valence threatLabs

2023 SaaS Security Trends & Insights

This infographic details some of the more notable trends and challenges related to third-party apps, OAuth integrations, external data sharing and unmanaged identities.

Pediatric Patient Exams.pdf
Github backup codes.docx
salary and budget breakdown.xlsx
1password emergency kit.pdf
Gary's New Passport.pdf
Microsoft Edge Passwords.csv

Integrations: Everything, Everywhere, All at Once

Sometimes SaaS administrators give third-party integrations access to everything. This gives third parties full read-write access to email, files, source code and more.

100% of organizations have granted full read/write access to email, files and calendars to at least one third party.

On average, there were **21 integrations per organization** with tenant-wide access to company and employee data.

IMPACT

A single compromised token at this level could compromise all employee email, files and calendars or leave the organization open to SaaS supply chain attacks.

Data: Great Power, Little Responsibility?

Employees are often just trying to get the job done. The risks of oversharing might not be clear to them. It takes only a few clicks to put massive amounts of data at risk through file and data sharing (via Google Drive, OneDrive, Box, etc).

90% of an organization's shared assets (e.g. files or folders shared to "anyone with the link"), on average, hadn't been accessed for at least 90 days.

30% of the time, files are shared with personal accounts such as Gmail.

IMPACT

Most sharing needs are urgent and temporary, but once the need passes, they are forgotten. Attack surface continually grows over time, never shrinking.

Identities: Sleepy Accounts, Active Risks

Dormant employee accounts can be a source of serious risk, especially when misconfigured. They're easy to overlook, and risky employee actions can remain, even when accounts are removed.

1 in 8 employee accounts are dormant, on average (and as high as 1 in 3 in some companies).

On average, **10% of an organization's shared integrations and privileges** can be traced back to ex-employees.

IMPACT

Attacks often target dormant accounts, as there is less focus and visibility on them, and there's a lower chance that they're compliant with current security policies.

Misconfigurations: Death by Exception

While issues with integrations and file sharing could be seen as 'death by a thousand cuts', it often only takes one misconfiguration to let an attacker in. Accounts that require exceptions (e.g. service accounts and guests) make it easy to overlook active user accounts missing basic security, like MFA enforcement.

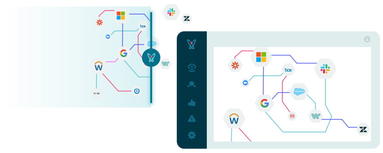
In most tenants, MFA wasn't enforced by default for all user accounts leading to at minimum **1% of accounts** without proper MFA configuration.

IMPACT

Even if as low as 1%, we've seen over and over, credential stuffing via a single misconfigured account can lead to total compromise.

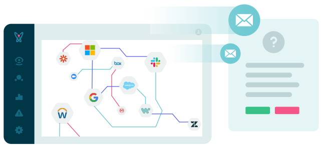
The Valence Platform

Valence enables you to eliminate your third-party integration, identity, and data sharing risk surface by automating workflows that engage with your business users across critical SaaS applications like Microsoft 365, Google Workspace, Salesforce and Slack.



Discover & Gain Unified Control Across Your SaaS Mesh

Valence's unified cross-SaaS data and permissions model reduces the need for in-house security expertise for each SaaS application, allowing security teams to easily enforce consistent security guardrails.



Engage, Educate & Empower Your SaaS Business Users

Scale remediation workflows by engaging business users, educating them about their SaaS security risks, and empowering your security team as business enablement champions.

Malicious 3rd Party App Detected
External Data Share Detected
User Without MFA Detected

Automate SaaS Security Policy Enforcement

Valence’s out-of the box SaaS security remediation workflows reduce the manual effort required to remediate SaaS risks associated with supply chain, identity, and data sharing.

Valence Use Cases

SaaS Mesh Discovery

Ensure continuous discovery and contextualization of your third-party SaaS applications.

SaaS-to-SaaS Governance

Remove risky and suspicious third-party integrations such as OAuth and APIs to reduce supply chain risks.

Data Protection

Secure your data from oversharing risky configurations that leave it exposed to external threats.

Misconfiguration Remediation

Detect misconfigured security controls/settings and drifts from defined SaaS security policies.

Identity Security

Detect identity and permission drift to ensure strong authentication and least privilege access.

About Valence

Valence secures critical SaaS applications like Microsoft 365, Google Workspace, Salesforce and Slack, while accelerating business productivity and the speed of SaaS adoption. Valence is backed by leading cybersecurity investors like Microsoft’s M12 and YL Ventures, and is trusted by leading organizations.

About Valence Threat Labs

Valence Threat Labs designs defenses against the latest SaaS risks. Through in-depth analysis of SaaS threats, Threat Labs helps protect organizations from account takeovers, data leaks and other SaaS-related risks. Threat Labs contributes to the SaaS security community with original research, advice and best practices.

Register to receive a copy of the full report when it is released.

valencesecurity.com/2023report