PORT1

CHECKRED For MSPs

The MSP's guide to posture monitoring and continuous compliance

A free guide for MSPs on building a posture monitoring and continuous compliance service: coverage, onboarding, a monthly routine, QBRs and evidence.

November 2026 | Jason Makevich, CISSP

PORT1 brings enterprise-grade security and AI solutions to MSPs and MSSPs and sells only through them.

port1.ai/learn/downloads/posture-monitoring-continuous-compliance-guide/

MSPs build a posture monitoring and continuous compliance service by checking each client's SaaS, cloud, identity, and DNS settings continuously, turning findings into business decisions, fixing the highest-risk issues first, and reporting progress and evidence at every QBR. This guide walks through each part, with CheckRed as the platform that runs it.

Why should MSPs monitor client security posture?

MSPs should monitor client security posture because much of a client's risk comes from settings and access: files shared publicly, admins without MFA, apps with broad access, storage open to the internet, and DNS records pointing at resources that no longer exist. These problems are common and easy to miss, and they're often the first step in a breach or an audit finding. A posture finding can point to a weakness even when no attack is happening.

Settings also drift. Normal admin work, new integrations, changed permissions, and vendor changes move settings away from where they were, which is why one-time reviews go stale. That's configuration drift, and audits only capture a moment while the environment keeps changing after the auditor leaves.

Microsoft 365 is the familiar starting point for most MSPs. The rest of a client's posture is usually spread across other SaaS apps, cloud accounts, DNS hosts, registrars, and certificate authorities, often with no one watching it continuously.

What does posture management cover?

Security posture management covers the settings, permissions, exposures, and controls across a client's SaaS apps, cloud, identities, DNS, and certificates, checked continuously from one platform with one way to prioritize, fix, and report on what it finds.

The terms, in plain English

- **Security posture:** the condition of the settings, permissions, exposures, and controls in an environment. A misconfiguration is a setting that leaves something more exposed than intended.
- **Configuration drift:** a change away from an intended or previously accepted setting. Drift is normal, and the risk comes from not noticing it.
- **Continuous monitoring:** checking environments repeatedly, on an ongoing basis, instead of relying on a one-time assessment. Timing depends on each connector and platform.
- **Risk-based prioritization:** ranking findings by severity, exposure, and business impact, so the most important issues get fixed first.
- **Guided remediation:** step-by-step instructions to fix each finding, with context about the affected asset and why it's risky.

- **Compliance mapping:** linking technical findings to the requirements in frameworks like CIS, NIST, ISO 27001, PCI DSS, HIPAA, or SOC 2. It shows where technical controls stand. Organizational requirements, like policies, training, and contracts, need their own processes.

The areas to cover

- **SaaS:** Microsoft 365, Google Workspace, Salesforce, ServiceNow, Okta, and other supported SaaS apps, covered by SaaS security posture management (SSPM).
- **Cloud:** AWS, Microsoft Azure, Google Cloud, and Akamai Linode accounts, covered by cloud security posture management (CSPM), plus cloud permissions, workloads, and Kubernetes clusters.
- **Identity:** human and non-human identities, excess privileges, MFA gaps, dormant accounts, and Active Directory.
- **DNS and certificates:** records, zones, takeover risks, lookalike domains, and certificate health, covered by DNS posture management (DNSPM).
- **Email authentication:** SPF, DKIM and DMARC, plus BIMI, across a client's domains.
- **DDoS readiness:** whether a client's DDoS protection will actually engage.

How do you turn findings into business decisions?

MSPs turn posture findings into business decisions by framing each one with four questions: what could this disrupt, what would it cost, what should be done first, and what risk is accepted by waiting.

Security usually gets explained too technically. The four questions keep the conversation on the client's business. CheckRed's risk-based prioritization gives the starting order, and the MSP adds the business context: which systems hold sensitive data, whether the client is regulated, and what the client has decided to accept. Explain without fearmongering. The goal is a clear decision.

Four examples

- **A file shared publicly.** A Google Workspace Drive file holding customer data is shared with anyone who has the link, which could put that data in the wrong hands. Confirm whether the share is intentional, then restrict it or record it as an accepted risk.
- **An admin without MFA.** One stolen password could hand an attacker admin control. CheckRed's identity posture flags missing MFA, and its Google Workspace checks cover accounts outside MFA policies. Bringing the account under MFA is usually quick, so it belongs near the top of the list.
- **A dangling DNS record.** A record still points at a retired hosted app or marketing site, and someone could claim that resource and take over the subdomain. Removing or updating the record closes the gap.

- **An expiring certificate.** A certificate nobody tracked is about to expire, which can take a site or service offline. Renewing it, and finding the other certificates no one tracked, prevents the outage.

The dangling record is a subdomain takeover risk. More on finding these is in what MSPs should check in client DNS, certificates and email authentication.

What to record when a client waits

Make deferrals explicit, and record accepted risks as exceptions instead of letting them sit as open findings.

What services can you build on posture monitoring?

Common services MSPs build on posture monitoring include ongoing posture monitoring, compliance readiness, DNS and certificate governance, assessments for new clients, remediation projects, co-managed security, and third-party app reviews.

