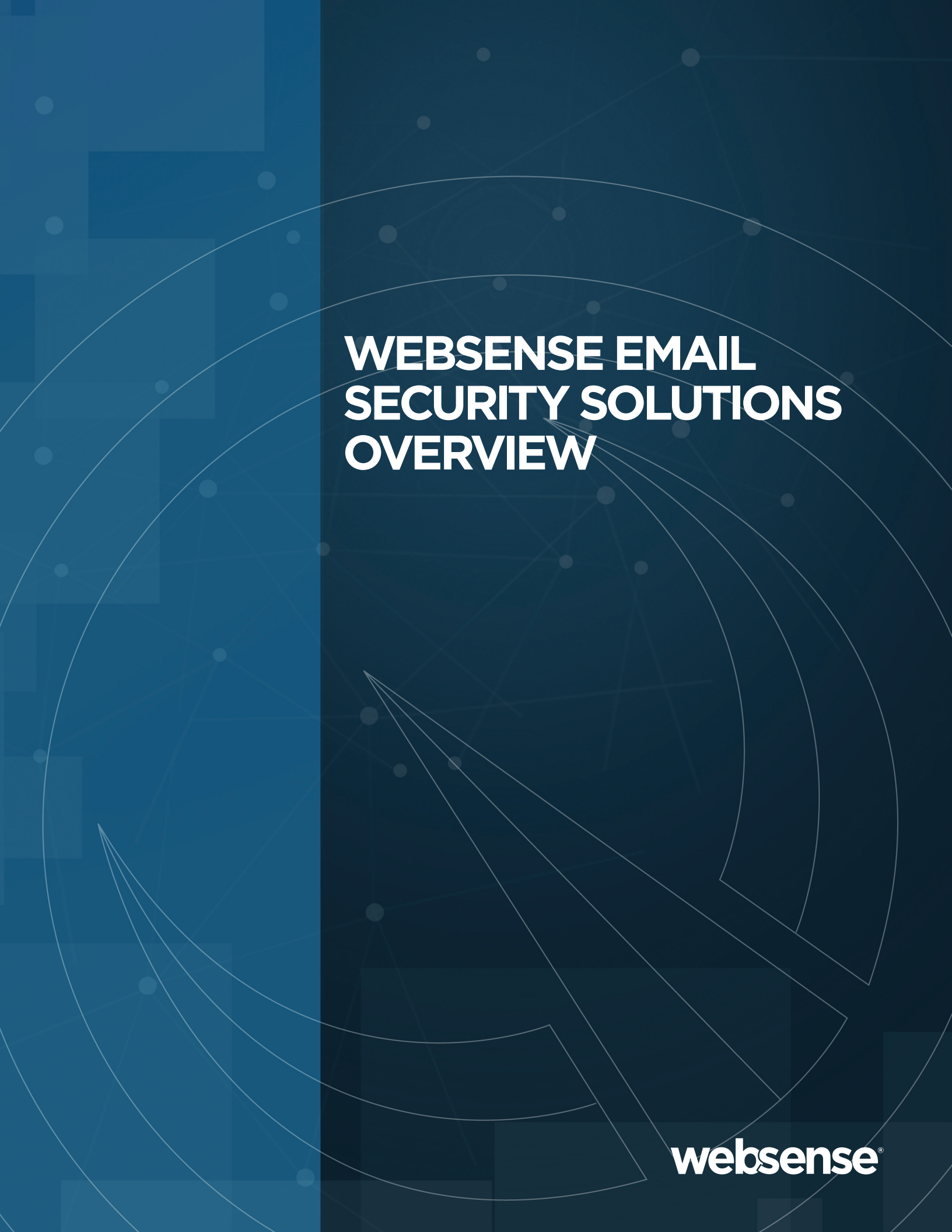
WEBSENSE EMAIL SECURITY SOLUTIONS OVERVIEW



websense®

Challenge

Many of today's biggest security compromises start with a simple email attack that exploits Web vulnerabilities. In fact, more than 92 percent of unwanted emails contain links, often to sites designed for malicious purposes.

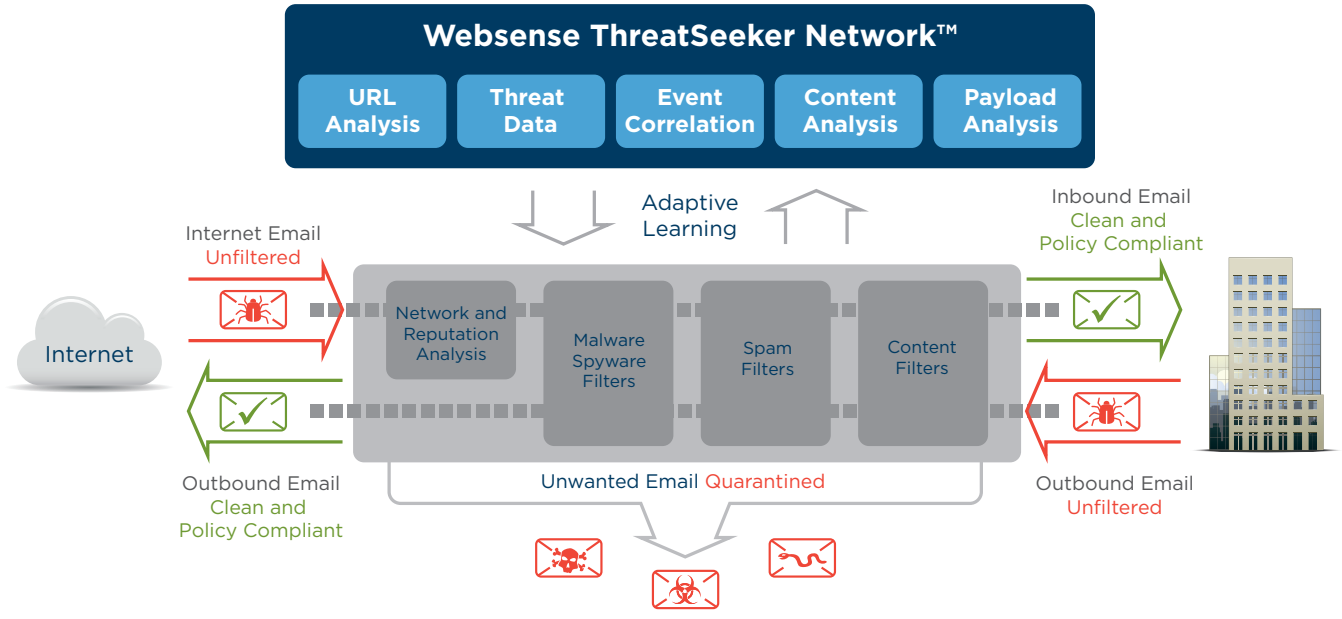
Typical email security products fail miserably to combat these modern blended threats. That's because they rely on security principles and technologies that are more than a decade old:

