Solution Brief

Grip SaaS Security Control Plane Boosts California Consumer Protection Act (CCPA) Compliance

Introduction

The California Consumer Privacy Act (CCPA) has set a precedent for stringent data privacy regulations, compelling companies to reevaluate how they store and manage consumer data. One of the significant challenges businesses face under CCPA is managing data across various SaaS applications, especially those used outside of the IT department's purview. This is where the Grip SaaS Security Control Plane (SSCP) comes into play, offering a robust framework to enhance compliance with CCPA. This paper explores how the Grip SSCP aids in discovering rogue SaaS usage, documenting data storage, automating compliance processes, and securing data in response to CCPA requests, with a focus on specific CCPA regulations.

Discovering Unauthorized SaaS Usage and CCPA's Right to Know (§ 1798.110)

Under CCPA, consumers have the right to know what personal information is being collected about them. This includes understanding the categories of personal information and the sources from which it is collected. The challenge for businesses is that unauthorized or shadow SaaS applications can store or process consumer data without IT's knowledge, creating a compliance risk.

Grip SSCP Discovers Shadow SaaS Usage:

The Grip SSCP addresses this challenge by providing comprehensive visibility into all SaaS applications being used within the organization. This ensures businesses can accurately respond to consumer inquiries under the CCPA's Right to Know provision. By identifying all applications, especially those outside of IT's purview, that are processing consumer data, the company's compliance team can review the stored data to determine whether the CCPA regulations apply.

Documenting Data Storage Locations and CCPA's Data Inventory Requirements (§ 1798.100)

CCPA requires businesses to maintain specific records of personal information, including the categories of personal information and the categories of sources from which the information is collected. The proliferation of SaaS makes this extremely difficult for most organizations. Employees often sign up for SaaS applications to complete a project or task, but they do not report these new applications to IT or compliance, even if the data being used includes consumer data. As a result, most companies lose track of where consumer data is stored.

Grip SSCP Identifies Where Consumer Data is Stored:

With the Grip SSCP, companies can automatically map identify where consumer data may be stored across all their SaaS applications. This mapping includes both sanctioned and unsanctioned applications, providing a comprehensive inventory of consumer data storage locations. This documentation is vital for maintaining the records required by CCPA, enabling businesses to quickly identify and report where a consumer's data may be held.

Automating Business Justification Queries and CCPA's Collection Minimization ($ 1798.100)

The CCPA emphasizes the principle of collection minimization, stating that businesses should collect only the personal information necessary for the purposes they have disclosed to the consumer. To comply, companies should evaluate any new SaaS applications that collect personal information and ensure that the purpose has been disclosed to the consumer. Documenting the business justification for these SaaS applications and updating any disclosures necessary is essential for compliance.

Grip SSCP Automates Justification and Minimizes Data Collection:

The Grip SSCP automates the process of querying users and departments for their business justification for using specific SaaS applications. The query can also ask the employees to attest to any personal data that is collected and alert compliance to update the company's disclosures. This ensures that justifications are consistently recorded and easily accessible, helping businesses demonstrate compliance with CCPA's collection minimization principle. The company's consumer disclosures can also be updated on a regular basis.

Securing Data for CCPA Requests and the Right to Delete ($ 1798.105)

Under CCPA, consumers have the right to request the deletion of their personal data held by a business. Responding to these requests can be challenging, particularly when data is dispersed across multiple SaaS applications. Those that have been provisioned by users on their own require individual employees to be a part of complying with any deletion request, which is not realistic. Without a comprehensive inventory of all the SaaS applications where data may be stored, any attestation to the consumer that their personal data has been deleted will be incomplete.

Grip SSCP Identifies Apps Where Data Deletion is Required:

The Grip SSCP simplifies this process by providing tools to track the SaaS applications where data deletion is required to comply with CCPA requests. This includes officially sanctioned applications and those that employees procured on their own and never reported to IT. By centrally tracking all the SaaS applications being used, Grip SSCP reduces the risk of errors and ensures that complying with CCPA's Right to Delete requirements can be done smoothly.

Conclusion

The Grip SaaS Security Control Plane is an invaluable tool for businesses looking to enhance their compliance with the CCPA. By providing comprehensive discovery of all SaaS applications, documenting data storage locations, automating compliance processes, and securing data in response to CCPA requests, the Grip SaaS Security Control Plane helps businesses protect consumer privacy and meet regulatory requirements efficiently and effectively. This proactive approach to SaaS security not only aids in compliance but also strengthens the organization's overall security posture, ensuring that consumer data is protected across every touchpoint.