

# Posture Management

See every misconfiguration. Fix what matters.

Ensure compliance with regulatory standards and mitigate the risk of misconfiguration, protecting your sensitive data from unauthorised access. CSPM and SSPM controls help identify and remediate risks in cloud infrastructure and cloud-based SaaS applications.

## THE PROBLEM

### Complex cloud. Silent misconfiguration.

The increasing complexity and interconnected nature of cloud environments make them particularly vulnerable to security misconfigurations. Improperly configured SaaS and IaaS policies are significant contributors to data breaches.



#### CLOUD INFRASTRUCTURE CSPM

- Automated security assessments and misconfiguration detection across cloud infrastructure.
- API-based connectors to major IaaS platforms such as AWS, Azure and GCP.



#### SAAS APPLICATIONS SSPM

- Extends TrustLayer's award-winning CASB technology via APIs to give visibility and control of security configuration across SaaS apps such as Salesforce and M365.
- Connect your cloud infrastructure and SaaS applications via API and continuously monitor their configurations for potential errors and settings that may put you at risk of data breach.



#### ONE MODULE Unified posture

- Combining CSPM and SSPM in a single module lets you focus on identifying and mitigating risk across all your cloud services.
- Integrating CSPM and SSPM with TrustLayer's CASB technology delivers a unified security posture across the entire digital ecosystem.

Automating the detection of misconfigurations to **prevent unauthorised access**, and to evidence compliance.

## SIMPLE CONFIGURATION

### Connect an API, scan in minutes.

New services are integrated by simply creating an API connection. Most IaaS and SaaS products enable this through creation of an API Key and Secret, which you copy and paste into the Compliance dashboard. Once set up, the system scans the configuration within minutes and displays a detailed report. The dashboard highlights all unconfigured or misconfigured controls with an associated risk level; if a setting is something you don't use, or you are comfortable with the risk, mark it as deactivated so subsequent scans don't alert you. Audit-ready against:

ISO 27001

NIS2

Cyber Essentials+

PCI DSS

NIST CSF

## CAPABILITY

### Identify. Remediate. Evidence.

Continuous configuration checks across cloud infrastructure and SaaS, prioritised by what actually matters.



#### Identify

- ✓ Instant visibility of non-compliant settings and Indicators of Risk direct you to the critical items to address, no guesswork
- ✓ Identify and prioritise risk based on potential impact
- ✓ Identify and mitigate excessive spread of unnecessary permissions



#### Remediate

- ✓ Direct links to remediation guide you towards where and how to implement corrective action
- ✓ Every risk identified can be inspected: what the control is, why it failed, and what to do about it
- ✓ For active alerts, simply configure the control from the dashboard



#### Evidence

- ✓ Assistance with audit preparation and documentation for compliance against major governance frameworks
- ✓ Run on-demand scans and download the reports for audit compliance and documentation
- ✓ Interactive activity report gives a view of top risks and highlights critical vulnerabilities

5

platforms connected via API

Minutes

to first scan after  
connecting

5

compliance frameworks  
mapped

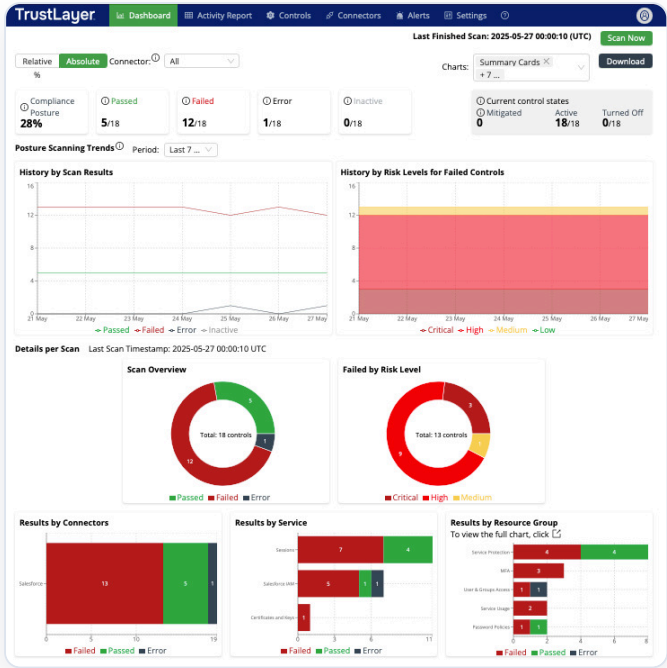
On-  
demand

rescan and export any time

THE DASHBOARD

Posture at a glance, drill-down on demand.

Once you have connected the service’s API, TrustLayer carries out regular scans of its configuration.



