



SaaS Security Posture Management



Complete Control For Your SaaS Security

Proactively find and fix weaknesses across your SaaS platforms and maintain continuous security for all global settings, user-specific settings and user privileges

The screenshot shows a security check failure notification for 'User Authentication to Join Meetings'. The status is 'Check Failed' and the score impact is 'Medium'. The description states: 'Participants don't need to authenticate before joining meetings scheduled by affected hosts.' Below the description, there is a table of affected users:

Users	Department	Status
daniel@thiscompany.com	Marketing	Global
steve@thiscompany.com	Marketing	Dismiss
jenna@thiscompany.com	Sales	Global
kate@thiscompany.com	Sales	Dismissed
michael@thiscompany.com	Legal	Dismissed

Spot Weaknesses Across Your Entire Stack

Continuously monitor all your SaaS apps, detecting any misconfigurations, incorrect permissions, and all possible exposures, wherever they may be

The screenshot shows a ticket creation interface. The ticket channel is 'ServiceNow, IT Service Management' and the assignee email is 'john.smith@thiscompany.com'. The ticket summary is 'Salesforce, Sales Ops: Security check "Custom Sites Cross-site Scripting Protection" Failed'. The ticket description includes a check description, remediation steps, and more info.

Check Description: Affected sites don't have cross-site scripting protection enabled

Remediation: In the Setup menu, User Interface > Sites and Domains > Sites, edit the affected site/s. Check "Enable Browsed Cross Site Scripting Protection" checkbox.

More Info: Determines whether protection against reflected cross-site scripting attack is enabled in custom sites. If a reflected cross-site scripting attack is detected, the browser shows a blank page with no content.

Automate the Entire Fixing Process

Disseminate risk context and remediation to each SaaS respective owners, track progress, validate and monitor risk reduction. Catch configuration drifts as they happen and stop minor incidents from becoming major problems



Native security controls, misconfigurations and exposures across SaaS platforms

- Analyze all built-in security controls and settings
- Identify exposures and misconfigurations
- Quantify security-related settings into a per-SaaS and overall normalized posture score
- Benchmark against compliance frameworks (e.g. SOC II, ISO 27001, PCI-DSS) and industry best practices (NIST, CIS)



Remediation and monitoring

- Automate remediation using ticketing with complete context
- Track progress and alert on degradation and configuration drifts
- Follow trends over time
- Perform retrospective investigation



Users' cloud access governance

- Discover all your SaaS users - employees, partners, guests
- Continuously measure each user level of exposure
- Identify users with excessive permissions
- Trim unused permissions and de-provision inactive users
- Identify and disable insecure user authentication methods



Enterprise-grade platform

- ISO 27001 certified
- Role based access and granular user profiles
- Single sign-on support
- Alerts and notifications
- User and system auditing

Supported SaaS Platforms Sample List

