

# TrustLayer Web Security

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.

Multiple security layers at the gateway offer comprehensive protection from web-borne malware and other threats using a powerful combination of real time traffic inspection, URL reputation analysis and heuristics.

Web Security is fully integrated with the TrustLayer Platform that also includes Email Security, Cloud Application Security and Multi-Factor Authentication. The TrustLayer Platform provides a single web interface for central policy configuration and management, as well as data visualization and reporting.

Web Security is deployed using agents or local gateways, or a combination of both to meet the needs of organizations of all sizes. Flexible deployment options simplify implementation, accelerating time to value.

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

Web Security provides a single pane of glass to analyze and manage web browsing activity across multiple networks and devices, whether users are on the corporate network or working remotely.

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.

## WEB SECURITY

- Manage over 550 categories of web content and billions of URLs.
- Protection against malware and Web threats using multiple security layers and a powerful combination of technologies.
- Complete browser protection, including deep inspection of SSL (https) encrypted traffic.
- New URL's analysed in real-time for malware and automatically categorised using ML techniques.
- BYOD and Guest device support with optional Captive Portal for zero-touch filtering.
- Highly granular policies can be set based on pre-defined categories or custom attributes, and then applied to directory user/device groups.
- Flexible deployment options via agent supporting Windows, MacOS, Chromebook, and gateway for mobile devices.
- Additional mobile device coverage by routing traffic (via VPN) through the TrustLayer Cloud or on-prem Gateway.
- Cloud Application Control (CASB) can be enabled instantly without the need for any additional hardware, software, or configuration changes providing visibility and management to thousands of cloud applications.

Mobile devices can be used to access web applications without causing content to be served based on the location of a cloud proxy, raising false identity theft alerts, or presenting frustrating or confusing error messages to mobile employees.

Users enjoy a fast, unobtrusive experience and the freedom to work however, whenever and wherever they want – with a consistent experience regardless of the device used. IT maintain visibility and where appropriate, control over web browsing.

Cloud Application Security can be enabled instantly without the need for any additional hardware, software, or configuration changes in your environment. It provides instant visibility into Shadow IT and potential insider threats originating from thousands of SaaS Apps with granular action-level controls enabling you to manage your cloud security without frustrating your users



Agents can be used in combination with the TrustLayer Cloud Gateway for sites with populations of fixed desktops, such as call centers. Installing a single gateway rapidly extends web content security policies to the entire network and optionally adds multiple security layers to defend against web-borne malware and other threats.

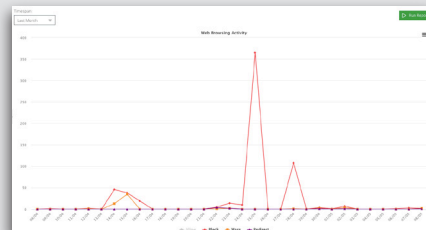
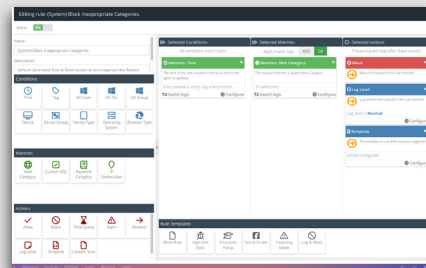
A sophisticated policy engine enables rules that block, allow, or allow and track web browsing activity. Time Quotas can be applied to rules to limit the time spent on shopping sites to 1 hour per day for example, enabling organizations to maintain productivity and effectiveness.

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.

Web Security is fully integrated with the TrustLayer Platform which provides rich data visualization and reporting across an extensive set of attributes and criteria. Analysis and reporting is available by time, user, device, Web Category, URL Category, domain, keyword and outcome (allow, block, redirect, warn).

Whether audit data is required purely for visibility into web browsing activity, or for more formal attestation of compliance with internal policies or external standards, regulations and legislation, Web Security will provide the evidence needed.



