ESG SHOWCASE

Secure SaaS Contract Management with Evisort

Date: February 2021 **Author:** Doug Cahill, Senior Analyst

ABSTRACT: As the adoption of software-as-a-service (SaaS) continues to expand, so too do the associated use cases, resulting in an increase in sensitive data being stored in public clouds. Contract management is such a use case, one highly appropriate for the collaborative workflows SaaS applications enable. But trusting a cloud service provider (CSP) with sensitive data such as contracts raises data security considerations, concerns which can be addressed via an assessment framework. This document provides a prescriptive approach for prospective subscribers to gauge the security posture of a cloud-based contract management service, with a review of how Evisort meets these core SaaS data security requirements.

SaaS Adoption is Leading to an Increase in Cloud-resident Sensitive Data

Collaboration is Driving SaaS Expansion

The broad adoption of software-as-a-service (SaaS) applications continues to be driven by a number of compelling business benefits, including the enablement of collaborative workflows. The increase in remote work due to the COVID-19 business interruption has clearly been a catalyst; ESG research participants cite the broader use of online collaboration tools as the most significant lasting impact of the increase in work-from-home mandates as a result of the COVID-19 pandemic.[1] And this trend will continue, per the 43% of organizations who noted that, while they have made some investments in collaboration, they need to make more.[2]

The purposeful nature of how cloud applications enable collaboration is well aligned with the requirements for SaaS-based contract management, including:

- Centralization of contract documents via the use of cloud-based file sharing services.
- Orchestrated contract review workflows that extend to internal team members as well as third parties.
- And, notably, the use of on-demand compute to employ artificial intelligence for the accurate classification of sensitive content embedded in such documents.

The Increase in Third-party Access and Cloud-resident Sensitive Data

Cloud-based file sharing and contract management applications have resulted in third-party access to cloud-resident sensitive data by partners, contractors, legal counsels, and others. In fact, according to ESG research, the types of third parties with access to cloud-resident sensitive data includes business partners (40%) and contractors (34%).[3] At the same time, the percentage of cloud-resident sensitive data is increasing; 9% of organizations indicated that they believe that

[1] Source: ESG Research Report, *2021 Technology Spending Intentions*, January 2021.
[2] Ibid.
[3] Source: ESG Master Survey Results, *Trends in Cloud Data Security*, January 2019.

This ESG Showcase was commissioned by Evisort and is distributed under license from ESG.
© 2021 by The Enterprise Strategy Group, Inc. All Rights Reserved.

50% or more of their cloud-resident data is sensitive currently and 21% believe that 50% or more of their cloud-resident data will be sensitive two years from now.[4]

The increase in cloud-resident data shows that companies have increasingly become more comfortable with cloud-hosted applications for storage of sensitive data, which is why the security requirements below are so important.

The increase in cloud-resident data shows that companies have increasingly become more comfortable with cloud-hosted applications for storage of sensitive data, which is why the security requirements below are so important.

Assessing the Security Posture of Software-as-a-service (SaaS) Applications

Evaluating the security posture of a CSP starts with establishing a clear understanding of the cloud security shared responsibility model in which the service provider and subscriber each have a role in protecting cloud-resident data. Assessing how a CSP meets their obligations should be based on the pillars of a cybersecurity program: the people, processes, and technologies a CPS employs to comply with applicable regulations and security objectives.

Standards such as Service Organization (SOC) 2 serve as an auditing procedure for service providers so subscribers can rest assured that best practices are being followed. Similarly, the Continuous Assessment Initiative Questionnaire (CAIQ) provided by the Cloud Security Alliance (CSA) offers a framework to determine whether the appropriate set of cloud security controls are being employed. Systems integrators, service providers, vendors, and others also offer such frameworks. As such, what is offered below is a summary-level amalgamation for subscribers to assess a CSP's data security measures.

Public Disclosers

Nearly all CSPs will provide, typically via links at the bottom of their websites, the following documents:

- Privacy Policy. This document will outline what data is collected and the treatment of personal information with respect to how it is used and with whom it is shared.
- Privacy Statement. This document will expand upon the privacy policy to also convey, notably, data residency and transfer policies with respect to whether customer data is being moved between data centers.

Certifications

Certifications will include attestations of compliance with standards and regulations, including local and international data privacy laws such as the General Data Protection Regulation (GDPR). Of note is SOC 2, designed specifically for auditing the processes and controls employed by CSPs to protect subscriber data. CSPs should, at a minimum, be able to provide SOC 2 Type 1 reports, or, ideally, a Type 2 report, the former speaking to the controls in use, and the latter more exhaustively covering the controls their relative efficacy at the CSP. The Cloud Security Alliance's (CSA) Cloud Controls Matrix (CCM) provides a mapping of compliance with a range of standards and best practices. Collectively, these certifications will indicate whether a CSP has a sufficiently robust data security program.

[4] Ibid.

© 2021 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Zero-trust-based Access Policies

Representing a departure from "trust, but verify" to "don't trust, continuously verify," zero trust has become a foundational cybersecurity approach, one that is highly applicable to the secure access to sensitive data by humans and machines. Examples of zero-trust measures include the use of multi-factor authentication and an expansion of how trust is established with consideration of the profile of the device being used to access critical systems. Zero trust also includes the use of micro-segmentation between server workloads and/or application containers to prevent threats from moving laterally.

