

TrustLayer One

One platform. Every layer.

TrustLayer One unifies web security, cloud application control, posture management, user authentication, security awareness training and email security in a single cloud platform and portal. Multi-tenant, multi-tier administration lets a parent account manage child tenants centrally.

THE PLATFORM

Four layers. Eight solutions. One portal.

A single portal across core security services for enterprises and MSPs alike, bringing the four layers together for central configuration and reporting.



Browse

Web

Stop web threats and filter distractions with a proxy-less agent or gateway.

CASB

Discover, analyse and control user interaction with cloud applications.

AI Exposure

Discover the AI tools your people use, score their risk and control what they can do.



Posture

CSPM

Continuous misconfiguration checks across AWS, Azure and GCP.

SSPM

Posture management across SaaS apps like Microsoft 365 and Salesforce.



Mail

Email

Stop known, unknown and emerging email threats before the inbox.

Archiving

Compliant, searchable storage for eDiscovery and continuity.



Users

SAT

Reduce human risk with engaging, automated security training.

WHY ONE PLATFORM

Move away from point products in silos.

Security teams configure policy once, monitor activity in one place and manage core defences together, instead of running separate point products in silos. Users work from any device or location, while IT keeps the visibility and control to protect everyone.

PLATFORM CAPABILITIES

Built for enterprises and MSPs.

One console, many tenants, with the residency, branding and integration controls that larger and managed environments need.



Cloud & residency

- ✓ 100% cloud-based, delivered from data centres in the US, UK and mainland Europe
- ✓ Specify data residency by region per account, selected at the time of provisioning
- ✓ Customer data segregated using separate database schemas, each tenant with a unique encryption key, all access over HTTPS



Multi-tenant & multi-tier

- ✓ Ideally suited to organisations of any size as well as MSPs
- ✓ Create 'child accounts' for multi-national organisations, multiple brands or reseller end users
- ✓ Each account has its own set of policies for local legislative and regulatory compliance



Branding & API

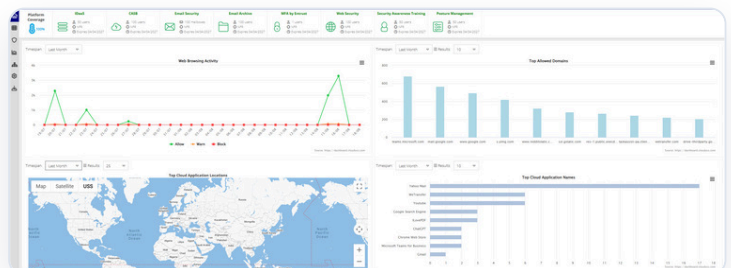
- ✓ White label the portal by changing logos and interface colour per account
- ✓ A REST API lets you embed any element of the TrustLayer One interface in your own applications
- ✓ Different email addresses can receive system, maintenance, unblock and log archive notifications

DASHBOARD & REPORTING

A home dashboard for every service.

Each administrator has their own Home Dashboard with charts and widgets specific to the services licensed, with multiple standard reports included for each service in the Analytics section.

Detailed analysis is available by time, user, device (hostname and MAC address), URL and web category, cloud application class, name and action, keyword, policy name, risk level, email direction, delivery status and outcome.



Rich visualisation across every service, with per-service widgets and global activity.

ADMINISTRATION

One hundred access controls, unlimited roles.

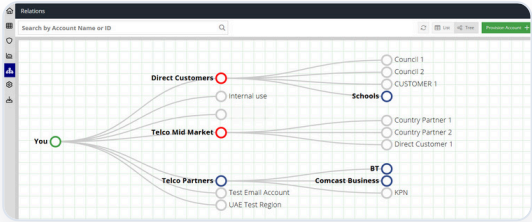
Split the admin function to match how your organisation, or your customers' organisations, actually work.

Ease of administration. Create unlimited admin roles based on over 100 access controls.

Delegated & RBAC. Split the admin function to match organisational requirements. Enterprises delegate admin to local or regional teams; MSPs reflect responsibilities within SLAs or use role based access control.

Parent assumes admin. Parent accounts can assume the administrator role for a child account to manage settings, policies and rules across all services, or troubleshoot issues, on behalf of business units or customers.

Comprehensive audit. A comprehensive audit trail of all administrator activity.



Multi-tier account relations: manage in-country businesses or reseller end users.

IDENTITY INTEGRATED

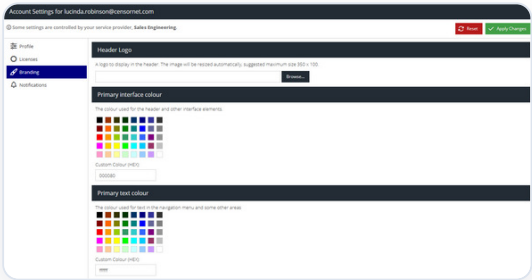
One shared identity store, AD-synced.

Single identity store. One identity store shared across Email Security, Web Security, CASB, AI Exposure, Posture Management and SAT.

AD Local Sync. A locally installed AD Connector Service (agent) pushes objects to the TrustLayer Cloud, with no firewall rule changes required.

AD Cloud Sync. Uses an LDAP or LDAPS connection to pull objects. Both methods require a read-only service account in AD.

No AD? No problem. For organisations without AD, local usernames are still captured where possible.



White label per account: logo and interface colour.

PARTNER TOOLS & REPORTING

Manage, monitor, evidence.

Partner Tools

Self-service tools for IT teams or MSPs: new account provisioning, service and licence management, the ability to suspend or delete an account, search, and reporting on service usage and licence status. Choose whether Partner Tools are visible within an account so a regional HQ can manage in-country businesses, or a reseller their end users.

Detailed reporting

Analyse by time, user, device (hostname and MAC address), URL and web category, cloud application class, name and action, keyword, policy name, risk level, email direction, delivery status and outcome.

Log retention

Logs are auto-archived per service: 90 days for Email and Web Security, and one year for Cloud Application Security. Archives can be downloaded on-demand in CSV format.

Scheduled & alerting

Link reports to schedules to send via email as CSV or PDF attachment, also used for email alerts.

One stack, under control.



Go direct

No proxies. No slowdowns. Just protection at full speed.



Get layered

Start with what you need, and scale as your business evolves.



Deploy fast

Live in minutes, not months, with prebuilt templates and zero fuss.



Stay quiet

Become invisible to users, but invaluable to your security team.

TRUSTLAYER LTD

4.2 Belvedere House, Basing View, Basingstoke,
Hampshire RG21 4HG

Phone: +44 (0) 845 230 9590

trustlayer.co.uk

WORKS TOGETHER

TrustLayer One gives you mail, web, user and SaaS security that actually works together. No patchwork, no platform fatigue, just what you need to protect your business and keep your stack under control.