Compliance posture, scan history and failures by risk level across every connector.

ACTIVITY REPORT

Every control, every scan.

The activity report gives an interactive view of the top risks and highlights critical vulnerabilities, mapped to the compliance standards each control supports.

TrustLayer

Dashboard

Activity Report

Controls

Connectors

Alerts

Settings

Last Finished Scan: 2025-06-02 00:00:13 (UTC)

Scan Now

Posture Management Activity

Columns: 

Category X + 4 ...

 Timespan: 

Last scan

Show Filters

Download

| Timestamp UTC       | Status | Risk Level | Control                                                            | Connector  | Service        | Compliance Standards                                    | Category                | Resource Group       | Actions                  |
|---------------------|--------|------------|--------------------------------------------------------------------|------------|----------------|---------------------------------------------------------|-------------------------|----------------------|--------------------------|
| 2025-06-02 00:01:19 | Failed | High       | Inactive users are deactivated.                                    | Salesforce | Salesforce IAM | Cyber Essentials<br>ISO 27001 PCI DSS<br>NIST CSF NIS 2 | User & Group Management | User & Groups Access | <div>Q</div> <div></div> |
| 2025-06-02 00:01:23 | Passed | High       | Cross-Site Request Forgery protection on GET requests is enabled.  | Salesforce | Sessions       | Cyber Essentials<br>ISO 27001 PCI DSS<br>NIST CSF NIS 2 | Service Management      | Service Protection   | <div>Q</div> <div></div> |
| 2025-06-02 00:01:24 | Passed | High       | Cross-Site Request Forgery protection on POST requests is enabled. | Salesforce | Sessions       | Cyber Essentials<br>ISO 27001 PCI DSS<br>NIST CSF NIS 2 | Service Management      | Service Protection   | <div>Q</div> <div></div> |
| 2025-06-02 00:01:25 | Passed | High       | Clickjack protection is enabled for setup pages.                   | Salesforce | Sessions       | Cyber Essentials<br>ISO 27001 PCI DSS<br>NIST CSF NIS 2 | Service Management      | Service Protection   | <div>Q</div> <div></div> |
| 2025-06-02 00:01:26 | Passed | High       | Clickjack protection is enabled for non-setup pages.               | Salesforce | Sessions       | Cyber Essentials<br>ISO 27001 PCI DSS<br>NIST CSF NIS 2 | Service Management      | Service Protection   | <div>Q</div> <div></div> |
| 2025-06-02 00:01:26 | Failed | Medium     | Session timeout is set for the Salesforce account.                 | Salesforce | Sessions       | Cyber Essentials<br>ISO 27001 PCI DSS<br>NIST CSF NIS 2 | Service Management      | Service Protection   | <div>Q</div> <div></div> |

Failed and passed controls by connector, service, category and compliance standard.

## KEY FEATURES

# The detail.

|                       |                                                                                                                                                                                          |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Services Supported*   | CSPM: AWS, Azure, GCP. SSPM: Microsoft 365, Salesforce.                                                                                                                                  |
| Automated Assessment  | Automated security assessments and misconfiguration detection of cloud infrastructure, with continuous monitoring of configuration for errors and risk settings.                         |
| Indicators of Risk    | Instant visibility of non-compliant settings and Indicators of Risk direct you to the critical items to address, with no guesswork.                                                      |
| Guided Remediation    | Direct links to remediation guide you towards where and how to implement corrective action. Every risk can be inspected to explain what the control is, why it failed and how to fix it. |
| Permission Sprawl     | Identify and mitigate excessive spread of unnecessary permissions.                                                                                                                       |
| Risk Prioritisation   | Identify and prioritise risk based on potential impact, so the most material items surface first.                                                                                        |
| Compliance Frameworks | Assistance with audit preparation and documentation for compliance against major governance frameworks such as ISO 27001, NIS2 and Cyber Essentials+.                                    |
| Control Deactivation  | Mark controls you don't use, or accept the risk on, as deactivated so subsequent scans don't alert you.                                                                                  |
| On-demand Scanning    | Run on-demand scans after making a change, and download the reports for audit compliance and documentation.                                                                              |
| Licensing             | Per API Connector.                                                                                                                                                                       |
| Support               | All connectors documented with Quickstart Guides: <a href="https://help.clouduss.com/posture-management-cspm-sspm">help.clouduss.com/posture-management-cspm-sspm</a>                    |

\* Additional services added by request. Service API must support writing configuration rules.

### PART OF THE TRUSTLAYER PLATFORM

Posture Management is the Posture layer. Eight solutions, four layers, one platform.



#### Browse

Web

CASB

AI Exposure



#### Posture

CSPM

SSPM



#### Mail

Email

Archiving



#### Users

SAT