websense®
ESSENTIAL INFORMATION PROTECTION™

Securing the Borderless Enterprise

Websense TRITON™ Solution

The Web 2.0 Workplace:
New Opportunities, New Risks

Web-enabled technologies are reshaping the modern enterprise. Powerful, cloud-based business tools such as SalesForce.com and Workday offer new ways to create, share, and manage information. Web 2.0 applications like Google Docs and Zoho have transformed the enterprise desktop, while blogs, wikis, and social networking sites offer revolutionary new collaborative capabilities.

These innovations enable a new breed of borderless enterprise — faster, nimbler, and more responsive than ever before. Yet they also introduce dangerous new security risks.

Sites built upon dynamic Web 2.0 content — including most of today's top online destinations — are uniquely vulnerable to aggressive, fast-moving security threats. A sales staff that works with social networking sites like LinkedIn and Facebook may be exposed to script-based exploits designed to deliver malware infections. Scam artists routinely target executives with sophisticated "spear-phishing" and spam-borne attacks. Employees may view inappropriate content or post confidential business data, creating serious liability and regulatory compliance risks.

Legacy security solutions were not designed to deal with these threats. Blended Web and email attacks easily evade stand-alone antimalware tools. URL filtering and reputation-based tools may catch yesterday's threats, but they lack the speed and agility to identify threats associated with dynamic online content or attacks against legitimate Web 2.0 sites. Point-based security solutions of all types leave gaps that attackers will target and exploit.

Companies must also consider the costs associated with legacy point security solutions. Overlapping products, multiple vendors, and redundant management and reporting systems drive up ownership costs while reducing ROI. Shifting, rapidly evolving security threats demand additional software, hardware, and infrastructure investments, all of which add additional layers of cost and complexity. The resulting hodge-podge of security solutions imposes extra management and integration challenges — without significantly improving a company's overall security posture.

A unified, completely integrated security solution offers the only practical way to escape this dilemma. Such a solution will address Web and email security threats associated with new communication and collaboration tools. It will mitigate the risk of losing valuable business data through external attacks and internal leaks. It will eliminate the complexity of deploying, managing, and maintaining multiple legacy security products.

Above all, a unified content security solution will deliver better protection against modern threats at a lower total cost of ownership (TCO). It enables innovation without sacrificing security.

TRITON™

Delivers modern security with Websense TruContent™ intelligence - the first and only system that unifies content visibility and analysis all the way to the data level, as it flows in and out of an organization. Organizations are able to prevent dynamic inbound Internet threats, control unauthorized content, ensure productivity, and effectively stop outbound data loss across key channels of information exchange including Web and email.

Lowers security costs by providing the industry's first unified inbound and outbound management, reporting, and deployment model for content security technologies with in-network, Security-as-a-Service, and Websense TruHybrid™ deployment capabilities. This enables organizations to increase coverage and deployment flexibility while lowering the complexity, overhead, and cost of administering disparate systems and deployment approaches.

The Solution:
Unified Content Security

The Industry's First Unified Content Security Solution

Websense® TRITON™ is the industry's first and only unified content security solution to deliver the best modern security for inbound threats and outbound risks, combined with the lowest total cost of ownership. Websense secures the modern business even as its infrastructure dissolves and users, data, and applications move to the Web.

With Websense TRITON organizations:

Get the best modern security to

- Leverage the power of new communication, collaboration, and social Web tools like Facebook, LinkedIn, Twitter, and other cloud-based services, without threats from malware, new Web-based attacks that evade antivirus software, inappropriate content, or confidential data loss.

- Secure the use of Security-as-a-Service (SaaS) and online applications without losing visibility and control over information.

- Stop blended attacks that leverage email and the Web to compromise users, infect systems, and steal information.

**Achieve the lowest total cost of ownership by**

- Consolidating Web, email, application control, and data loss prevention management into a unified console for security across the organization.

- Consolidating security appliance infrastructure and using SaaS to reduce cost and complexity while extending coverage and visibility.

- Covering mobile workers, distributed sites, and central sites with persistent controls through one management and reporting console.

Websense TRITON is the first and only solution to provide truly unified content security designed to slash deployment and administrative costs while providing industry-leading protection. This Websense solution includes unified policy management for on-premise and cloud-based deployments spanning Web security, email security, and data loss prevention. Its hybrid deployment architecture reaches across the global enterprise, combining high-performance appliances at a corporate headquarters with SaaS at branch and remote offices.

Websense TRITON offers a number of unique capabilities:

A fast, flexible, hybrid deployment architecture that enables enterprises to protect remote offices and mobile workers just as effectively as a corporate headquarters. With a hybrid deployment:

- Security administrators set policies using a single, unified interface.

- Network administrators employ a cost-effective, cloud-based network infrastructure.