- Sender Email Reputation
- Lexical Analysis
- Antivirus

Solution

To defend against today's email threats, you need to have top-notched web and data security intelligence, too. Websense offers this and more with next generation email security solutions:

- **Gateway Threat Analysis** leverages security intelligence from the Websense ThreatSeeker™ Network and Websense ACE (Advanced Classification Engine) — collecting data from more than 900 million endpoints and analyzing up to 5 billion Web pages per day — to thwart advanced malware, spam, and blended threats.
- **Point-of-Click Threat Analysis** sandboxes suspicious links embedded in emails at the recipient's point-of-click.
- **Built-in Data Loss Prevention (DLP)** monitors and prevents sensitive data such as product roadmaps or customers' Personally Identifiable Information (PII) from leaving the corporate network via email.



websense®

The Websense Difference

Websense Advanced Classification Engine (ACE) uses composite scoring with predictive analysis. Combined with classifiers for real-time security, data and content analysis — the result of years of research and development — they enable ACE to detect more threats than traditional antivirus engines every day (the proof is updated weekly at securitylabs.websense.com). ACE is the primary engine behind all Websense TRITON® solutions, and is supported by the Websense ThreatSeeker Network, which collects data from more than 900 million endpoints and analyzes up to 5 billion web pages every day.

Gateway Threat Analysis

Advanced malware protection

ACE analyzes inbound and outbound email for malware, spyware, and targeted and blended threats. With real-time composite risk scoring, antimalware engines, and security intelligence from the ThreatSeeker Network, protection is provided against known and unknown threats within email.

Accurate spam detection

Websense provides highly accurate spam blocking with very low false positives that is backed by a 99% or higher SLA. A combination of identification technologies is used, including: sender reputation, connection management, adaptive learning, URL analysis, heuristics, suspicious PDF identification, and optical recognition of image spam.

Point-of-Click Threat Analysis

URL Sandboxing

Isolates suspicious links embedded in emails and analyzes the payload of the corresponding Web page at the recipient's point-of-click. Modern phishing attacks succeed primarily because phishing emails now contain embedded links that point to dynamic-IP botnets or web pages that host dynamic code — two techniques that may elude even the most robust gateway malware analysis.

Built-in Data Loss Prevention (DLP)

Policy templates and dictionaries

Pre-defined dictionaries in multiple topics and languages plus built-in PCI-DSS and data privacy templates help you quickly identify and stop email policy violations and meet regulatory requirements.

Flexible encryption

Protect sensitive and regulated data by securing email through TLS encryption for server-to-server protection. Advanced Email Encryption (optional) secures the email and any attachments from sender-to-recipient.

Websense offers multiple deployment models for email security, so that you get to choose which method makes the most sense for your organization.

Cloud

An all-cloud email security solution that saves time and money with no equipment to install or maintain, built-in resilience, predictable costs, and reduced administrative overhead.

Protecting email with Websense is easy. Simply point MX records to the Websense datacenters and email is cleansed before it reaches your network, saving bandwidth by removing spam and threats in the cloud. Websense data centers are

- Load balanced
- Redundant
- Located worldwide

Appliance

Maximum control of all policies and reporting with an on-premises appliance.

The Websense® V-Series appliances are high-performance, preconfigured, security-hardened hardware platforms designed to support flexible deployment of the Websense leading Web, email, and data security solutions. The appliances are available in two modes:

Websense V10000 – For headquarters and large office deployments.

Websense V5000 – For branch office and medium business deployments.

Hybrid

Integrates in-the-cloud deployment with an appliance for an optimal balance between scalability and control.

Feature	Cloud Email Security & Content Control (CES & CC)	Email Security Gateway (ESG)	Email Security Gateway Anywhere (ESGA)
Deployment model	**Cloud**	**Appliance**	**Hybrid**
Websense Advanced Classification Engine	✔	✔	✔
Multiple Anti-Malware Engines	✔	✔	✔
Antispam and antiphishing	✔	✔	✔
URL Sandboxing	✔		✔ (Winter 2012)
Spam filtering in the cloud	✔		✔
Service level agreements (SLAs)	✔		✔
Data Loss Prevention for Email	✔	✔	✔
TLS encryption	✔	✔	✔
Advanced Email Encryption*	✔		✔
Image Analysis/Virtual Image Analyzer*	✔	✔	✔
Managed through TRITON console	✔	✔	✔

*Optional Add-On

websense®