The Value Proposition
Targeted attacks have increased four times in 2011 and headlines continue to note data theft and loss incidents making security and risk reduction top business issues. Cybercrime continues to step over traditional defense hurdles lined up sequentially and often lacking any unified intelligence while social media, mobility and cloud computing stretch security perimeters.

Websense and WSGA uniquely provide:

- Websense® Advanced Classification Engine (ACE), with real-time classifiers for content, security and data, plus defense assessments providing a unified composite score
- ThreatSeeker Network unites over 900M end points for big data & cluster analysis of 3-5B requests per day feeding machine learning systems to create analytics for real-time updates to ACE
- Contextual defense leverages an integrated DLP engine to detect outbound data theft and call-home communications to contain infected systems
- TRITON® architecture provides a single console for policies with re-use per channel, plus workflows and reporting for web, email, and data security
- TRITON solutions enable a lower TCO with the integration of web, email, data, mobile security

Why Websense® TRITON™ Solution?
Unified Console
- Single console to create policies with re-use per channel, plus workflows and reporting for web, email, and data security

Unified Architecture
- Ability to deploy web, email and data security on one appliance or expand for performance and scale

Unified Security Intelligence
- ACE composite risk scoring combines multiple advanced analytics derived from ThreatSeeker® Network for web, email & data

Product Capabilities
- Performance and scale from V5K, V10K and the new X10G blade server, providing security for 250 to over 100,000 users
- ACE composite risk scoring combines multiple advanced analytics (including real-time analysis and classification) to detect modern malware that evades traditional AV and FW defenses
- Inline ACE real-time defense assessments for HTTPS and social networking private pages, plus social web app controls
- Integrated enterprise DLP provides unique data fingerprinting, natural language processing, and over 1,100 pre-defined DLP policy templates for compliance and data theft/loss protection
- Single management console to reduce administration & training
- Hybrid architecture with cloud security for remote users
- Role-based policy controls and reporting

Why Web Security Gateway Anywhere—Independent Analysts
Cybercrime counts on traditional defenses lacking real-time defense assessments, unified security intelligence and composite risk scoring so they can succeed. With the web security landscape changing, leading independent analysts have recognized the capabilities of WSGA as being well-positioned to defend against modern attacks.
- SWG Leaders Quadrant, Gartner MQ 2011
- DLP Leaders Quadrant (5 years), Gartner MQ 2011
- WW Market Share Leader for SWG, Gartner 2010

Sound Bites
- “The Websense WSG provides extensive on-box, non-signature-based methods for detecting malware and advanced persistent threats (APTs).”
  – Gartner Magic Quadrant, SWG 2011
- “All security and reporting features are seamlessly integrated into a single unified management console.”
  – Binary Test Product Review, Q2 2011
- “Websense offers a unified console that is capable of managing a hybrid SWG solution (on-premises and SWG as a service).”
  – Gartner Magic Quadrant, SWG 2011
- “Websense is a good candidate solution for buyers looking for integrated Security Web Gateway and Secure Email Gateway functionality and advanced DLP capability.”
  – Gartner Magic Quadrant, Email Security 2011
Managing Objections

Websense is a web filtering company

- Websense manages the largest security intelligence network with over 900M end points, providing big data & clusters for machine learning to produce analytics in ACE for web, email and data security. Websense partners with Facebook and other social media. Websense ®TRITON® solutions are data-aware for a contextual defense containing data theft and loss, plus providing unmatched defenses against advanced malware. Websense is a “security” company.

Websense uses Command AV, no leading AV engines

- ACE real-time defenses provide composite risk scores that are tested daily against five top AV engines (available on the WSL web site). ACE not only integrates a commercial AV engine, plus an internal AV engine, it unites three real-time classifiers (content, security, data) using over 10,000 analytics derived from ThreatSeeker with real-time updates. ACE is included in TRITON® solution at no extra charge, why pay extra for traditional AV that is a low hurdle for cybercrime to step over in competitive solutions.

Websense lacks large enterprise performance and scale

- The new Websense X10G™ blade server scales WSGA up to 100,000 users and opens new doors to large enterprise, educational, service provider, system integrator and federal customers. The X10G is a 10U blade chassis with the capacity for 16 blades each performing beyond current V10K levels. At full capacity, the X10G consumes 40% less rack space and at a lower price per user than V10Ks. Websense provides large enterprise performance and scale with real-time defenses for advanced malware and data theft/loss.

<table>
<thead>
<tr>
<th>Customer Pain Points</th>
<th>Discovery and Measurement Questions</th>
</tr>
</thead>
</table>
| **Advanced Malware & Targeted Attacks** | - How are you currently addressing web threats and controlling web access? What’s working? What’s not working? What is the impact of this to your business?  
- What security defenses beyond AV are deployed for real-time analysis against targeted attacks?  
- What security defenses analyze web pages, active scripts, links and files in real-time to block attacks using dynamic delivery, payloads and call-home methods?  
- Describe your ability to contain an attack from an internal infected system? |
| **Data Theft/Loss Compliance/Regulations** | - How are you addressing data theft & data loss (compliance) for web access?  
- What defenses do you have for outbound data theft and call-home analysis?  
- How does your current solution detect outbound proprietary encrypted files, password files, geo-location destinations, or the use of dynamic DNS? |
| **Social Media/Networking Employee Productivity** | - How are you monitoring and providing policy controls for social media and networking?  
- How do your current defenses collect security intelligence from Facebook or Twitter?  
- What real-time ratings are in use for objectionable and unproductive content?  
- Would time quotas and policy controls on app functions improve productivity? |
| **Too Many Disparate Point Products** | - How many systems do you login to manage policies/reporting for your Web Security, Email Security, and Data Security products?  
- How many total devices (appliances, reporting servers, management servers, encryption servers, etc.) do you require for your Web, Email, and Data Security products?  
- Are you able to leverage your administrative knowledge for your web security system and extend that to manage your email and data security systems?  
- What happens when your primary web/email/data security administrator goes on vacation? Do you have additional resources who understand how to perform basic management of the system? |

For more information, refer to the Websense Partner Portal at https://www.websense.com/content/Partners.aspx