Websense® TRITON® ThreatScope™

Prepare for the Most Advanced, Targeted Zero-Day Threats and APTs.

Mass-market attacks have given way to more tailored threats ranging from phishing to custom malware. Websense® TRITON® ThreatScope™ provides additional defenses for the most advanced, targeted zero-day threats and advanced persistent threats (APTs) that may attack through web or email channels. Organizations can also become more proactive through behavioral sandbox forensics and phishing activity reports with actionable insights.

Why TRITON ThreatScope?

TRITON® ThreatScope offers unrivaled protection enhancements to Websense web and email security defenses. Integrated behavioral sandboxing results are considered along with other Websense ACE (Advanced Classification Engine) analytics to counter innovative, emerging evasion techniques and ensure accurate identification of threats. Networked and mobile users enjoy real-time feedback regarding suspicious email communications, even when working remotely. And detailed sandbox forensics and phishing reports provide insights to help organizations assume a more proactive security posture against future attacks.

TRITON ThreatScope enhances defenses in five areas:

• **File sandboxing for web.** Monitor web traffic for real-time code analysis in a behavioral sandbox for advanced threat identification.
• **File sandboxing for email.** Intercept attachments in real-time for additional threat analysis in a behavioral sandbox.
• **Email URL sandboxing.** Embedded links are disarmed and analyzed in real time at point of click.
• **Detailed forensic reporting.** Use sandbox results to guide any necessary response or proactive measures against future attacks.
• **Phishing education and reporting.** Increase phishing awareness at both the user and network levels to drive effective change.

Granular Policy and Social Web Controls

TRITON ThreatScope provides an online sandbox environment for safely testing potential malware. Using ACE analytics, all activity is monitored and documented in a detailed report including:

• The infection process and post-infection activity.
• System-level events and changes to files, processes, registry, etc.
• Network communications including connections/methods used and destination.

Observed behavior is correlated with known threats to provide valuable, actionable Insights.

Behavior Sandboxing and Forensics

- Allows safe execution of suspicious code away from network resources.
- Research-grade sandbox used and managed by Websense researchers.
- Integrated behavioral sandboxing enhances advanced threat detection.
- Detailed forensic reporting provides actionable insights.

Advanced Assessment Capabilities

- ACE applies eight defense assessment methods, through 10,000+ analytics for maximum effectiveness.
- Real-time threat visibility through Websense ThreatSeeker® Intelligence Cloud, which receives up to 5 billion requests per day from over 900 million endpoints.
- Improves accuracy while mitigating false positives.

Forensic Investigation Resources*

- Manual sandbox access to support special forensic investigation scenarios.
- Online security labs presentations and other investigation education resources.

*Provided through a bundled license for CyberSecurity Intelligence Services

“Malware today is targeted, polymorphic, and dynamic. It can be delivered via Web page, spear-phishing email, or any other number of avenues.”

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.

<table>
<thead>
<tr>
<th>Your Needs</th>
<th>Websense Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure web and email against advanced malware</td>
<td>Suspicious code is triggered in an isolated behavioral sandbox allowing it to execute safely, yet reveal any malicious intentions. Intercepted in-line, IT is alerted of newly revealed threats in real time, along with detailed forensic report.</td>
</tr>
<tr>
<td>Actionable information from forensic reporting</td>
<td>The ThreatScope forensic report provides details of both infection and post-infection activity that can be used to fine tune defenses against attack, as well as identify and possibly recover infected systems.</td>
</tr>
<tr>
<td>Integrated defenses for maximum effectiveness</td>
<td>Sufficient clues to a truly advanced, targeted attack may not exist solely in a well-crafted malicious code. Because behavioral sandbox results are considered along with other ACE analysis of the delivery vehicle (web or email), advanced threat detection capabilities grow exponentially.</td>
</tr>
<tr>
<td>Advanced email link defenses</td>
<td>Suspicious URLs are modified such that when a user clicks the link in a message from any device (e.g. laptop, smart phone, tablet), the URL is analyzed in real time before allowing access. Despite other benefits, this is invaluable when a website is compromised well after the link is originally delivered via email.</td>
</tr>
<tr>
<td>Personalize phishing facts</td>
<td>Both users and IT staff are provided with customized information. User education and feedback alert users to risks, while IT reports can identify trends that may indicate a need for policy, process or other changes.</td>
</tr>
<tr>
<td>Security education</td>
<td>Online training provides on-demand access to security courses ranging from exposing encrypted code to troubleshooting compromised mobile devices. New courses are added based on current Websense Security Labs research projects.</td>
</tr>
</tbody>
</table>

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](http://www.websense.com) | +1 800-723-1166 | info@websense.com

TRITON STOPS MORE THREATS. WE CAN PROVE IT.