

Secure Zoom Collaboration with Confidence

Unchecked Zoom Settings Create Security and Compliance Risks

Zoom's dynamic features make it an essential collaboration tool, but also a complex security risk. Unrestricted access, unmanaged chat and file sharing, and misconfigured meeting settings can expose organizations to session hijacking, data leakage, and compliance violations. With hybrid work becoming the norm, Zoom needs proactive, continuous security governance—not just best-effort oversight.

Enforce Zoom Security Policies and Prevent Misuse

AppOmni enables security teams to continuously monitor and enforce secure Zoom configurations across meetings, recordings, and user access settings. It identifies deviations from established security baselines—such as unrestricted join access, anonymous recording links, and inadequate password controls—and provides clear, actionable insights to remediate risks.

With controls to enforce waiting rooms, restrict screen sharing, disable private chat, and block unsanctioned file transfers, organizations can reduce exposure and align Zoom usage with security and compliance requirements, without disrupting collaboration.

Prevent SaaS Breaches

AppOmni continuously monitors Zoom for risks and misconfigurations, helping security teams prevent breaches caused by weak access policies, excessive permissions, and meeting misuse. We close the loop between posture and threat detection, stopping problems before they escalate.



THE BENEFITS

- **Centralize visibility** across Zoom meetings, recordings, and user settings
- **Identify and fix** risky configurations and permissions
- **Align Zoom controls** with leading security frameworks, including NIST, ISO 27001, and CISA's SaaS Misconfiguration Guidance
- **Strengthen collaboration security** without disrupting user experience



KEY USE CASES

- Posture & Permissions Monitoring
- Identity & Access Control
- Meeting Misuse Prevention
- Compliance & Policy Enforcement

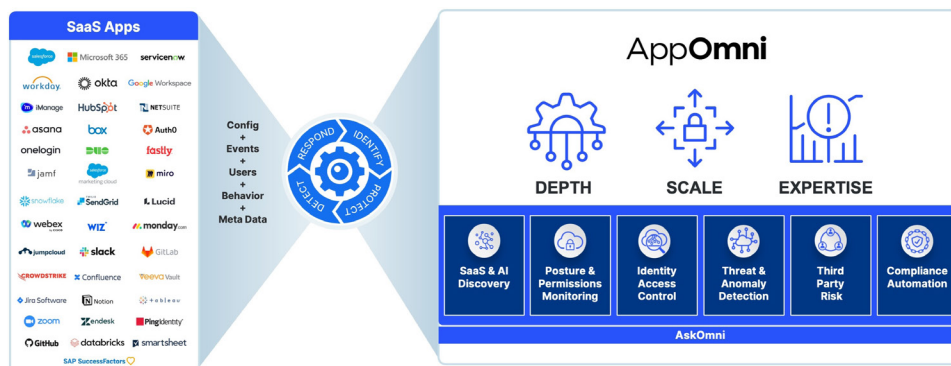
How AppOmni Prevents Zoom Breaches

AppOmni stops Zoom bombing, unauthorized recording access, and impersonation by enforcing least-privilege policies, securing recording links, and surfacing configuration gaps in real time.

Use Case	How To Use It	Security Impact
Posture & Permissions Monitoring	Continuously audit Zoom meeting, recording, and participant settings.	Detect misalignments and enforce secure configurations.
Identity & Access Control	Enforce SSO, lock name changes, and restrict join-before-host.	Stop impersonation and unauthorized access.
Meeting Misuse Prevention	Block private chat, control screen sharing, and limit file transfers.	Eliminate in-meeting threats and session abuse.
Compliance & Policy Enforcement	Enforce passcodes, control recording access, and auto-delete expired data.	Meet compliance mandates, reduce exposure risks.

Achieve Effective SaaS Security for Zoom

Gain visibility, enforce guardrails, and reduce Zoom data exposure with AppOmni.



“AppOmni gives us the visibility we otherwise wouldn't have, allowing us to identify potential risks and address them before they become issues, ensuring our SaaS environment stays secure and aligned with our policies.”

**Information Security
Director, Rightmove**

See AppOmni in Action

Discover how AppOmni secures Zoom with continuous monitoring, policy enforcement, and deep visibility.

[Get a demo](#)

About AppOmni

AppOmni, the leader in SaaS Security, helps customers achieve secure productivity with their applications. Security teams and owners can quickly detect and mitigate threats using unmatched depth of protection, continuous monitoring, and comprehensive visibility. Trusted by the world's largest enterprises, AppOmni specializes in securing diverse SaaS environments. Learn more at appomni.com. © 2025 All Rights Reserved