Bitglass SaaS Security Posture Management (SSPM)

When organizations use a software-as-a-service (SaaS) solution, they inevitably receive a myriad of benefits, including improved efficiency and flexibility. SaaS offerings such as Salesforce, ServiceNow, and Office 365 are highly effective tools for any enterprise.

SaaS vendors go to great lengths to make sure that the infrastructures upon which their app offerings are built are highly secure; however, it is the responsibility of the customer to use said apps in a safe fashion. SaaS security posture management (SSPM) is a key tool for organizations striving to do so.

Why SSPM Matters

SaaS solutions require various configurations in order to make sure that they function properly. Failing to apply even a single setting correctly can prove disastrous for any company. Consequently, fixing misconfigurations within SaaS applications is a critical step in the quest to prevent data leakage and malicious data corruption. Fortunately, SSPM solutions are designed to address this.

Bitglass SSPM

With Bitglass, organizations have everything that they need in order to identify and remediate costly misconfigurations within SaaS applications. By integrating with SaaS apps via API, Bitglass SSPM can crawl SaaS instances in search of inconsistencies with custom benchmarks defined by your organization, as well as established security standards like the Center for Internet Security (CIS) Benchmark, the Health Insurance Portability and Accountability Act (HIPAA), or the General Data Protection Regulation (GDPR).

Uncovered misconfigurations are then grouped by category. Misconfiguration categories and example misconfigurations for Salesforce and ServiceNow are summarized in the tables below.

Salesforce

Misconfiguration Category	Example Misconfiguration
Network Access	IP range restrictions are not activated
Identity and Access Management	Password policy does not prevent the reuse of previous passwords
Session Settings	Requirement for HttpOnly attribute not set
File Security Details	Number of security risk file types with hybrid behavior is more than zero

ServiceNow

Misconfiguration Category	Example Misconfiguration
Multi Factor Authentication	MFA for high-privileged roles is not enabled
Identity and Access Management	Blacklisted passwords are not set
Session Settings	No limit set on concurrent sessions
Data Protection Baseline	No session timeout set

Through Bitglass' dashboard, the number of misconfigurations in each of these categories is displayed graphically, revealing how organizations' SaaS security postures are changing over time. In addition to this information, companies are provided with tailored remediation steps that they can follow in order to address discovered issues and ensure the proper configuration of their SaaS instances. Alternatively, with the click of a button, they can allow Bitglass to perform this remediation on their behalf and fix all misconfigurations automatically.

About Bitglass

Bitglass' Total Cloud Security Platform is the only secure access service edge offering that combines a Gartner-MQ-Leading cloud access security broker, the world's only on-device secure web gateway, and zero trust network access to secure any interaction. Its Polyscale Architecture boasts an industry-leading uptime of 99.99% and delivers unrivaled performance and real-time scalability to any location in the world. Based in Silicon Valley with offices worldwide, the company is backed by Tier 1 investors and was founded in 2013 by a team of industry veterans with a proven track record of innovation and execution.