Comprehensive web and email defenses against advanced threats and data theft.

Timed and targeted attacks with custom lures, spear-phishing focus, hidden redirects and the unique ability to detect exploits are bypassing traditional defenses. A new security standard of "point-of-click" protection is required, provided by web and email security gateways using real-time analytical defenses with containment against data theft and loss.

Why is Websense the best choice?

Websense® TRITON® Security Gateway Anywhere combines premier hybrid Websense web and email gateways into a single smart investment. Both integrate enterprise data loss prevention (DLP) to protect intellectual property (IP) from theft and loss, and provide regulatory compliance. Websense ACE (Advanced Classification Engine) provides inline real-time defenses for point-of-click protection for both web and email. The optional Websense ThreatScope™ tool, a Websense CyberSecurity Intelligence™ (CSI) service, provides malware sandboxing analysis.

TRITON Security Gateway Anywhere includes the following:

Websense Web Security Gateway Anywhere

- ACE defenses provide equal protection for on-site and remote users.
- Websense ThreatSeeker® Intelligence Cloud unites global threat awareness and telemetry from over 900 million endpoints.
- Advanced threat dashboard offers high severity alerts, maps, charts and forensic details that can be exported to SIEM solutions.
- Data theft defenses include OCR of text within images; detection of slow data leaks, password file theft and custom encryption; and geo-location destination awareness.
- Integrated enterprise DLP contains over 1700 policies and templates easily selected by region and industry to protect IP and confidential data.
- Industry-leading web security policy controls, time quotas and social web controls with multiple authentication options for users and groups.
- Scalable appliances are deployed for critical web gateways, while cloud services are used to protect small offices or remote users in any location.

Websense Email Security Gateway Anywhere

- ACE defenses use email URL sandboxing for point-of-click protection against spear-phishing and targeted attacks.
- Features include email content controls and filtering, anti-spam, commercial bulk email detection, and TLS server-to-server encryption with optional image analysis and identity-based encryption services.
- Integrated enterprise DLP contains over 1700 policies and templates easily selected by region and industry to protect IP and confidential data.
- ActiveSync agent for mobile email DLP policy controls supports any ActiveSync-compatible mobile device.
- Hybrid design cleanses spam and threats from incoming email in the cloud to reduce bandwidth consumption, and uses appliance-based DLP to protect IP and confidential data from leaking in outbound email.
- Leading web security defenses are used for embedded email web links.

PROTECTIONS
WEB ☑ EMAIL ☑ DATA ☐

PLATFORMS
SOFTWARE ☐ APPLIANCE ☐ CLOUD ☐ HYBRID ☑

Advanced Threat Defenses

- ACE real-time inline defenses for on-site and remote users
- Enterprise DLP with data theft defenses for data containment
- Advanced threat dashboard with forensic reporting details
- Optional ThreatScope malware analysis sandboxing service

Improved Protection

- Reduce malware incidents and risk of data theft and damage to reputation
- Reduce help desk incidents and time spent re-imaging systems
- Free up IT staff to work on new business opportunities

Superior Services and Certifications

- Industry-leading 99.999% SLA
- FIPS, IPv6, CC EAL2+ certifications
- Global ISO 27001-certified data centers
- 24/7 staffing
- Physical intrusion detection systems
- Video surveillance
- Restricted access lists
- Photo and biometric verification

"Websense TRITON Security Gateway Anywhere represents the next generation of business security solutions."

Dave Mitchell
Director and Founder
Binary Testing

---

websense
TRITON®

The Websense difference:
ACE (Advanced Classification Engine)

ACE provides real-time, inline, contextual defenses for web, email, data and mobile security by using composite risk scoring and predictive analytics to deliver the most effective security available. It provides containment by analyzing inbound and outbound traffic with data-aware defenses for data theft protection. Over 10,000 analytics across eight defense areas include real-time classifiers, behavioral sandboxing and other advanced capabilities, enabling ACE to detect and stop more threats. ACE is the primary defense behind all Websense TRITON® solutions, and is supported by the Websense ThreatSeeker® Intelligence Cloud, which collects data from more than 900 million endpoints and analyzes 3–5 billion web requests every day.

Websense Web and Email security gateways use ACE defenses to detect threats in real-time.

Your Needs	Websense Solutions
Protect all users with one solution for web and email security	TRITION Security Gateway Anywhere combines leading web and email security gateways into one smart investment. Manage corporate, branch and remote users with one unified architecture.
Real-time protection against advanced malware	ACE goes beyond anti-virus defenses by using seven defense assessment areas in a composite scoring process that uses predictive analysis. Multiple real-time content engines analyze full web page content, active scripts, web links, contextual profiles, files and executables.
Forensic reporting and alerts for advanced threats and data theft incidents	Advanced threat dashboard provides forensic reporting on who was attacked, what data was attacked, where the data almost went, and how the attack was executed, plus exportability to SIEM solutions. Security incidents include data theft capture when possible.
Prevent data theft and loss at web and email gateways	Integrated enterprise DLP detects and intercepts data theft attempts and provides regulatory compliance for DLP. Ten new defenses include detection of custom encrypted uploads, password file data theft, and slow data leaks (drip DLP), plus optical character recognition (OCR) of text within images and geo-location destination awareness.
Leading web security and controls, plus reporting	Social web controls for Facebook, LinkedIn and YouTube for Education. Custom/allow deny lists with controls for viral, entertainment and surveillance videos. Network Agent non-proxy protocol and application controls across all ports. Multiple dashboards and over 60 reports.
Leading email security with point-of-click protection	Email URL sandboxing wraps web links for point-of-click protection with ACE real-time defenses. ACE also provides anti-malware and anti-spam protection. Email content controls and filtering, commercial bulk email detection, and TLS server-to-server encryption.
Value-add security options	Optional ThreatScope malware analysis sandboxing for web and email files provides full forensic infection and call-home analysis with CSI: On-Demand services. Add-on email security options include image analysis, archiving, and identity-based encryption services.

Mobile, social, and cloud technologies drive productivity. But they also open the door to data theft and advanced attacks that can slip right by anti-virus, URL filtering and firewall defenses. Websense® TRITON™ solutions keep you a step ahead with web, email, data, cloud and mobile security solutions (available together or separately) that share a common architecture. The real-time defenses of Websense ACE (Advanced Classification Engine), plus flexible deployment options and a unified management console, make TRITON solutions vital in today's dynamic environments.

Learn more at **www.websense.com | +1 800-723-1166 | info@websense.com**

TRITON STOPS MORE THREATS. WE CAN PROVE IT.

websense
TRITON®