APPSIAN

SOLUTION BRIEF

Addressing CCPA: Legacy ERP and Data Privacy Compliance

Abstract

Going into effect on January 1, 2020, the California Consumer Privacy Act (CCPA) has many organizations scrambling to prepare. A recent survey[1] by PwC indicated that only 52% of respondents expect to be compliant with CCPA by its 2020 launch date. Even with an additional 6-month grace period before punitive enforcement, organizations face a looming deadline to meet the compliance criteria.

Since the introduction of the EU's General Data Protection Regulation (GDPR), more and more regulatory authorities are coming up with data protection mandates to safeguard the privacy and integrity of their citizens' personal information. While CCPA is the latest in a growing list of regulations, other states are beginning to follow. In fact, 17 states have already introduced legislation[2] concerning a comprehensive approach to governing the use of personal information in their state. This is in addition to the data breach notification laws which all 50 states and major US territories have previously enacted[3] – laying the foundation for more sophisticated data privacy laws to come.

CCPA & ERP Applications

The abundance of personally identifiable information (PII) within ERP applications creates a risk for organizations that will only grow with compliance requirements. Non-compliance with CCPA or data privacy regulations in general can lead to punitive fines along with loss of consumer trust and reputational damage. The cost of non-compliance can quickly add up in expenses associated with investigations, lawsuits, remediation efforts, and more.

While the compliance guidelines may vary from one regulation to another, organizations must adopt data protection best practices to avoid non-compliance with all data privacy regulations, current and upcoming. Organizations must also strengthen breach detection and reporting capabilities so that incidents can quickly be addressed in the stipulated timeframe as required by specific breach notification mandates.

This solution brief explores how organizations can enhance their legacy ERP applications to improve compliance with CCPA and establish the capabilities to prepare for the uncertainty around data privacy. This document aims to highlight the gaps within existing security capabilities and provides solutions to overcome them with Appsian Security Platform.

The California Consumer Privacy Act - What is it?

Expanding the rights of Californians, the CCPA demands businesses to be more transparent about how they collect, use, and disclose personal information. The CCPA aims to empower consumers by giving them more control over their personal information and provides citizens with the following rights:

a. Right to access information
b. Right to erasure
c. Right to opt-out
d. Equality of service
e. Right of minors

Penalties for Non-Compliance

Non-compliance with the CCPA can lead to fines of up to $2,500 per violation or $7,500 per intentional violation and businesses will be allowed 30 days to remedy alleged violations. However, actual penalties can only be assessed by the Attorney General of California. The CCPA also offers a private right of action that allows consumers to seek damages if a business fails to protect their personal information. While statutory damages can only be between $100 and $750 per incident, a higher amount of actual damages will be levied if deemed appropriate by the Attorney General of California.

Ambiguity in the Regulation Guidelines

The CCPA has captured the spotlight for its ambiguous guidelines and unclear implications as the regulation continues to undergo substantive legislative changes. A lack of adequate 'solid' guidelines under CCPA will be the cause of chaos in the days to come. For instance, a business's obligations under the CCPA arise if it receives a 'verifiable consumer request'. However, the mandate does not explain how a business can verify such a request (in case consumers are unwilling to provide any additional personal information).

In its current form the act also seems to lack clarity in how organizations can prove compliance. In the event that a business complied (and deleted consumer data), will they be allowed to retain any consumer information in order to substantiate their compliance? The statute currently does not provide an answer to this.

There are several similar points of scrutiny and over 40 bills have been introduced to make changes to the law so far. Despite the uncertainty, by following a standard set of data protection best practices, organizations can prepare for CCPA compliance and establish readiness ahead of time.

Compliance Challenges for Legacy ERP Applications

Legacy ERP applications offer limited visibility

Out-of-the-box, most legacy ERP applications do not record sufficient details around user activity such as what PII was accessed, who accessed it, and from where. Native application logs are typically limited to high-level activity or focused on system performance data required for application testing and troubleshooting. Also, logs are often bulky and unstructured, and manual analysis of these logs can be time-consuming and inaccurate. In the absence of granular and detailed user activity logs, organizations will fail to derive the necessary information for audit requests under CCPA and stand the risk of non-compliance.

Manual, time-consuming audits are unscalable

As the CCPA deadline draws closer, organizations must prepare for an avalanche of audit requests from individuals as well as the regulatory body. Once live, organization will need the capacity and capabilities to produce an abundance of specific information, all within the stipulated timeframe of 30 days.

ERP applications house PII on hundreds of pages. Sifting through massive, complex and detailed logs to track down a specific security incident or a specific record can be tedious and time consuming. With CCPA's strict breach notification and redressal timelines, it is essential that organizations are equipped with access to real-time data that helps security teams identify, investigate, and remediate security incidents quickly – and to minimize if not eliminate the implications of non-compliance.

