Unlike encryption, there is no mathematical tie between the token and the original data. Tokenization, also referred to as data masking, is commonly used in countries or regions with strict data residency laws specifying that certain types of sensitive data cannot leave national boundaries. Tokenization is also often used for PCI compliance and meets Requirement 3 of the PCI Data Security Standard (PCI DSS).

Data Loss Prevention (DLP)

Lookout DLP identifies content in real time and provides support for ServiceNow custom and standard native objects. This powerful application awareness ensures that sensitive data is discovered in both structured and unstructured objects. When there are policy violations, Lookout DLP will enforce actions to include alerts, restricted sharing, or automatic encryption of sensitive files. Policies can also give the user time for self-remediation, which provides a time window to fix identified problems. Customers can integrate DLP policy with existing on-premise enterprise DLP systems. CipherCloud's Global Data Security Report identified that almost 20% of enterprise customers required tokenization. In specific regions like Europe and Asia Pacific, tokenization was the only essential data tool for protecting the organization against accidental compliance violations.

Digital Rights Management (DRM)

Our comprehensive data security also includes native DRM such as secure offline data access. Data that is downloaded from ServiceNow to a user's device can still be protected based on predefined policies, including defining what devices are allowed to access the data (for example, that users cannot use personal devices to access sensitive data). In the event that downloaded data needs to be protected from misuse - former employees taking customer data to new companies, for instance - administrators have the ability to retract access to the data, even if it was downloaded and copied to another device. Real-time key revocation can protect data on even lost and stolen devices. CipherCloud is also integrated with major third-party DRM packages such as Microsoft's.

Threat Protection

User Entity and Behavior Analytics (UEBA)

Lookoutfor ServiceNow includes advanced threat protection capability to keep your ServiceNow cloud secure and protected. Our UEBA capability uses machine learning to monitor user activity, including time of day of activity, attempts at bulk file download, and other anomalous behavior. UEBA can make real-time decisions to flag unusual activity or block it based upon variation from normal patterns.

Adaptive Access Control

Our adaptive access control can also block access, even to what appear to be authorized users, based upon platforms used, time of day, originating location, and more that might suggest the theft, compromise of authentication credentials, or a sophisticated cyberattack.

Antivirus / Antimalware Protection

Virus, malware, and ransomware protection is provided by our anti-virus anti-malware (AVAM) scanning. This powerful option option helps keep ServiceNow data safe. URL link protection and on-premise sandbox integration enable us to discover and remediate even the most challenging Zero-Day threats.

Lookout CASB is the only cloud security platform that also provides tokenization as an adjunct to the encryption capability.





Support for Global Compliance Requirements

The Lookout CASB architecture enables the largest multinational to deploy in alignment with complex compliance regulations such as the European Community General Data Protection Regulation (GDPR), HIPAA, PCI, GLBA, SOX, and many other regulations around the world. Our unique hybrid deployment option allows any enterprise to manage one integrated secure deployment for key cloud applications across multiple countries with controls and key management configurable to address a broad variety of differing regulatory requirements. Each country may have different compliance controls for data privacy, data protection, data sovereignty, and data residency. The CASB platform can also support any combination of customer-controlled keys, for multiple applications, in configurations that can include one or more on-premise key management systems.

Many countries have data protection laws that stipulate the processing of personal data for citizens must occur within the country or within regions for which there is an adequate level of data protection (e.g., EU GDPR). This requirement is sometimes referred to as “data residency” and many enterprises face such a policy constraint. For more information on country-specific data protection laws, see the Lookout Global Compliance Resource Center.

Most cloud providers cannot ensure data residency because data can be moved between multiple regions, accessed by “command and control” in other countries, or accessed by remote support services offered across regions. Many global organizations have not been able to adopt cloud applications without deploying additional security controls such as Lookout CASB.



Lookout Connectors Protect Data in All Your SaaS Applications

CASB also offers application connectors to support many popular SaaS-based business applications, including SAP SuccessFactors, ServiceNow, Office365®, Adobe®, Box®, Dropbox®, SAP S/4HANA, SAP Hybrid Cloud, and many others. These connectors provide data protection to application content while preserving application functions and ensuring compliance beyond the SaaS application provider's offering. PaaS ecosystem applications offered in each provider's marketplace are also protected by the CASB platform, providing customers greater control and visibility over which data is shared with these third-party PaaS providers. This suite of capabilities gives you one consistent approach and front-end interface to protect your data and help enforce compliance across all of your cloud environments. Our connectors can extend our security to the enterprise edge, so there is never any data within your clouds that is not protected, either by encryption or tokenization.

Lookout AnyApp for all of your Custom Applications

Our Lookout CASB AnyApp connector allows customers to integrate these powerful data protection capabilities for their own custom cloud-based applications. This allows enterprises to ensure that customer applications will be able to protect data regardless of their chosen cloud platform. AnyApp allows customers to bring their custom cloud-based applications the benefits of encryption, tokenization, dynamic access control, DRM, UEBA, threat prevention, and many other security features.

Flexible Delivery Models Speed Deployment

You can deploy in a matter of hours by using our hosted delivery. Administration and set-up are simplified and fast, so you can set up our powerful CASB protection to secure your ServiceNow instance in hours, ensuring all protection is applied beyond data encryption. We also support on-premise deployment in your data centers, fully hosted in the cloud, as well as hybrid (combining on-premise and hosted) options as necessary to support your compliance and operations strategy. Our cloud-native CASB platform simplifies deployment substantially and extends the definition of CASB to add end-to-end data protection with major enterprise SaaS, PaaS, and IaaS applications.