Segregation of Duties and Least Privilege Access Management

The focus on people also requires segregation of duties (SoD), an approach requiring more than one person to perform a task to mitigate against fraud and errors, as well as to establish an audit trail of activity. SoD is closely related to least privilege access (LPA) management, in which the least number of employees have access to the least amount of data with the least amount of privileges required to perform a given task. For example, some employees may only need read rights and not full administrative privileges or access to only a subset of subscriber information.

Given the need to implement SoD and LPA best practices, CSPs should have an identity governance and administration (IGA) program which, amongst other measures, should include the regular review of roles to identify overly permissive accounts.

Data Security

Encryption

CSPs should be encrypting sensitive customer data while it is both in motion and at rest. Once at rest, key management practices such as rotation are critical as is the use of hardware security modules (HSM) for the secure separation of data. CSPs should also employ strong authentication measures (i.e., multi-factor authentication) to control access to the keys.

Residency, Transfer, and Auditing

Beyond location, transfer is more relevant when it comes to data privacy regulations, such as the GDPR and the California Consumer Privacy Act (CCPA), with respect to the controls in place for when an individual outside of a geography in which the data is located accesses the data. To that end, logging provides an audit trail of who had access to what data when, a requirement for many regulations, and critical for investigative purposes. Financial institutions have extra audit requirements for which CSPs should be able to provide additional audit rights as required by regulatory bodies.

Threat and Vulnerability Management

While the aforementioned sections refer largely to insider access to subscriber data, CSPs should also be proactive in protecting against external threats. Vulnerability management measures should span the application lifecycle starting in the development phases via the use of application security testing (AST) controls and continue to the build and runtime stages. In the build and runtime stages, vulnerability management requires identifying and correcting both configuration and software issues. To protect against new and unknown vulnerabilities, CSPs should also employ runtime controls, which can detect and prevent anomalous activity that may be indicative of a new and unknown exploit. Similar to scanning for vulnerabilities in different environments, CSPs should also be scanning for malware in pre-deployment and production.

© 2021 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Configuration Management

As noted, vulnerability management should be extended to the configuration of cloud services, which should be hardened pre-deployment based on standard benchmarks such as those published by the Center for Internet Security (CIS). CSPs should also be able to prevent the deployment of misconfigurations, inclusive of unauthorized software via admission control measures. This focus on configuration management best practices should include vetting infrastructure-as-code (IaC) templates pre-deployment to assure only hardened configurations are deployed to production.

Cyber Resiliency

The more critical a SaaS application and the more sensitive the data stored with that service, the more important it is for a CSP to be able to convey how its service is resilient. Business continuity and data recoverability measures must be in place to restore service and recover data from secure backups. Incident response measures, including playbooks, should be in place for the prompt remediation of threats and the responsible disclosure of such incidents to subscribers.

Penetration Testing

All of the above needs to be tested for efficacy via regular penetration testing at least annually. Prospective subscribers may want to consider penetration testing periodicity, the results of recent tests, and, if issues were surfaced, proof of remediation. Some CSPs may also employ a bug bounty program as a proactive means to a continuous approach to penetration testing versus relying solely on point-in-time tests.

Evisort's Approach to Cloud Data Security

Evisort is SaaS-based contract management service that utilizes cloud-based services to enable centralized contract management and collaborative workflows. Given the sensitive nature of many contracts, subscribers to Evisort's service may want to assess the company's security posture relative to the framework offered above. ESG has found that Evisort meets these requirements as follows:

- Publicly Available Information. Evisort publishes its privacy policy, privacy statement, and a statement of GDPR compliance via links on the bottom of its homepage. These documents provide transparency with respect to what information is collected, how it is used, with whom it is shared, how it is stored, and more.
- SOC 2 Report. Evisort can provide the results of the company's successful SOC 2 Type 2 audit, completed by an independent CPA firm, inclusive of the results of the auditor's tests of the company's security controls.
- Cyber Resiliency. The company has both a business continuity plan and data protection plan, as well as an incident response plan.
- Restricted Access. Evisort has a series of policies and measures that restrict access to subscriber data consistent with the zero-trust approaches discussed above.
- Data Security. The company's approach to data security includes the classification of sensitive data, the use of encryption for both in-flight and at-rest data, and a series of key management practices.
- Change Management. In addition to an asset management plan, Evisort utilizes change management processes and controls to maintain known-good standard configurations and prevent the introduction of unsanctioned components.

© 2021 by The Enterprise Strategy Group, Inc. All Rights Reserved.

The Bigger Truth

Cybersecurity, and specifically data security, is a strategic imperative for any cloud service provider who serves as the custodian of customers' sensitive data. Doing so is simply fundamental to their business model since confidence in a CSP's ability to protect cloud-resident data is a clear requirement for prospective subscribers. As such, subscribers understandably require a level of transparency from their CSPs.

To assuage any concerns, a framework that serves as an approach to assess the security posture of a CSP is required. Such a framework must encompass both the processes and technologies employed by the CSP to protect cloud-resident sensitive data from compromise. ESG ascertains from reviews of Evisort's public disclosures and other materials a strong and consistent commitment to data privacy and security across the domains discussed previously. Furthermore, Evisort effectively leverages cloud services, including the use of cloud-based file sharing, integrated workflows, and artificial-intelligence-powered data classifications, as the basis for a modern approach to contract management.

ESG ascertains from reviews of Evisort's public disclosures and other materials a strong and consistent commitment to data privacy and security across the domains discussed in this showcase.

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of The Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at 508.482.0188.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

www.esg-global.com contact@esg-global.com 508.482.0188

© 2021 by The Enterprise Strategy Group, Inc. All Rights Reserved.