Static security controls hinder data protection

To reduce the risk of non-compliance, organizations need methods that avoid unnecessary exposure of PII in the first place. However, certain limitations can prevent organizations from achieving the desired level of data and access controls:

- Data Masking

Under the CCPA, organizations can avoid penalties if the compromised data is masked, redacted or encrypted. Legacy ERP systems often offer data masking for sensitive records, but those capabilities can be limited to specific records and fields (DOB, SSN, and bank account number) and can be time consuming to implement. Moreover, data masking is implemented based on static roles only. As a result, users either cannot view sensitive information at all, or they can view all of it. Also, masking often extends to the UI-level only – meaning queries and reports can still expose otherwise masked data.

- Static Access Control Rulesets

Like data masking, access controls in legacy ERP applications are controlled by static roles and permission lists. For example, privileged users can access sensitive data regardless of where they are accessing it from. This is so because access is not governed by the context of access such as location, IP address, nature of data, time of the day, and more. Due to the lack of contextual controls, organizations cannot customize access rules and are at risk of PII exposure through external attacks, malicious insiders, and accidental insider data leakage.

Solution

Appsian Security Platform (ASP) addresses the end-to-end security and compliance needs of legacy ERP applications in today's modern, dynamic environment. Equipped with detailed user behaviour visibility, integrated analytics, contextual access controls and fine-grained data security, ASP enhances the security and compliance posture of SAP, PeopleSoft and Oracle ERP applications.

Detailed User Activity Logging

ASP's enhanced logging records all transactions within legacy ERP applications on a granular level, providing the level of detail needed to comply with CCPA, fulfill audit reporting, and to investigate and respond to breaches efficiently. ASP expands native ERP logging capabilities to capture additional field-level information on what information was accessed, where it was accessed from, user ids, IP addresses, pages accessed, actions performed and more – information that can be critical for compliance reporting. The logging data does not require additional infrastructure and can be stored within existing security information and event management systems. In some cases, ASP facilitates the recording of missing information in existing logs and allows organizations to combine the two for accurate and detailed compliance reporting.

Real-Time Analytics for Security & Compliance

ASP features an analytics extension called Real-time Analytics. While ASP records all transactions within ERP applications creating detailed activity logs, data trends are aggregated and displayed on engaging, visually rich dashboards. Integrated analytics were always a 'nice-to-have' feature for security teams; however, keeping CCPA deadlines of breach identification and reporting in mind, they have become a must-have feature. These advanced dashboards equip security professionals with real-time snapshots of data usage. The drill-down capabilities allow for enhanced data discovery and exploration to expedite breach detection and response, thereby helping organizations stay compliance ready not only for CCPA but other existing and upcoming regulations as well.

Fine-Grained and Contextual Security Controls

Appsian Security Platform enables organizations to tighten security around protected information while still maintaining usability. ASP addresses the data protection requirements of CCPA and other data privacy mandates in two key ways: 1.) improving field and transaction level security and 2.) enhancing access control capabilities. ASP's dynamic data masking allows organizations to minimize the exposure of sensitive information, and in turn, reduce compliance risk. Data fields can be fully or partially masked, redacted, or protected with a click-to-view masking feature that limits exposure without eliminating usability.

To improve access control, ASP combines static roles and privileges with dynamic user and data attributes to enable contextual security – allowing organizations to tighten their access control policies without hindering usability. For example, access to certain high-risk transactions can be restricted based on a user's location, or access can be granted but with masked data fields. By reducing the threat surface, ASP reduces the risk of data leakage and mitigates the damages of compromised access.

Conclusion

Risk management and compliance have evolved from being IT centric issues to impacting enterprise-wide business functions like legal, HR, supply chain, finance and more. Data protection mandates such as CCPA and GDPR have increased the pressure on security teams to better manage sensitive data and the risks surrounding it. The key to success lies in understanding the needs of your organization's unique IT and business structure and incorporating prevention and remediation features throughout.

When it comes to legacy ERP applications like SAP, Oracle, or PeopleSoft, layering prevention, visibility, as well as remediation features within your applications, on a granular level, can ensure that you are prepared to minimize if not eliminate potential risk to sensitive data. Monitoring user activity, establishing access controls, and eliminating unnecessary privilege can help propagate compliance as an organizational culture rather than being an obligatory operational burden.

References:

[1] https://www.pwc.com/us/en/services/consulting/cybersecurity/pulse-survey-ccpa.html

[2] https://iapp.org/news/a/us-state-comprehensive-privacy-law-comparison/

[3] http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx