Reduce SaaS and Data Risk with Zscaler SSPM

Secure all your SaaS platforms, including AI and third-party integrations, with one integrated approach.

OCTOBER 2026

zscaler™

SaaS sprawl creates hidden exposure

SaaS and AI adoption are outpacing security oversight, creating blind spots across apps, integrations, identities, and access. Risk now extends beyond misconfigurations to excessive permissions, risky SaaS–to–SaaS connections, orphaned accounts, unmanaged AI services, and compliance drift.

Today, top SaaS Security challenges include:

Shadow Apps & AI Risk	Breach Impact	Risk Governance
55%	4.44M	75%
Employees adopting SaaS w/o security's involvement	average breach cost due to SaaS configuration error	of organizations experienced SaaS security incident

- Shadow SaaS and unsanctioned AI tools expand the attack surface
- Misconfigurations and posture drift create exploitable gaps
- OAuth apps and third–party integrations introduce unmanaged access and excessive privileges
- Compliance becomes difficult to maintain across dynamic SaaS environments

Legacy security tools lead to fragmented visibility, control and slow response that often leave SaaS risk unresolved leading to data loss, unauthorized access, audit gaps, and business disruption. Organizations need unified visibility, automated control and continuous posture management—not point–in–time assessments—to reduce risk and stay ahead of change.

©2026 Zscaler, Inc. All rights reserved.

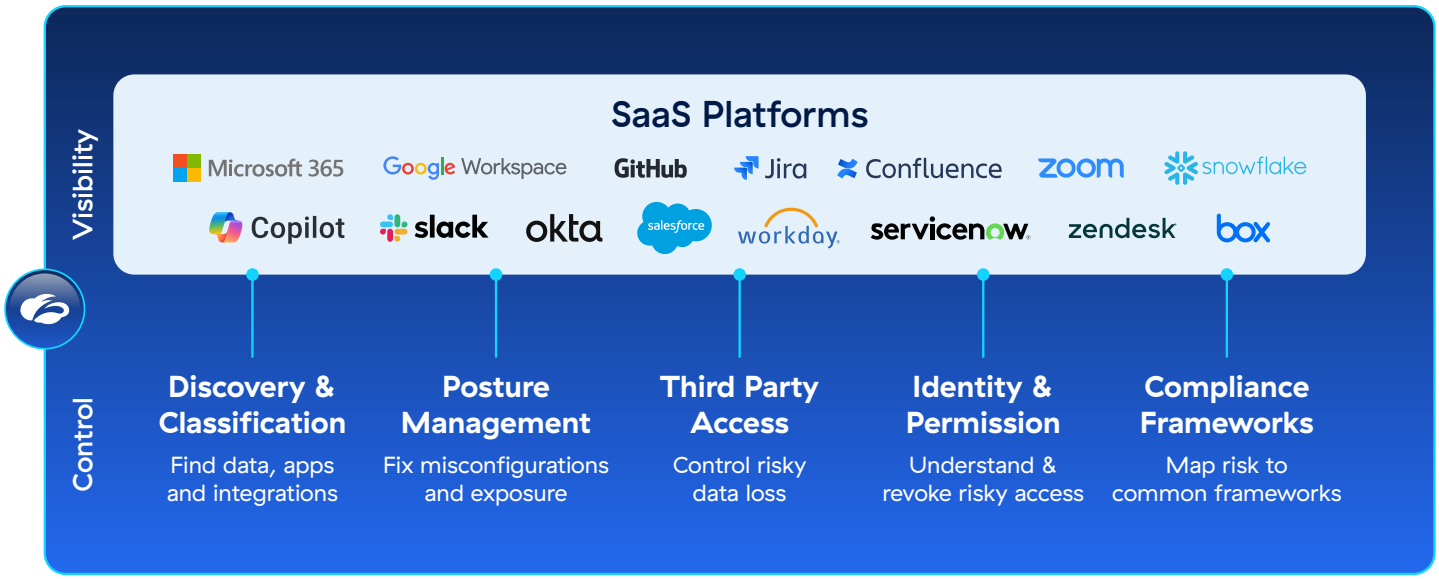
Take control of SaaS Security with Zscaler SSPM

Reduce SaaS and AI risk across apps, identities, integrations, and compliance.

Zscaler SSPM helps organizations secure SaaS apps and platforms with unified visibility into apps, users, data, identities, configurations, exposure, and connected services. It connects SaaS posture, identity, third party integration, compliance, and data context to uncover hidden risks and attack paths. It prioritizes and accelerates risk remediation with risk insights, alerts and workflow automation to reduce data exposure, and ensure compliance with industry standards while keeping pace with modern SaaS and AI adoption.

This enables security and GRC teams to:

- **Discover the entire SaaS estate,** including shadow apps, data and AI tools
- **Manage access risk** such as configuration drift, policy violations, and risky integrations
- **Prioritize risk remediation** based on risk, context, and business impact
- **Automate compliance** with predefined best practices and industry standards.



©2026 Zscaler, Inc. All rights reserved.

Zscaler SSPM Benefits:

- Reduce SaaS risk: Continuously identify and reduce risk from SaaS misconfigurations, risky settings, excessive access, configuration drift, and exposed integrations.
- Reduce SaaS Supply Chain Risk: Discover and assess third-party apps, OAuth grants, browser extensions, add-ons, and SaaS-to-SaaS integrations that expand the attack surface.
- Improve identity and access governance: Identify risky users, privileged roles, dormant accounts, external collaborators, and over-permissioned access before they become attack paths.
- Prioritize what matters most: Focus teams on the highest-impact risks using contextual risk scoring across posture, identity, access, data exposure, and integration risk.
- Accelerate secure AI adoption: Govern AI-enabled SaaS apps and integrations, such as Microsoft 365 Copilot, by assessing configurations, access controls, and oversharing risk.
- Protect Browser Extensions: Assess and secure browser extensions with continuous visibility, monitoring, context, prioritization and policy-driven governance.
- Maintain compliance and audit readiness: Simplify compliance with built-in and custom frameworks, continuous control monitoring, and audit-ready reporting.

Top use cases

- Strengthen SaaS security posture: Continuously monitor SaaS applications for misconfigurations, risky settings, policy drift, and posture gaps that could expose the business to risk.
- Govern third-party and SaaS supply chain risk: Discover, assess, and control third-party apps, OAuth permissions, add-ons, browser extensions, and SaaS-to-SaaS integrations.
- Reduce identity and access risk: Assess users, admins, external collaborators, dormant accounts, privileged roles, and excessive entitlements to reduce identity-based attack paths.
- Maintain compliance posture: Map SaaS configurations, access controls, data exposure risks, and security policies to frameworks, best practices, and regulatory requirements.
- Automate remediation workflows: Integrate with SIEM, SOAR, ITSM, and collaboration tools to trigger alerts, create tickets, route approvals, and accelerate remediation.

©2026 Zscaler, Inc. All rights reserved.

Why Zscaler SSPM?

- Unified platform approach: Consolidate SaaS posture, discovery, data classification, risk correlation, and automated workflows into one platform to strengthen security, reduce operational complexity, and maintain compliance.
- Broad SaaS, AI and Integration coverage: Gain visibility and control across thousands of unique SaaS services, third party add-ons, browser extensions – including sanctioned, shadow apps, AI tools, third-party integrations, and identity driven risk.
- Beyond basic SSPM: Go beyond configuration checks with continuous governance across posture, identity and access risk, data exposure, AI usage, third-party integrations, browser extensions, and SaaS supply chain risk.
- Fast time to value: Deploy quickly with a single read-only connection, reducing heavy configuration, complex integrations, and long implementation cycles.
- Security and compliance alignment: Connect SaaS security posture directly to regulatory frameworks with dedicated compliance dashboards, continuous control monitoring, and audit-ready reporting.

Learn more

Visit Zscalers SaaS Security Website

Watch the Interactive Product Tour

Schedule a Demo now

About Zscaler
Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 200 data centers globally, the SASE-based Zero Trust Exchange is the world's largest inline cloud security platform.
Learn more at **zscaler.com** or follow us on X **@zscaler**.

© 2026 Zscaler, Inc. All rights reserved. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, ZPA™ and other trademarks listed at zscaler.com/legal/trademarks are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners.

+1 408.533.0288 Zscaler, Inc. (HQ) • 4401 Great America Parkway • Santa Clara, CA 95054 zscaler.com

zscaler™

Act Fast.
Stay Secure.