

Web Security

Filter the web without proxying the web.

Web Security from TrustLayer provides protection from harmful, offensive or inappropriate content, as well as managing time spent on websites that can have a significant impact on productivity.

DEPLOYMENT

Agent, gateway or ICAP. No proxy required.

Deployed using agents or local gateways, or a combination of both, to meet the needs of organisations of all sizes. Flexible deployment options simplify implementation, accelerating time to value.



ENDPOINT-ENFORCED

Agent

- Agents for Windows and MacOS enforce policies at the endpoint. Tamper-proof and easy to deploy using an install wizard or via Intune/Group Policy.
- Using agents on endpoints, Web Security offers a proxy-less approach which significantly reduces latency, preserves the user's real IP address and maintains user privacy by allowing the browser direct communication with the destination web server.



NETWORK-WIDE

Gateway

- TrustLayer Cloud Gateway installs on a lightweight virtual machine or physical server in under 30 minutes to extend security policies to the entire network. Also available in the cloud.
- Ideal for sites with populations of fixed desktops, such as call centres. Mobile device coverage by routing traffic via VPN through the TrustLayer Cloud or on-prem Gateway.



NO TRAFFIC PROXYING

ICAP service

- Built on the lightweight ICAP protocol with servers deployed in multiple locations worldwide. More sophisticated than DNS-based solutions, with significantly less overhead than cloud-based proxies.
- Only http request metadata is sent to the TrustLayer Cloud and compared against policy, eliminating the need to proxy all traffic with no user-perceived impact.

Users get a fast, unobtrusive experience on any device, while IT keep **visibility and control** over web browsing.

POLICY ENGINE

Block, allow, or allow and track.

A sophisticated policy engine enables rules that block, allow, or allow and track web browsing activity. Rules can be user, device or time based and applied to web content based on Web Category, custom URL Category or keyword match. Conditions can be combined using AND OR logic for power and flexibility:

User

Device

Time

Web Category

URL Category

Keyword

Time Quota

AND/OR logic

CLOUD APP CONTROL

Filter. Protect. Control.

Multiple security layers at the gateway offer comprehensive protection from web-borne malware and other threats.



Filter

- ✓ Manage over 550 categories of web content and billions of URLs
- ✓ New URLs analysed in real-time for malware and automatically categorised using ML techniques
- ✓ Sub-categories are grouped for ease of administration and granularity of control



Protect

- ✓ Multiple security layers combining real-time traffic inspection, URL reputation analysis and heuristics
- ✓ Complete browser protection, including deep inspection of SSL (https) encrypted traffic
- ✓ Prevent access to anonymous proxy sites



Control

- ✓ Highly granular policies set on pre-defined categories or custom attributes, applied to directory user/device groups
- ✓ Time Quotas limit time spent on shopping sites to one hour per day, for example
- ✓ BYOD and Guest device support with optional Captive Portal for zero-touch filtering

550+

categories of web content

Billions

of URLs classified

30 min

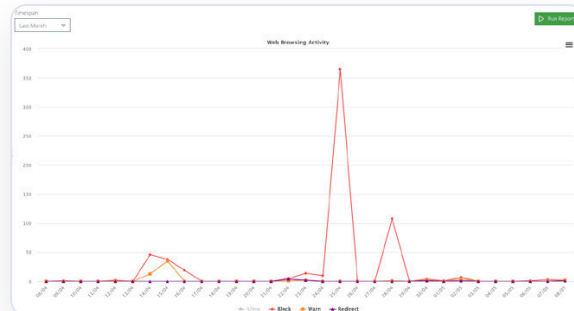
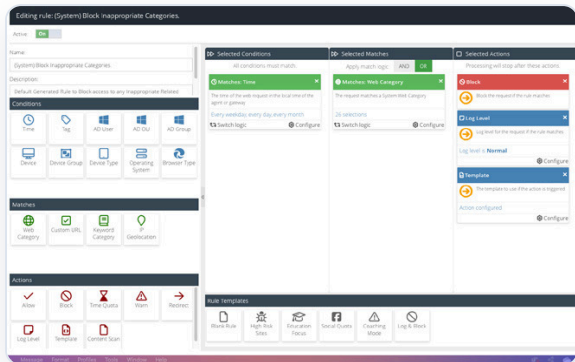
gateway deployment

Real-time

unknown URL analysis

DEPLOYMENT

Deploy your way.