- IT executives manage risk and achieve greater security coverage at a lower TCO.
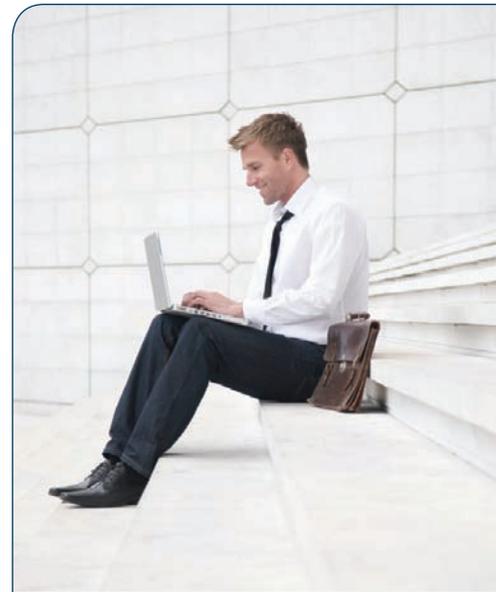
An embedded, fully scalable data loss prevention solution that combines enterprise-class outbound content inspection with the industry's leading inbound Web and email security solutions. This approach provides the granular, deep content control capabilities associated with full data loss prevention tools, integrated within a single Web, email, or combined security solution. With embedded data loss prevention:

- Security administrators implement a single, unified content security architecture.
- Network administrators eliminate the need for costly infrastructure upgrades.
- IT executives avoid the cost and complexity associated with multi-vendor solutions.

Unified policy management and reporting that enables superior control and flexibility compared to multi-vendor point solutions. A single management interface controls a company's Web, email, and data security policies, and advanced, fully customizable reporting tools provide visibility into an organization's security operations. With unified policy management and reporting:

- Network administrators gain visibility into a company's infrastructure usage.
- Security administrators streamline the policy definition and management process.
- IT executives gain real-time tools to monitor key security metrics, identify trends, and enforce compliance directives.

The TRITON Architecture: Fast, Flexible, Powerful

TRITON rolls the industry's leading Web, email, and data loss prevention (DLP) security technologies into a single content security solution, combining an integrated architecture with exceptional power and flexibility. The resulting combination of Websense technologies offers a unique and powerful set of interlocking security capabilities.

Unified Content Analysis

The Websense TRITON Advanced Classification Engine (ACE) provides a real-time threat analysis infrastructure for the TRITON solution. Powered by the Websense ThreatSeeker® Network, ACE combines multiple analytic methods, including URL filtering, antivirus, reputation services, data fingerprinting, and more, to dynamically classify both incoming and outgoing content.

Rather than relying on legacy file and database-driven detection methods, ACE performs a multipoint analysis that assesses the intent of users, Web sites, scripts, and executable code. If a banking site, for example, employs Javascript in a manner that resembles a script-based attack, ACE will instantly identify this potentially malicious activity and can prevent it.

"Websense alone leads the content security suite market because of its current functionality and suite-oriented product strategy."

Independent Report: "The Forrester Wave™: Content Security Suites, Q2 2009",

Forrester Research, Inc., April 2009
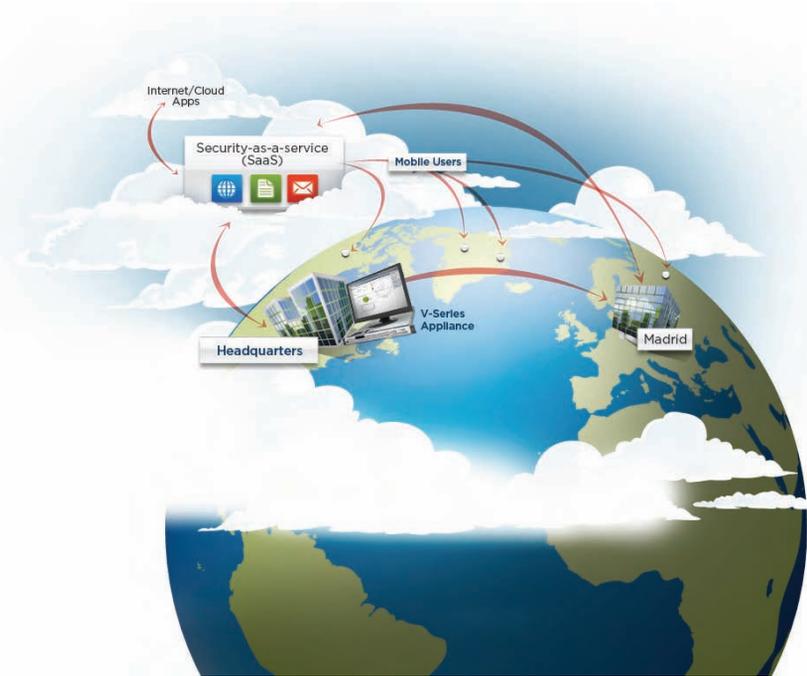
Websense TruHybrid Deployment

ThreatSeeker Network is a global network that analyzes potential security threats through the use of advanced, real-time reputation analysis and behavioral analysis techniques. It feeds newly discovered security findings to ACE, which is part of Websense Web, email, and DLP solutions.

