Websense® TRITON® RiskVision™

GAIN ACTIONABLE THREAT INTELLIGENCE INTO DATA THEFT, ADVANCED CYBER THREATS AND OTHER SOURCES OF RISK TO YOUR CRITICAL DATA

Websense® TRITON® RiskVision™ is an extensible threat platform that collects and correlates threat intelligence from multiple detection engines and channels. It identifies infected systems, call home communications, blended attacks and data exfiltration. This unrivaled threat monitoring solution also proactively discovers Advanced Threats via sandboxing and many other real-time techniques, delivering actionable data and reports on threats to your data. With key advantages such as global security intelligence, cloud application visibility and data loss/data theft detection in a single appliance that is easy to deploy via a network TAP or SPAN port, TRITON RiskVision provides immediate visibility into Advanced Threats, data exfiltration and infected systems.

REAL-TIME DEFENSES, GLOBAL THREAT AWARENESS, SANDBOXING AND DLP

TRITON RiskVision unifies four key defenses into one platform:

- **Websense® ACE** (Advanced Classification Engine) uses seven defense assessment areas with over 10,000 analytics to provide real-time threat analysis of web and email traffic.
- **Websense® ThreatSeeker® Intelligence Cloud** unites over 900 million endpoints and analyzes 3-5 billion requests per day, providing global threat awareness and vital defense analytics to ACE.
- **Websense® TRITON® ThreatScope™** sandbox analyzes behavior of web downloads and email attachments to uncover Advanced Threats and provides actionable forensic reporting.
- **Data loss prevention** (DLP) detects data exfiltration for registered data, criminal-encrypted uploads and password file data theft.

PROTECTIONS
WEB ☑ EMAIL ☑ DATA ☑

PLATFORMS
SOFTWARE ☐ APPLIANCE ☑ CLOUD ☐ HYBRID ☐

File Sandboxing & Forensics

- Integrated web download and email attachment file sandboxing for behavioral analysis and forensic reporting with actionable insights.

Cloud Application Visibility powered by Skyfence

- Identify critical data threats from “shadow IT” by uncovering high risk cloud application usage and those users putting your data at risk.
- Identify safer, alternative cloud applications.

Integrated DLP Defenses

- Content and context aware DLP detects data exfiltration related to theft or loss.
- Data theft features include detection of data loss via outbound email, web communication including webmail, and cloud app usage.

Advanced Threat & Data Theft Detection

- ACE real-time defenses for advanced threat and data theft detection.
- More than 10,000 analytics enable defenses against undetected threats.

Global Threat Awareness

- Security intelligence from the ThreatSeeker Intelligence Cloud.
- Analyzes up to 5 billon web, email and social networking requests per day.
- Facebook partnership provides insight into social media lures and threats.

“Websense is improving security technology by examining web and data content as it attempts to enter and leave an organization. The company continues to innovate and deliver security technology that protects organizations from the latest malware.”

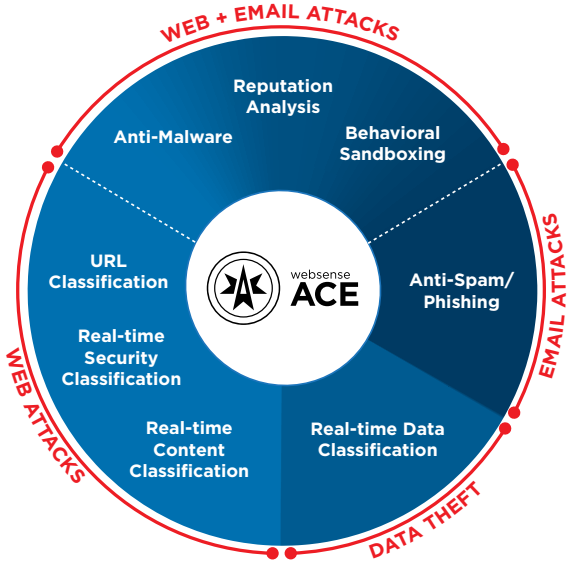
– Jeff Wilson, Principal Security Analyst, Infonetics

Raytheon | websense®

Websense® TRITON® RiskVision™

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.



GLOBAL THREAT INTELLIGENCE

The ThreatSeeker Intelligence Cloud uses all eight ACE defense assessment areas, plus a series of out-of-band analyses. These might include developments in, or adjustments to, existing ACE analytics, all performed under the careful watch of Websense® Security Labs™ researchers.

Your Needs	Websense Solutions
Advanced threat intelligence that works with existing countermeasures.	Extensible threat intelligence platform channels threat intelligence into existing security controls for zero-latency defenses against Advanced Threats.
Visibility into cloud application usage and IT compliance.	Identifies critical data threats from “shadow IT” by uncovering cloud application usage and those users putting your data at risk.
Visibility into Advanced Threats and data theft/data loss incidents.	TRITON RiskVision combines real-time advanced threat defenses, global security intelligence, file sandboxing and data loss/data theft detection into a threat monitoring solution that provides insight into threats unseen by traditional defenses.
Advanced threat detection beyond traditional defenses.	ACE goes beyond anti-virus defenses by using seven defense assessment areas in a composite scoring process that applies predictive analysis. Multiple real-time content engines analyze full web page content, active scripts, web links, contextual profiles, files and executables. ACE leverages over 10,000 analytics derived from the ThreatSeeker Intelligence Cloud.
Detection of data theft and data loss within multiple channels.	Advanced DLP defenses detect data theft and data loss. Advanced data theft defenses include detection of custom encrypted uploads and password file data theft. Provides visibility into potential data loss and theft from outbound emails and file uploads to well-known cloud applications.
Sandboxing of files and objects to detect Advanced Threats, with actionable forensic reports.	ThreatScope web file sandboxing provides behavioral analysis to uncover Advanced Threats and communications, plus detailed forensic reporting. An advanced threat dashboard provides forensic insight on who was attacked, what data was attacked, where the data was destined and how the attack was executed. Security incidents include data theft capture when possible, with the ability to export forensic details to SIEM systems.
Ready-to-deploy appliance provides immediate visibility.	TRITON RiskVision deploys on Websense V10000 appliance via a network TAP or SPAN port deployment alongside TRITON management and reporting servers. Please refer to the latest V-Series datasheets for hardware specifications. Integrates with industry leading SSL decryption products.

Contact us to learn more: www.websense.com/Contact

Raytheon | websense®