TrustLayer Web Security (WS)

Web security from Censornet 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 Censornet Platform that also includes Email Security, Cloud Application Security and Multi-Factor Authentication. The Censornet 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 proxies, 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 Censornet 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 purely agents on endpoints, Web Security offers a proxy-less, no gateway approach which significantly reduces latency, preserves the user's real IP addres

WEB SECURITY

- Manage over 500 categories of web content and billions of web pages
- Optionally protects against malware and other web threats at the gateway using multiple security layers and a powerful combination of technologies
- Complete protection – including deep inspection of SSL encrypted traffic
- New URLs are analyzed in real-time for malware and automatically categorized using machine learning techniques
- BYOD and guest device ready with Captive Portal for zero-touch filtering
- Policies can be set based on pre-defined Web Categories or custom URL Categories or keywords, and applied to groups of users or device groups
- Flexible deployment options – agent or proxy, or both
- Agents for Microsoft Windows and MAC OS X complement endpoint AV and ensure web content management policies are persistent when mobile users are working remotely
- Mobile device coverage by routing traffic (via VPN) through the TrustLayer Cloud Gateway, on premise or in the Cloud
- Optional Image Analysis gateway add on analyses image content in real-time for inappropriate 'Not Safe For Work' (NSFW) images
- Cloud Application Security can be enabled instantly without the need for any additional hardware, software or configuration changes to additionally provide discovery, visibility and management of access to 100s of cloud apps and 1000s of actions within apps.

and maintains privacy by allowing the browser to maintain direct communication with the web application server. 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 to additionally provide discovery, visibility and management of access to 100s of cloud apps and 1000s of actions within apps.

TrustLayer

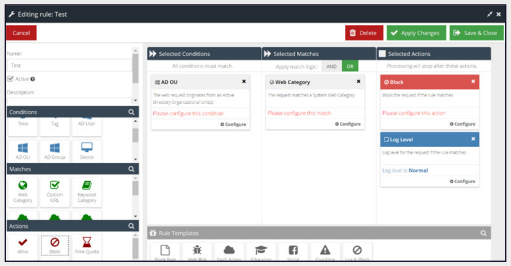
Agents can be used in combination with the TrustLayer Cloud Gateway for sites with populations of fixed desktops, such as call centers. Installing a single gateway rapidly extends web content security policies to the entire network and optionally adds multiple security layers to defend against web-borne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

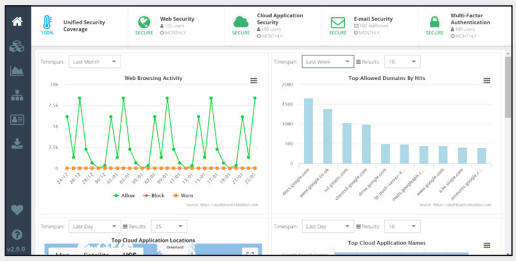
A sophisticated policy engine enables rules that block, allow, or allow and track web browsing activity. Time Quotas can be applied to rules to limit the time spent on shopping sites to 1 hour per day for example, enabling organizations to maintain productivity and effectiveness.

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	• TrustLayer Cloud Gateway can be installed on a virtual machine or physical server within 30 minutes to extend security policies to the entire network. Also available in the Cloud.
Agents	• Agents for Microsoft Windows and MAC OS X enforce policies on the device. Tamper proof and easy to deploy using an install wizard or via AD Group Policy. Complement existing endpoint AV with web content management.
Deployment Modes	• Agent software, direct proxy (set by group policy, WPAD or manually), or gateway mode for guest, personal (BYOD) or non-domain devices.
WPAD Support	• Automatic creation of Web Proxy Automatic Discovery (WPAD) file based on network configuration.
WCCPv2 Support	• Supports Web Cache Communication Protocol (WCCP) v2 for transparent traffic redirect from Cisco routers / switches.

KEY FEATURES

ICAP	• ICAP servers in multiple locations worldwide compare web request metadata against policy removing the need to proxy all traffic for speed, reliability and scalability.
Real-time Anti-Malware Scanning	• Incorporates multiple security layers each using a powerful and effective combination of tools and techniques including online threat detection, reputation and heuristics.
URL Filtering	• Over 500 categories of web content cover billions of web pages in multiple languages, constantly updated for accuracy and protection. Sub-categories are grouped into categories for ease of administration.
Automatic Unknown URL Classification	• New URLs are analyzed in real-time to ensure only acceptable content is accessed.
Image Analysis	• Optional gateway addon provides real-time analysis of image content for inappropriate 'Not Safe For Work' (NSFW) images. Three sensitivity levels – high, medium, low.
Anonymous Proxy Detection	• Prevent access to anonymous proxy sites.

HTTPS Inspection	• Deep HTTPS inspection allows SSL encrypted content to be scanned for malware (requires TrustLayer Cloud Gateway on premise or in the Cloud). • Ability to disable SSL inspection for specific trusted apps. • Option to use Server Name Indication (SNI) within the TLS protocol to determine destination domain when a connection is initiated – for light touch URL filtering of BYOD or guest devices without certificate management issues (used in conjunction with the Captive Portal).
Safe Search	• Enforce safe search mode on popular search engines including Google, Yahoo, Bing and YouTube.
BYOD / Guest Device Support	• Safely allow BYOD and guest device access via the built-in Captive Portal (with SNI support for zero-touch filtering). Allows existing users to log in from personal devices using valid credentials (e.g. Active Directory).
URL Overrides	• Create URL categories that can be applied to override or create exceptions within filtering policies.
Gateway Modes	• TrustLayer Cloud Gateway can operate in explicit or transparent mode.

MANAGEMENT

Policy Engine	• Sophisticated policy engine including Active Directory attributes, device IP and MAC address, device type, tag, and differential actions.
Time Schedule	• Policies can be applied on a rolling 7-day time schedule.
User Authentication	• Multiple authentication methods are supported including Active Directory Kerberos, single-signon, Captive Portal and RADIUS accounting.
User Synchronization	• Active Directory synchronization service ensures changes to Active Directory are replicated.
Web Interface	• Fully integrated with the Censornet Platform.
Delegated Administration	• Allows creation of multiple administrators with different levels of access to the Censornet Platform
Customized Notification Pages	• Brand notification pages (Block, Captive Portal, etc.) with logo, text and terms of service information.

REPORTING

Real-time Visibility	• Productivity charts display instant visibility on compliance with defined access policies. Query web activity in real-time by user, device, domain and category. See exactly which users are accessing which websites.
Report Builder	• Administrators can define their own reports based on available field names and criteria. • Reports can be saved and then exported. • Audit reports can be searched using criteria including time, user, device, Web Category, URL Category, domain, keyword and outcome (allow, block, redirect, warn).
Scheduling and Alerting	• Link reports to schedules and optionally only receive a report when there is content (alert mode). Alert on keywords, blocked categories, specific domains, etc.
Top Trend Reports	• A selection of pre-defined trend reports with chart and table data. Trend reports can be exported to PDF and emailed to recipients.
Extended Web Reports	• Optional addon provides additional reports by Active Directory Group including Top Web Categories by Group, Top Domains, Time Spent.
Multiple Views	• Analyze and report by user, device, Web Category, action.
Log Retention & Autoarchiving	• Web Security log data is archived automatically after 90 days and available to download from the TrustLayer Platform for a period of a further 12 months. Longer retention periods are available.