What CheckRed checks

What CheckRed checks for MSPs: SaaS apps like Microsoft 365 and Google Workspace, cloud accounts, identity, DNS, certificates, email and DDoS readiness.

November 2026 | PORT1

CheckRed checks the settings, access, and exposure in a client's SaaS apps, cloud accounts, identities, DNS and domains, certificates, email authentication, and DDoS protection, and it maps what it finds to compliance frameworks. As of November 2026, CheckRed counts 80+ connectors, more than 6,000 security policies, and 20+ compliance frameworks.

The lists below reflect CheckRed's published pages as of November 2026. Check depth varies by app, so confirm a specific check with PORT1 before you promise it to a client.

Which SaaS apps does CheckRed support?

As of November 2026, CheckRed lists 54 SaaS apps, including Microsoft 365, Google Workspace, Salesforce, ServiceNow, and Okta. PORT1 grouped them below so they're easier to scan.

- **Productivity suites:** Microsoft 365, Google Workspace
- **Identity and access:** Okta, Microsoft Entra ID (Azure AD), JumpCloud, SailPoint
- **Communication:** Slack, Zoom, Microsoft Teams, Cisco Webex, Chorus, Twilio, SendGrid, Calendly, Freshchat
- **Work management:** Asana, Monday.com, Trello, Smartsheet, Wrike, Lucidchart, Jira, Confluence
- **Developer platforms:** GitHub, GitLab, Atlassian Bitbucket
- **IT service and support:** ServiceNow, Freshservice, Freshdesk, Zendesk
- **CRM, sales, and finance:** Salesforce, HubSpot, NetSuite, Gong
- **HR:** BambooHR, Gusto, HiBob, Freshteam
- **Documents and e-signature:** Microsoft SharePoint, Box, Dropbox, DocuSign, Adobe Sign
- **Security and device management:** Microsoft Defender, Microsoft Intune, Zscaler, KnowBe4
- **Data and analytics:** Microsoft Power BI, Snowflake, Splunk, Tableau
- **Web hosting:** WP Engine
- **Learning:** Canvas, Moodle

What do CheckRed's SaaS checks look for?

CheckRed's SaaS security posture management (SSPM) checks look for misconfigurations, excessive permissions, insecure data handling, improper access controls, inactive users, and third-party app access. Alerts are ranked by severity, and each finding comes with remediation guidance.

As of November 2026, CheckRed's Google Workspace page says it runs over 75 automated checks, covering super-admin privileges, MFA, Drive sharing, Gmail SPF, DKIM and DMARC, risky OAuth apps, and audit logging. For Microsoft 365, CheckRed describes checks for misconfigured security settings, excessive privileges, risky third-party access, configuration drift, and unauthorized changes.

See how MSPs monitor Microsoft 365 and Google Workspace across clients, and what to look for in SaaS apps beyond Microsoft 365.

Which clouds does CheckRed cover?

CheckRed covers AWS, Microsoft Azure, Google Cloud, and Akamai Linode, including multi-cloud and hybrid setups. Cloud security posture management (CSPM) checks those accounts for misconfigurations, excessive permissions, and unauthorized access, and CheckRed describes the scanning as agentless.

- **Cloud infrastructure entitlement management (CIEM):** excessive, unused, and cross-account permissions, insecure service accounts, MFA violations, and exposed credentials.
- **Cloud workload protection platform (CWPP):** visibility into workloads, user accounts, and runtime environments, with detection of anomalies, unpatched software, and vulnerable software dependencies.
- **Kubernetes security posture management (KSPM):** RBAC settings, pod security, network policies, and unencrypted traffic.

Azure resources fall under cloud posture, separate from a Microsoft 365 tenant, and Google Cloud is separate from Google Workspace.

What identity risks does CheckRed find?

CheckRed finds identity risks like excess privileges, dormant accounts, missing MFA, and unused or expired credentials, across both human and non-human identities. Its identity threat detection and response (ITDR) module also watches SaaS sign-in and account activity for identity-based threats.

- **Identity Posture:** human and non-human identities, excess privileges, dormant accounts, MFA gaps, and unused or expired credentials.
- **ITDR:** privilege escalation, anomalous behavior, abnormal policy changes, session hijacking, brute force attempts, unusual access to sensitive files, and dormant account reactivation.
- **Active Directory posture management (ADPM):** risky configurations, excessive permissions, and privilege escalation.

What does CheckRed check in DNS and domains?

CheckRed's DNS posture management (DNSPM) checks DNS records, zones, and subdomains across providers for misconfigurations and takeover risks, tracks who changed what, and watches for lookalike domains.

- **Providers:** Amazon Route 53, Azure DNS, Google Cloud DNS, Cloudflare, GoDaddy, Akamai Edge DNS, Infoblox, legacy on-premises DNS, and more.
- **Risks:** sensitive data in TXT records, dangling DNS, name collisions, reflection and amplification exposure, DNS tunneling, fast flux, and subdomain takeover.
- **Also:** drift (who changed what), and typosquatting and lookalike domains.

What does CheckRed check for certificates and email?

CheckRed flags expiring, rogue, or misconfigured certificates, weak keys, and deprecated algorithms, shows which certificates rely on quantum-vulnerable algorithms, and checks email authentication across a client's domains.

- **Certificate Posture Management (Certificate PM):** expiring, rogue, or misconfigured certificates, weak keys, deprecated algorithms, and certificates from unsanctioned authorities.
- **Post-Quantum Cryptography (PQC) Monitoring:** which certificates rely on quantum-vulnerable algorithms.
- **Email Posture Management (Email PM):** SPF, DKIM and DMARC, plus BIMI, across a client's domains, along with unauthorized senders and drift.

For what to look at first in each area, see what MSPs should check in client DNS, certificates and email authentication.

How does CheckRed check DDoS readiness?

CheckRed's DDoS posture management (DDoSPM) checks whether a client's DDoS protection will engage, using outside-in readiness checks that each come back pass, warning, or fail.

- **Providers:** Akamai Prolexic, AWS Shield, Azure DDoS Protection, Cloudflare, F5, and Netscout Arbor.
- **Readiness checks:** IP prefix announcements, prefix configuration with the provider, routing through the DDoS network, origin ASN accuracy, and ROA validity.

Which compliance frameworks does CheckRed name?

As of November 2026, CheckRed says it maps findings to 20+ compliance frameworks, and its pages name SOC 2, ISO 27001, NIST, CIS, PCI DSS, HIPAA, GDPR, DORA, NIS2, SOX, and FedRAMP, plus mapping to MITRE ATT&CK.

Framework mapping means CheckRed maps its findings to a framework's controls. It isn't a certification of CheckRed or of your clients. See how MSPs offer continuous compliance to clients.

Which tools does CheckRed send findings to?

CheckRed sends alerts and tickets to Slack, Jira, Amazon SNS, PagerDuty, and Splunk, and it describes an API for SIEM, SOAR, GRC, and XDR platforms.

All of this runs from one multi-tenant console in CheckRed for MSPs, with each client in its own tenant.

Download: What CheckRed checks ›

See it across your own clients. Book a CheckRed demo or Talk to PORT1.