- **Posture monitoring:** ongoing checks across the client's SaaS, cloud, identity, and DNS, with prioritized findings.
- **Compliance readiness:** keeping the technical controls behind the client's frameworks current, with evidence ready when an auditor or a customer questionnaire asks.
- **DNS and certificate governance:** keeping DNS records, domains, and certificates clean and owned.
- **Assessments for new clients:** a baseline that shows what you're inheriting, so you can agree on priorities early.
- **Remediation projects:** scoped work, like a permissions cleanup or a configuration overhaul, when it's outside the client's existing agreement and the client approves it.
- **Co-managed security:** the MSP handles oversight, priorities, and reporting, and the client's IT team makes some of the changes.
- **Third-party app reviews:** a regular look at the apps connected to Microsoft 365, Google Workspace, and other SaaS platforms, what each can access, and which to remove or restrict with the client's approval.

You decide how to package your services. Agree on scope, owners, and approvals before changing anything, since a finding on its own isn't a project or permission to act.

Agree on ownership early

Before you change anything, agree with the client on what the MSP fixes, what the client's team fixes, and what gets accepted as an exception. In a co-managed setup, also agree on who reviews, implements, approves, and reports.

How do you onboard a client?

MSPs onboard each client to CheckRed with the same sequence: create the client's tenant, connect the core SaaS first, add the rest, choose frameworks, run the baseline, set alert routing, and agree on remediation scope.

Before you start

Collect these before the first connection. The MSP connects each environment with the client's authorization.

- Who at the client authorizes each connection, and who makes business decisions about findings
- Their SaaS apps, starting with Microsoft 365 or Google Workspace
- Their cloud accounts
- Their domains and DNS providers
- Their identity systems, including Active Directory if they run it
- The frameworks and security questionnaires they answer to

Exact permissions vary by connector, so confirm with PORT1 what access each connection needs.

The standard sequence

1. **Create the client's tenant** in the MSP console.
2. **Connect the core SaaS first,** usually Microsoft 365 or Google Workspace. That's often where small and mid-sized clients carry the most risk, and it gives a quick first result.
3. **Add the rest:** cloud accounts, identity providers, DNS providers, and the other SaaS apps the client uses.
4. **Choose the client's frameworks.**
5. **Run the baseline** and review it internally before you share it.
6. **Set alert routing,** for example a Slack channel or Jira project for the client, and PagerDuty for critical findings. Confirm per-client routing options during setup.
7. **Agree on remediation scope** with the client.

CheckRed says a quick SaaS posture scan produces a report with remediation guidance in minutes. The client conversations take longer than the connections. For the details of the first step, see Microsoft 365 and Google Workspace posture for MSPs.

How do you run the service month to month?

MSPs run a posture monitoring service month to month by triaging critical and high findings across all clients first, working guided fixes through tickets, recording exceptions with a reason and a review date, and watching for new drift.

Triage across clients

With every client in one console and one consistent ranking, start with the critical and high findings across all tenants, then work down. Findings are ranked by severity and potential impact, and CheckRed maps its rules to MITRE ATT&CK tactics and techniques.

Fix and track

Each finding comes with step-by-step guidance, and each alert is tracked from discovery to resolution. Send findings to Jira so each one has an owner, and route alerts to Slack, PagerDuty, or Amazon SNS. Many fixes need a business decision first, like whether an external share is intentional, so the client decides and the MSP makes the change.

Exceptions and compensating controls

Some findings can't be fixed right away, because a legacy app needs an older setting or a business process needs broader access. Record those as exceptions with a reason, an owner, and a review date, or document the compensating control that meets the requirement's intent. Exceptions are the client's decision, so the MSP documents each one and reviews it at the next QBR. CheckRed's DNS posture management page lists exception management workflows that use compensating controls.

Watch for drift

Ongoing monitoring catches new drift between reviews, like new admins, new third-party apps, or certificates nearing expiry.

What do you show at QBRs?

At a QBR, MSPs show posture and compliance status against last quarter, the critical and high findings fixed, in progress, or accepted as exceptions, new risks since the last review, and the next recommended projects, framed as business risk.

Give leadership an executive summary and the client's IT contact the detailed findings. The QBR shows ongoing value in a service that's otherwise invisible when it's working, and it surfaces the next project.

How does continuous compliance fit the service?

Continuous compliance fits the service by keeping the technical controls in connected systems checked continuously and mapped to the client's frameworks, with evidence collected as you go.

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, and NIS2. Compliance readiness fits clients facing their first SOC 2, healthcare and financial clients, and clients whose own customers send security questionnaires.

Policies, procedures, training, vendor contracts, HR, physical security, and controls in systems CheckRed isn't connected to still need their own processes. CheckRed keeps the technical side of compliance current and provides the evidence, and the auditor still does the audit. More detail is on continuous compliance for MSPs.

How does CheckRed for MSPs fit?

CheckRed for MSPs runs all of this from one multi-tenant platform, with SaaS, cloud, identity, DNS, and compliance posture together and each client in its own isolated tenant.

PORT1 brings enterprise-grade security and AI solutions to MSPs and MSSPs and sells only through them. Partners get PORTER, PORT1's partner platform.

For the apps, clouds, providers, and frameworks CheckRed names, see what CheckRed checks, and for the rest of a client's apps, see what MSPs should check in SaaS apps beyond Microsoft 365.

Build the service on one platform. Book a CheckRed demo or Talk to PORT1.