Partner Playbook – Email Security

websense®

Elevator Pitch

Websense® Email Security Gateway Anywhere (ESGA) combines the power of the cloud to cleanse inbound mail (threats & spam) to optimize appliance performance while enforcing outbound data loss prevention (DLP). ESGA includes Websense® Advanced Classification Engine (ACE) , which provides advanced protection against targeted, blended attacks and TruEmail DLP for fully integrated, enterprise-class DLP—all managed through a single unified console.

The Value Proposition

Over 89% of all unwanted emails contain links, often times to sites designed solely for malicious purposes. In fact, attacks blending web and email vulnerabilities have been responsible for some of the biggest security compromises over the past 18 months—email is the open door to these attacks.

Websense ®Email Security Gateway Anywhere (ESGA) provides unmatched protection against these modern threats. The **Websense® Advanced Classification Engine** (ACE) leverages leading ***real-time web intelligence*** to effectively identify and thwart emails that contain malicious URLs. Effective defense against today's malicious emails require an in-depth understanding of the web.

While ESGA combats modern threats, it is also extremely effectively in combating traditional spam and malware. 84% of all email is spam. **Websense® TruHybrid™ deployment** helps alleviate this by cleansing all inbound mail in the cloud, removing spam before it ever reaches your network—all backed by Service Level Agreements. This ensures your organization will retain ***maximum resiliency*** during spikes in email volume without increased costs.

And, of course, many of these threats have been designed to capture your confidential data. Email is a channel where sensitive data is deliberately or accidentally lost. **Websense® TruEmail DLP™** capability provides ***built-in enterprise-class DLP*** that is highly accurate in detecting and blocking data that should not leave your network—all without constant manual tuning or 3rd party hardware.

Why Websense® TRITON™ Solution?

Unified Console

- Single console to create policies, workflows, reporting for email, Web, and data security

Unified Platform

- Single Websense® V-Series™ appliance, management server, and reporting server for combined Web, Email and Data Security deployment

Unified Security Intelligence

- Composite risk scoring combines multiple advanced analytics (including real time analysis and classification)

Product Capabilities

- **Advanced Classification Engine** (ACE) uniquely provides:
  - Composite risk scoring combines multiple advanced analytics (including real-time analysis) to detect modern malware that evade independently operating security products
  - URL Sandboxing pre-examines web links in emails that have unknown reputations or have not been previously analyzed
  - Sender reputation, adaptive learning, URL analysis, heuristics, digital fingerprinting, optical recognition of image spam help to guarantee 99% spam detection
- Enterprise-class DLP with over 1,100 pre-defined DLP templates
- Manual or policy-based encryption without the need for complex key management, and no additional hardware or software required (Optional Add-On)

Why Websense Email Security Gateway Anywhere

Cybercrime counts on traditional email gateways lacking data theft protection, advanced real-time malware detection and encryption services so they can succeed. With the email landscape changing, leading independent analysts have recognized the capabilities of ESGA as being well-positioned to defend against modern attacks.

- **Value Leader For Message Security**, EMA Radar Report 2011
- **Best Hybrid Strategy for Message Security**, EMA Radar Report 2011
- **Visionary for Secure Email Gateways**, Gartner MQ 2011
- **DLP and Secure Web Gateway Leaders Quadrant—**5 years in a row, Gartner

Sound Bites

- "Websense has a very strong security research capability for Web-based threats... Because most email threats have a Web destination, data from these activities should translate to solid email security."
  – Gartner Magic Quadrant, Email Security 2011
- "The company processes a very high amount of email, and it consistently meets its SLAs that guarantee 99% spam catch rate, 100% detection rate for known viruses, 99.999% uptime."
  –EMA Research, Message Security Services Radar Report 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
- "All security and reporting features are seamlessly integrated into a single unified management console."
  -Binary Test Product Review, Q2 2011

Partner Playbook – Email Security

websense

Managing Objections

Websense is not an email security-focused vendor

- Websense has over 10 years of experience in the email security market, where over 2000 organizations worldwide—spanning all industries and sizes—rely on our expertise in this domain. In the past year alone, Websense has issued four email security product releases and continues to innovate for the evolving email threats.

Websense Email Security Gateway (ESG) is not respected by analysts

- ESG/A has garnered positive recognition by leading independent analysts. EMA Research awarded Websense as having the *Best Hybrid Strategy* and being a *Value Leader*, while Gartner recognized Websense as the *Visionary* in the changing email security market.

  These same analysts have also cautioned that for customers to properly defend against modern attacks, an email security solution must have deep understanding of web threats and be able to protect sensitive data. ESG/A leverages the intelligence from Websense leading Web Security product and the same enterprise-class DLP technology as our standalone data security solution, which has been in the *Leaders Quadrant* in the Gartner DLP Magic Quadrant for 5 consecutive years.

Implementation of DLP in ESGA is a 6-12 month project

- Websense® TruEmail DLP™ capability, and its over 1,100 pre-configured rules and compliance policies, is fully integrated into ESG/A and can be up and running in hours—all part of the standard getting started process.

  Down the line, as part of a more holistic DLP initiative, a customer can extend to full-enterprise DLP across all channels (i.e. web, USB, endpoints) with a simple license upgrade. Administration across these channels are conducted within a single interface/login. Best of all, policies created prior for email can be used and applied for the new channels—without the need to re-create policies.

Customer Pain Points	Discovery and Measurement Questions
Blended, Targeted Threats Elude Current Solution	▪ Have you encountered a recent email security incident? ▪ Cybercriminals have unified their attacks (blending email and web threats), have you unified your defenses? ▪ What email security solution are you using today? How does your current solution defend against the latest threats, such as low-volume spear-phishing attacks that incorporate email and Web vulnerabilities to steal sensitive data? Is it primarily based on past reputation of IP/send address/web page?
Loss in Employee Productivity	▪ What percentage of your emails is spam? How much of that is being captured by your current solution? What are the SLAs for detecting malware and spam? ▪ How does current email infrastructure respond to a spike in spam/email volume? ▪ What happens when you experience a network or mail server outage? When this occurs, do you have a system in place so that no emails are lost?
Liability Risk	▪ What regulatory or compliance mandates are you required to meet? ▪ How are you currently detecting sensitive/confidential data is leaving your organization via email? ▪ How you had any data leak/data theft incidents in the past year?
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