Supporting flexible and fast deployment is the Lookout platform architecture. Our Cloud Security Broker (CSB) provides API-connected integration to allow CASB capabilities to be embedded and used by SaaS vendor provided applications. The CSB uses the APIs published and well-supported by the cloud providers. The CSB integration model allows deeper inspection of all the users, content and collaboration aspects of select clouds to achieve higher levels of monitoring, control and protection (encryption).

Cloud Security Gateway (CSG) is an in-line proxy to enforce the strongest security policies and achieve data protection. Our in line support for applications provides the deepest and completely transparent field-level data protection for vendor-provided SaaS programs, such as ServiceNow, SAP SuccessFactors, ServiceNow, and many others as well as your custom applications.

You can deploy in a matter of hours by using our hosted delivery.



Leverage Existing Infrastructure

The Lookout platform allows you to integrate with existing enterprise security solutions to optimize existing investments including EDLP, SSO, and Antivirus/Antimalware solutions, to name a few. Customers can also integrate with existing SIEM solutions as well as consume data from enterprise firewalls and proxies to provide additional visibility on all clouds in use, including non-approved SaaS applications (Shadow IT).

- External DLP (EDLP) integrates existing enterprise DLP solutions with the Lookout platform, enabling organizations to maintain existing enterprise-specific DLP policies, extending them to data being uploaded to SaaS and cloud services. With this solution, organizations can maintain policy details specific to their environments while benefiting from the encryption and policy enforcement offered by Lookout.
- Single Sign-On (SSO) provides the ability to create and apply access policies to login actions. This ability enables more fine-grained access control over login activities for ServiceNow. The Lookout platform supports this feature by providing an IdP proxy entity. You can activate this feature by setting up the CSB IdP proxy to be part of the SSO flow in your enterprise.
- Antivirus/Antimalware (AVAM) provides additional detail for detection of many types of malware such as zero-day threats, viruses, spyware, ransomware, worms, and bots. This integration can ensure that any additional files uploaded to ServiceNow are protected from carrying malicious content that can affect internal ServiceNow users. You can configure multiple external services and apply specific services to policies as needed.



**Integrate
with existing
enterprise
security
solutions to
optimize existing
investments.**



Lookout CASB Benefits

- **Accelerate Cloud Adoption.** Expand your cloud adoption beyond ServiceNow by overcoming cloud security, data privacy, and compliance obstacles.
- **Increase Cloud Visibility.** Discover usage, data movement, and user activity within ServiceNow to minimize data loss and compliance risk.
- **Reduce Cost of Ownership.** One centrally controlled, easy-to-deploy hosted or hybrid platform to address all enterprise cloud requirements, providing end-to-end data protection and minimizing the scope of compliance audits.
- **Minimize Data Breach Risks with Powerful Data Protection.** End-to-end data protection and other key features ensure data is never stored unprotected in ServiceNow and other cloud applications or platforms, minimizing the risk of data breach, financial loss, and reputational and legal impact.
- **Prevent Forced 3rd Party Disclosures and Be in Control.** CASB brings a unique and powerful key management capability that is always in the customer's jurisdiction.
- **Enhance Collaborative Governance.** CASB provides a full solution for the collaborative sharing of data with 3rd parties, including full control over sensitive content and full monitoring and logging of activity.
- **Improve GDPR Readiness - One Solution to Meet Global Compliance Requirements.** The Lookout CASB architecture can address any mix of global compliance requirements and local privacy laws to simplify your cloud-based application adoption.



Lookout CASB Differentiation

- **Transparent Workflow Experience.** Lookout CASB extends data protection transparently and seamlessly to the user experience, ensuring application workflows are not affected.
- **AnyApp Connector.** Customers can integrate powerful CASB protection for sensitive data within their own custom cloud applications.
- **Application Specific Data Protection.** Lookout CASB provides the deepest levels of data protection within common enterprise SaaS applications.
- **Hybrid Architecture.** A single Lookout platform can support multiple application clouds and any mix of cloud and on-premise key management.
- **Enterprise Integration.** Complete integrations with EDLP, EDRM, SIEM, IAM, SSO, EMM, NGFW, and many more are available.
- **Encryption - Full End-to-End Data Protection.** Encryption at rest, in-flight, and in-use can address the strongest security requirements while still providing user transparency for typical application functions including search, reporting, sorting, charts, and more.
- **Zero Trust Key Management.** Full support for HMS and multiple on-premise keys enable you to address the most diverse compliance requirements.
- **Native Device Management.** Limit authenticated users by device type so that access is done only from trusted, designated platforms.
- **Secure Offline Data Access.** Built-in DRM or EDRM integration enable secure document access online and offline with the ability to revoke access instantly.

The Largest Multinationals in the World Use Lookout

5 of the Top 10 U.S. Banks

6 of the Top Banks Worldwide

3 of the Top 10 Insurance Firms

3 of the Top 10 U.S. Health Care Firms

3 of the Top 10 Pharmaceutical Firms

2 of the Largest Telecommunications Firms

Government agencies in the United States, United Kingdom, Canada, Australia, and beyond



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 and follow Lookout on its blog, LinkedIn, and Twitter.

© 2021 Lookout. All rights reserved. Lookout® is a registered trademark of Lookout. All other trademarks are the property of their respective owners. Cyber Killchain® is a registered trademark of Lockheed Martin. SharePoint®, OneDrive® and Office 365® are registered trademarks of Microsoft. SAP® SuccessFactors® are registered trademarks of SAP. ServiceNow® is a registered trademark of ServiceNow.