## DEPLOYMENT

Gateway	<ul style="list-style-type: none"> <li>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.</li> </ul>
Agents	<ul style="list-style-type: none"> <li>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.</li> </ul>
Deployment Modes	<ul style="list-style-type: none"> <li>Agent software, direct gateway (set by GPO, WPAD or manually), or gateway mode for guest, personal (BYOD) and non-domain devices.</li> </ul>
WPAD Support	<ul style="list-style-type: none"> <li>Automatic creation of Web Proxy Automatic Discovery file based on network configuration.</li> </ul>
WCCPv2 Support	<ul style="list-style-type: none"> <li>Supports Web Cache Communication Protocol v2 for transparent traffic redirection from Cisco routers/switches.</li> </ul>

## KEY FEATURES

ICAP	<ul style="list-style-type: none"> <li>Globally distributed ICAP Servers compare web request metadata against central policy rules removing the need to proxy traffic - delivering speed, reliability, and scalability without complexity.</li> </ul>
Realtime Anti-malware scanning	<ul style="list-style-type: none"> <li>TrustLayer Web Security incorporates multiple security layers, each using a powerful and highly effective combination of tools and techniques to detect sophisticated malware in it's tracks.</li> </ul>
URL Filtering	<ul style="list-style-type: none"> <li>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.</li> </ul>
Automatic Unknown URL Classification	<ul style="list-style-type: none"> <li>New URL's are analysed in realtime to ensure only acceptable content is accessed</li> </ul>
Anonymous Proxy Detection	<ul style="list-style-type: none"> <li>Prevent access to anonymous proxy sites.</li> </ul>

HTTPS Inspection	<ul style="list-style-type: none"><li>• Deep inspection allows SSL encrypted content to be scanned for malware</li><li>• Ability to disable SSL inspection for internal/trusted sites.</li><li>• Option to use Server Name ID (SNI) within the TLS protocol to determine destination domain without certificate management issues</li></ul>
Safe Search	<ul style="list-style-type: none"><li>• Enforce Safe Search mode on popular search engines including Google, Yahoo, Bing and YouTube.</li></ul>
BYOD/Guest Devices	<ul style="list-style-type: none"><li>• Safely allow BYOD and guest devices internet access via the built-in Captive Portal. Allows existing users to login from personal devices using valid credentials from Azure AD.</li></ul>
URL Overrides	<ul style="list-style-type: none"><li>• Create lists of categories or individual domains and URL's that can be bypassed through the filters.</li></ul>
Gateway Modes	<ul style="list-style-type: none"><li>• TrustLayer Cloud Gateway can operate in Explicit or Transparent mode</li></ul>

## MANAGEMENT

Policy Engine	<ul style="list-style-type: none"><li>• Sophisticated policy engine including AzureAD attributes, IP, MAC address, device type, custom tags, and differential actions.</li></ul>
Time Schedule	<ul style="list-style-type: none"><li>• Policies can be applied on a rolling 7-day schedule to customise access restrictions.</li></ul>
User Authentication and Synchronisation	<ul style="list-style-type: none"><li>• Multiple authentication methods supported including AD Kerberos, SSO, Captive Portal and RADIUS accounting. AD sync service ensures changes are replicated seamlessly.</li></ul>
Web Portal	<ul style="list-style-type: none"><li>• Fully integrated with TrustLayer's other modules, the CloudUSS dashboard offers a single pane of glass interface for management and reporting.</li></ul>
Delegated Admin	<ul style="list-style-type: none"><li>• Full Role-Based Access Control (RBAC) enables a range of access profiles and control/visibility permissions.</li></ul>
Custom Notifications	<ul style="list-style-type: none"><li>• Customise and brand notification and block pages with logo, html text, and other useful user information.</li></ul>

## REPORTING

Real-time Visibility	<ul style="list-style-type: none"><li>• Multiple charts and tables give instant insights on your user activity. Query the logs in realtime by numerous filter attributes to see exactly which users are accessing which sites.</li></ul>
Curated Reports	<ul style="list-style-type: none"><li>• Admins can build their own reports based on available fields and criteria, and can then export via PDF.</li><li>• Audit reports can be searched using multiple criteria including time, user, device, Web Category, URL Category, domain, keyword and outcome (allow/block/warn/redirect)</li></ul>
Scheduling and Alerting	<ul style="list-style-type: none"><li>• Link curated reports to a delivery schedule so analytics can be delivered to email inboxes on a regular cadence.</li></ul>
Interactive Reports	<ul style="list-style-type: none"><li>• Charts and Tables in the portal are fully interactive enabling admins to go from high-level trends to forensic-level detail with just a few clicks enabling prompt incident response.</li></ul>
Log Retention	<ul style="list-style-type: none"><li>• Web Security log data is archived automatically after 30 days. Log Streaming functionality is available to send logs to a 3rd party SIEM tool in realtime.</li></ul>