Browsing activity by allow, block and redirect over time.

Build rules from categories, conditions and matches, with AND/OR logic.

Gateway

TrustLayer Cloud Gateway can be installed on a lightweight Virtual Machine or physical server in under 30 minutes to extend security policies to the entire network. Also available in the cloud.

Agents

Agents for Windows and MacOS enforce policies at the endpoint. Tamper-proof and easy to deploy using an install wizard or via Intune/Group Policy.

Deployment Modes

Agent software, direct gateway (set by GPO, WPAD or manually), or gateway mode for guest, personal (BYOD) and non-domain devices.

WPAD Support

Automatic creation of Web Proxy Automatic Discovery file based on network configuration.

WCCPv2 Support

Supports Web Cache Communication Protocol v2 for transparent traffic redirection from Cisco routers/switches.

Gateway Modes

TrustLayer Cloud Gateway can operate in Explicit or Transparent mode.

KEY FEATURES

What you get out of the box.



ICAP

Globally distributed ICAP servers compare web request metadata against central policy rules, removing the need to proxy traffic and delivering speed, reliability and scalability without complexity.



Realtime Anti-malware scanning

Incorporates multiple security layers, each using a powerful and highly effective combination of tools and techniques to detect sophisticated malware in its tracks.



URL Filtering

Over 550 categories of web content classification covering billions of web pages in multiple languages, constantly updated for accuracy and efficacy. Sub-categories are grouped for ease of administration and granularity of control.



Automatic Unknown URL Classification

New URLs are analysed in realtime to ensure only acceptable content is accessed.



HTTPS Inspection

Deep inspection allows SSL encrypted content to be scanned for malware, with the ability to disable SSL inspection for internal/trusted sites. Option to use Server Name ID (SNI) within the TLS protocol to determine destination domain without certificate management issues.



Safe Search

Enforce Safe Search mode on popular search engines including Google, Yahoo, Bing and YouTube.



BYOD, Guest Devices & Overrides

Safely allow BYOD and guest devices internet access via the built-in Captive Portal, with existing users logging in from personal devices using valid Azure AD credentials. Create lists of categories, domains and URLs that bypass the filters, and prevent access to anonymous proxy sites.

MANAGEMENT

Central control

Policy Engine	Sophisticated policy engine including AzureAD attributes, IP, MAC address, device type, custom tags, and differential actions.
Time Schedule	Policies can be applied on a rolling 7-day schedule to customise access restrictions.
Authentication & Sync	AD Kerberos, SSO, Captive Portal and RADIUS accounting. AD sync service ensures changes are replicated seamlessly.
Web Portal	Fully integrated with TrustLayer's other modules, the CloudUSS dashboard offers a single pane of glass for management and reporting.
Delegated Admin	Full Role-Based Access Control (RBAC) enables a range of access profiles and control/visibility permissions.
Custom Notifications	Customise and brand notification and block pages with logo, html text, and other useful user information.

Evidence on demand

Real-time Visibility	Multiple charts and tables give instant insight. Query logs in realtime by numerous filter attributes to see exactly which users are accessing which sites.
Curated Reports	Build reports from available fields and criteria and export via PDF. Search audit reports by time, user, device, Web Category, URL Category, domain, keyword and outcome (allow/block/warn/redirect).
Scheduling & Alerting	Link curated reports to a delivery schedule so analytics reach email inboxes on a regular cadence.
Interactive Reports	Fully interactive charts and tables take admins from high-level trends to forensic detail in a few clicks for prompt incident response.
Log Retention	Web Security log data is archived automatically after 30 days. Log Streaming can send logs to a 3rd party SIEM tool in realtime.

PART OF THE TRUSTLAYER PLATFORM

Web Security is part of the Browse layer. Eight solutions, four layers, one platform.



Browse

Web

CASB

AI Exposure



Posture

CSPM

SSPM



Mail

Email

Archiving



Users

SAT