By employing a unified content analysis model, Websense delivers real-time protection against blended and emerging threats, no matter where they reside. Customers avoid the cost and complexity of point security solutions, gain enhanced regulatory compliance capabilities, and enjoy the ability to enable new, Web-based communication and collaboration technologies.

Unified Platform

A modern enterprise network infrastructure extends far beyond a single location; it must also encompass branch offices and mobile workers. Websense addresses this challenge with a hybrid solution that integrates both cloud-based and on-premise delivery platforms. Companies are free to choose a single platform or to implement a mix that best suit their needs. In the process, a unified platform enables administrators to reduce complexity, take full advantage of existing infrastructure, and eliminate management overhead — all while reducing total cost of ownership (TCO).

Websense V-Series™ Appliance - Extensible, Simple, Powerful
The V-Series appliance delivers a unique mix of flexibility, performance, and simplicity. V-Series appliances significantly reduce deployment time and operational costs for Websense customers, yet they are scalable enough to support even the largest enterprise environments. The V-Series appliance integrates seamlessly with the Websense Security-as-a-Service (SaaS) platform, giving customers additional options for deploying and managing their content security solutions.

Security-as-a-Service – Fast, Simple, Effective
Websense SaaS provides a quick deployment path for Websense products. SaaS shifts all security inspection, enforcement, and management processes from the customer's location to 10 globally available datacenters "in the cloud." Customers gain all the benefits of the industry's leading content security solution, even as they shed the burden of deploying and upgrading on-premise hardware.

Safely Enable Your Enterprise

As more companies seek to gain a competitive edge with today's dynamic Web 2.0 technologies, their security solutions must also rise to meet new challenges. Websense offers the answer, providing the industry's first and only unified content security solution.

With Websense, organizations can build a comprehensive security infrastructure that offers complete protection against Web, email, and data security threats. They are able to minimize their exposure to security risks, maximize productivity, and enable innovation —all without introducing new sources of cost, complexity, and management overhead. A unified content security solution allows enterprises to tear down barriers to innovation and enable vital new technologies.

Unified Solution

TRITON combines the management and reporting capabilities for Websense Web, email, and data loss prevention technologies into a single interface, providing greater visibility, control, and management capabilities. The Websense TRITON Console lets users set policies, manage incidents, run reports, and perform administrative tasks from a central, Web-based manager.

Web Security

The Websense Web Security Gateway inspects inbound and outbound content, protecting businesses against dynamic Web malware, preventing sensitive data loss, and enhancing employee productivity. TruHybrid™ deployment supports on-premise appliances and SaaS while managing the entire environment from a single policy and reporting infrastructure. Unlike alternative approaches, Websense customers are free to choose a deployment option that suits their unique operational requirements, without being forced to manage multiple systems or to deal with multiple vendors.

Websense Web Security Gateway can be deployed as on-premise software, as the Websense V-Series appliance, as SaaS, or as a hybrid offering.

Email Security

With Websense email security solutions, customers are able to implement mission-critical security and to develop a consolidated security strategy with the trusted leader in Essential Information Protection™.

Websense email security protects against converged Web and email threats, including data loss and regulatory violations. Only Websense email security provides email compliance and security backed by the intelligence of the Websense ThreatSeeker Network.

Websense email security is available both as on-premise software, as a cloud-based, Security-as-a-Service (SaaS) platform, or as a hybrid deployment option.

Websense Data Loss Prevention

Websense offers the industry's leading data loss prevention technology designed to identify, monitor, and protect confidential data. Leveraging the unified content analysis delivered by Websense Web security and data loss prevention (DLP) technologies, Websense DLP solutions accurately prevent data loss, secure business processes, and manage compliance and risk.

Websense takes a modular approach to address data loss threats. Its solution delivers unparalleled visibility into who is sending sensitive data; what kinds of data are being sent; and where this data is going. Websense data loss prevention solutions empower organizations to address DLP problems at a lower cost and with less complexity than competing solutions.

Websense is the first and only company to deliver a complete content security platform that integrates all of these elements within a single, fully integrated solution. A unified solution ensures consistent policy definition and enforcement, allows an administrator to assume a security posture that meets an organization's specific needs, reduces complexity and management overhead, and provides immediate cost savings compared to an approach that relies upon redundant multi-vendor management tools.

For a free evaluation of all Websense products or to view our online demos, visit **www.websense.com/evaluations**.

websense ®
ESSENTIAL INFORMATION PROTECTION™