TECHNOLOGY BRIEF

ENHANCE MICROSOFT OFFICE 365 WITH WEBSENSE® EMAIL SECURITY AND DATA PROTECTION SOLUTIONS
The benefits of moving business applications to the cloud continue to entice many organizations. In particular, Microsoft Office 365 provides organizations of all sizes a viable alternative to managing their email system in-house.

Historically, Microsoft has relied on third parties to deliver advanced administration, reporting, anti-virus and other features, and Office 365 is no different. It’s a great foundation, but its email security in particular requires further enhancement to keep pace with the rapidly evolving threat and data loss landscape.

Backed by our years of experience protecting Microsoft Exchange email environments, Websense® Email Security Gateway Anywhere and Websense Cloud Email Security solutions enhance Office 365 with advanced email threat protection and industry-leading email data loss prevention (DLP). These advanced email security and DLP solutions keep you out in front of the latest phishing attacks and new and updated compliance regulations, while allowing you to realize the benefits of Office 365.

**Advanced Email Security Informed by Global Intelligence**

Because email remains the primary form of business communication, hackers, nation states and other cyber-criminals continue to attack via email with increasingly catastrophic consequences. Today’s most dangerous attacks use a combination of email and malicious web links — a very challenging combination for traditional technologies to contend with. It is therefore vital to protect this attack vector with real-time defenses that go beyond signature-based anti-malware, anti-virus and reputation-based anti-spam.

Combatting advanced targeted attacks requires a cohesive approach to cybersecurity that correlates both email and web security data. Websense ACE (Advanced Classification Engine) and Websense ThreatSeeker® Intelligence Cloud work in this way to deliver real-time email security against the most advanced threats.

ThreatSeeker Intelligence Cloud is among the largest security intelligence networks. It processes up to 5 billion requests every day to provide content analysis through more than 900 million endpoints. This content takes the form of emails, web pages, documents, social media, streaming media, mobile applications and other Internet traffic.

ACE is the key real-time defense engine used in-line with Websense email security and web security products. The broad exposure of ThreatSeeker Intelligence Cloud to email and web activity, and Facebook and other social media sites, fuels ACE defense assessment areas with threat intelligence and analytics for the predictive composite analysis required for proactive capabilities (e.g., identifying zero-day exploits, new malware, innovative social engineering tactics, phishing email and other aspects of emerging threats).

The more than 10,000 analytics and other methods applied by ACE encompass a broad spectrum of security assessment technologies — from proprietary real-time security, content and data classification processes to traditional security technologies. Composite scoring across eight defense assessment areas enables ACE to minimize false positives and improve accurate classification.
Malicious Link Protection at the Point of Click

Websense recognized early that blocking 100 percent of spam and malicious email would never happen, and that a solution was needed for protection after message delivery. Using URL sandboxing and information from ThreatSeeker Intelligence Cloud, Websense email security analyzes all web links contained in an email to determine their trustworthiness. Suspicious links are rewritten so that, at the time of click (from any device, including smartphones and tablets), the URL request is forwarded to the Websense cloud, where the final link destination and any redirects are examined. Any files discovered as part of the URL scan are also analyzed in real time for malicious intent.

Enhanced Reporting

Office 365 email protection provides limited reporting that depends on the service level purchased but still limited to only a small set of standard reports. Advanced reporting requires either a third party add-on or the Office 365 Reporting web service and writing your own code and queries. Websense provides email security administrators with enhanced visibility and reporting, including over 100 predefined and customizable reports covering the categories most useful to administrators.

User Management

Default settings for Office 365 anti-spam place all suspected spam messages in the Outlook Junk Email folder. This creates a potential security issue for email security administrators concerned that users might release a malicious email. Websense enhances quarantined message management by providing a completely separate interface to manage spam, enabling users and administrators to clearly know what is clean and what is suspect. The Websense Personal Email Manager provides users with additional details as to why a message was quarantined, enhancing user education, an increasingly vital element in email security.

Regulatory Compliance and Intellectual Property Protection

Regulations such as PCI-DSS, GLBA and HIPAA have created complex requirements for the protection of confidential information delivered via electronic communications. In addition, non-regulated industries are realizing a need to protect intellectual property (IP).

Websense data protection allows both regulated and non-regulated industries to quickly and easily address even the most complex data protection requirements. Websense provides a number of data protection enhancements over Office 365. For example:

- Office 365 DLP provides 40 templates covering 9 countries and requires the Office 365 Enterprise E3 plan.
- By comparison, Cloud Email Security provides 240 templates covering 12 languages and is included at no extra charge.
- For organizations requiring an even higher level of data protection, Email Security Gateway Anywhere increases the number of policies and templates to 1700, driven by an intuitive DLP wizard that quickly identifies the applicable policies based on country and industry.
- Advanced features such as protection from slow data theft (Drip DLP); geolocation destination awareness (limiting where data can be sent); detection of custom encrypted uploads and password file data theft; optical character recognition (OCR) of text contained within images; and machine learning are also available.

In addition, advanced email encryption can be added to provide transparent encryption for secure communication of messages containing sensitive information to both desktop and mobile users. Websense DLP solutions allow organizations to meet all regulatory compliance requirements as well as protect vital IP from exfiltration.
Unified Threat Protection

Over time many organizations have implemented additional layers of security to address the increasingly complex threat landscape. Each layer comes with a unique management console resulting in an over-abundance of consoles for today’s security professional to contend with. Websense advanced email security solutions are based on the Websense TRITON® architecture, which delivers unified policy and management across web, email and DLP. From a single management interface you can create policies that are then applied to any or all of the underlying security solutions, generate and view reports and manage all users and groups. This singular view and unified management allows Websense to provide the lowest TCO while providing the highest level of security.

<table>
<thead>
<tr>
<th>Tech Highlights</th>
<th>Simplified Integration</th>
</tr>
</thead>
</table>
| Websense is a proven supporter of Microsoft Exchange customers. | Advanced Email Security  
• MX records are pointed to Websense  
• Websense forwards clean messages to Office 365 |
| ThreatSeeker Intelligence Cloud and ACE provide real-time protection based on up to 5 billion requests per day and 10,000+ analytics. | Data Protection  
• Messages are routed to Websense using the Office 365 Outbound Smart Host Connector |
| Advanced security solutions offer enhanced reporting and visibility in to your email infrastructure. | Websense maintains current list of Office 365 sending IPs to guarantee delivery and accurate outbound processing |
| Gartner Inc. positioned Websense as a leader in its “Magic Quadrant for Content-Aware Data Loss Prevention (DLP)”.* | |
| URL sandboxing protects against malicious links on all devices, including smartphones and tablets. | |

* Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings. Gartner research publications consist of the opinions of Gartner’s research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

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

TRITON STOPS MORE THREATS. WE CAN PROVE IT.