PORT1

CHECKRED For MSPs

SaaS security beyond Microsoft 365: what MSPs should check

Admins, MFA, sharing, leftover accounts and connected apps: what MSPs should check in client SaaS apps beyond Microsoft 365, and how CheckRed helps.

November 2026 | Jason Makevich, CISSP

Beyond Microsoft 365, MSPs should check five things in every SaaS app a client runs: who holds admin rights, whether multi-factor authentication (MFA) covers every account, what's shared outside the company, which accounts are inactive or left over, and which third-party apps can reach the data. Where an app supports it, confirm audit logging is on too.

Checking settings, access, and connected apps across a client's SaaS apps on a regular cadence is called SaaS security posture management (SSPM).

Why look past Microsoft 365?

MSPs should look past Microsoft 365 because client data also lives in CRM, HR, ticketing, and file-sharing apps, and each of those apps has its own admins, sharing settings, and connected apps. Microsoft 365 is the familiar starting point, and the same responsibility carries over to everything else a client runs.

Settings in those apps change with updates, admin work, and new integrations. That's configuration drift. Drift is normal, and the risk comes from missing it, especially when reviews are done by hand and go stale.

Three questions map the rest of a client's SaaS footprint. Besides email and files, which apps hold customer, financial, or employee data? Who administers each one: someone on staff, a vendor, or no one in particular? Which apps are connected to each other, and what can each connection reach?

What should MSPs check in any SaaS app?

MSPs should check the same five areas in any SaaS app: admins and excess privileges, MFA coverage, external and public sharing, inactive and leftover accounts, and third-party app access. One checklist for every app gives you a consistent review method across a mixed client base.

Admins and excess privileges

Count the admins in each app and confirm each one still needs the role. Look for admins who don't need to be admins and users with more access than they need, then trim access toward least privilege with the client's approval.

MFA coverage

Confirm MFA covers every account, admins first, and find the accounts that sit outside the policy. When an app signs in through an identity provider like Okta, the identity provider handles sign-on and MFA, so a misconfiguration there can expose every app behind it.

External and public sharing

Look for files, records, and pages shared with anyone who has the link, with outside domains, or with guest users who never sign in. Some sharing is on purpose, like website files or a public form, so confirm intent with the client before changing anything.

Inactive and leftover accounts

Find accounts nobody uses and accounts that belong to people who've left. Include non-human identities like service accounts, API keys, and integrations, which are easy to forget when people leave. Building this check into onboarding and offboarding keeps it from piling up again.

Third-party and OAuth app access

Review the apps connected to each SaaS platform and what each one can reach. Under OAuth 2.0, a connected app gets an access token for a specific scope instead of the user's password (RFC 6749), so the scopes someone approved decide what the app can touch. Flag apps with broad access to mail, files, or admin functions and apps nobody recognizes, then remove or restrict them with the client's approval and watch for new ones.

What does CheckRed check in Google Workspace?

For Google Workspace, CheckRed checks super-admin privileges, MFA policies and the accounts outside them, Drive files shared publicly or outside approved domains, Gmail SPF, DKIM, and DMARC, risky OAuth apps, and whether audit logging is turned off. CheckRed's Google Workspace page describes a read-only API integration with no agents. As of November 2026, that page says CheckRed runs over 75 automated checks.

CheckRed flags the issues, and admins make the changes, like enforcing MFA or revoking an app's access. Google Workspace and Google Cloud are separate environments with separate coverage. For tenant-level detail, see monitoring Microsoft 365 and Google Workspace settings across clients. For the email records, see what MSPs should check in DNS, certificates and email authentication.

How does CheckRed help MSPs check SaaS apps across clients?

CheckRed gives an MSP one consistent SaaS review across every client, whatever mix of supported apps each one uses. Its SSPM checks connected SaaS apps for misconfigurations, risky access, inactive users, and third-party app exposure, ranks findings by severity, and gives remediation guidance for each one. CheckRed describes the scanning as agentless.

Here's what CheckRed describes for its featured apps and for identities:

- **Featured apps:** Microsoft 365, Google Workspace, Salesforce, ServiceNow, and Okta.
- **Salesforce:** misconfigurations, access management gaps, risky user activity and data access, granular permissions, and third-party integrations.
- **ServiceNow:** misconfigurations, excessive permissions, and compliance gaps.
- **Okta:** misconfigurations, risky access, and unusual behavior.
- **Identity Posture:** human and non-human identities across cloud and SaaS, flagging excess privileges, unused or expired credentials, missing MFA, and dormant accounts.

As of November 2026, CheckRed lists more than 50 supported SaaS apps, including Slack, Zoom, GitHub, Box, DocuSign, and BambooHR. Check depth varies by app, so confirm a specific check with PORT1 before promising it to a client. The apps CheckRed names are in what CheckRed checks.

Each client sits in its own isolated tenant in one multi-tenant console. Every finding comes with step-by-step guidance, and each alert is tracked from discovery to resolution. That makes SaaS review a repeatable service: connect a client's apps, review one prioritized list instead of going console by console, agree on what's fixed now,

scheduled, or accepted as a known risk, and repeat. For more on building that service, see the MSP's guide to posture monitoring.

PORT1 brings enterprise-grade security and AI solutions to MSPs and MSSPs and sells only through them. Want to see what CheckRed finds across your clients' SaaS apps? Book a CheckRed demo to see how CheckRed for MSPs works across your clients, or Talk to PORT1.

Sources

- RFC 6749: The OAuth 2.0 Authorization Framework, IETF, October 2012. Accessed November 8, 2026.