Bailing Out Your Budget: How Websense Lowers Your TCO

websense®
ESSENTIAL INFORMATION PROTECTION™

Table of Contents

websense®

Introduction

The unfortunate reality for today's enterprises is that IT security risks continue to escalate at the same time that the resources available to mitigate them are diminishing or, at best, remaining constant. This is particularly true for the content security domain where:

- The dynamic Web joins email as another major threat vector, and more importantly, a vector against which traditional and static countermeasures are no longer effective.
- The dangers of data loss have become greater than ever.
- A highly distributed workforce is dictating the need for a new, more cost-effective model for achieving comprehensive protection.

Complicating matters further is the need to demonstrate compliance with a seemingly never-ending collection of regulatory requirements intended to ensure the privacy and security of sensitive information.

The net result when it comes to content security is the need to do more with less. The Websense® TRITON™ solution is ideally suited to meet this need. In contrast to the legacy, point-product approach — which inevitably leads to gaps in coverage, additional layers of complexity, and spiraling costs — the TRITON solution is a unified content security solution that not only delivers better protection against modern threats but also does so with the lowest total cost of ownership (TCO). This latter characteristic is made possible by the unmatched set of strengths and capabilities the TRITON solution has to offer in four specific areas: security effectiveness, infrastructure consolidation, operational efficiency, and overall flexibility and adaptability.

websense®

The Content Security Challenge

Modern enterprises face a daunting challenge. To achieve greater operational efficiency and remain competitive, they must steadily roll out new applications, technologies, and services — often making them available not just to employees, but to external constituents as well. At the same time, however, they must also provide an effective level of protection for all of these elements — including the associated data — even as risk levels rise and resources remain constrained.

Risks Are on the Rise

Prominent drivers for content security risk include the following:

Email is still a major threat vector

Websense Security Labs™ reports that 86 percent of emails are spam. And according to Gartner, 90 percent of spam has a URL associated with it.[i] This growing prevalence of blended threats further emphasizes the need not just for email security, but for complementary Web security as well.

The dynamic Web

Widespread use of Web 2.0 technologies and services has rendered traditional content and Web security technologies, such as antivirus and URL filtering, ineffective. The dynamic nature of associated sites means that countermeasures based on periodic scanning and classification are no longer adequate. Compounding this challenge are:

> Websense Security Labs Q3-Q4 2009 report says 71 percent of websites with malicious code are legitimate sites that have been compromised.

- Many popular social networking sites and collaborative Web tools are being used not just on a personal level but also for business purposes — which means simply blocking them is not an option.

- Dynamic technologies, support for user-generated content, and, therefore, associated Web threats are finding their way into all types of sites — including ones that are generally classified as legitimate business tools and services.

Among organizations surveyed by Osterman Research in April 2010, those with 500 or fewer employees said that 31 percent of their employees used Facebook and 23 percent used Twitter for work purposes. Organizations with more than 500 employees responded that 16 percent of their employees used Facebook and 11 percent used Twitter for work purposes. – "Results of a Survey on the Use of Email, Social Networking and Other Applications," an Osterman Research Survey Report, published April 2010.

Websense Security Labs Q3-Q4 2009 report says 71 percent of websites with malicious code are legitimate sites that have been compromised.

The dangers of data loss

Rapid proliferation of mobile computing platforms, widespread use of peripheral devices, and easy access to file-sharing software have all elevated the potential for data loss — as has the rapidly growing population of Web 2.0 sites and services that support user-generated content. The result is that the Web has not only become the leading channel for data distribution but also for data loss. The potential impact to enterprises: just a single incident of data loss can tarnish brand reputation, erode a business's competitive advantage, sacrifice hard-earned customer goodwill, damage or destroy potentially irreplaceable intellectual property, and be the cause of fines or penalties from regulators.

websense®

According to Chris Christiansen, vice president, Security Products and Services at IDC, the need has never been greater for a new unified security paradigm to provide consistent protection from both inbound threats and outbound risk with single policy management for on-premise and Security-as-a-Service (SaaS) deployments across dispersed enterprises. "The Web has become the preferred platform from which cybercriminals launch their various types of complex malware attacks on individuals and businesses, because it is perceived to be an easy way to access valuable information assets."
– Websense TRITON solution press release, February 9, 2010.

The shift to a distributed workforce.
Yesterday's road warriors now have a lot of company. IDC Research predicts that by 2013, mobile workers will comprise more than one third of the world's workforce.[ii] In addition to business travelers, tens of millions of employees now work from home or from remote and branch offices at least part of the time. The implication: organizations need to find an effective and affordable way to extend their content security strategy and solution to also provide comprehensive coverage (i.e., across all of the issues noted above) for all of their mobile and remote users.

The compliance mandate
Another aspect of the challenge facing today's enterprises is the expansion of regulatory requirements, such as HIPAA and HITECH, and PCI-DSS. Demonstrating compliance with these and other local and regional legislation and industry-specific requirements is a significant undertaking. It is also one that often competes for scarce manpower and budgetary resources and for which there is no reasonable alternative — organizations that fail to comply run the risk of punitive penalties and negligence lawsuits.

Resources Remain Constrained

Unfortunately, IT security budgets are not growing at a rate commensurate with the change in risk levels. In some instances they are even shrinking. This is due in no small part to the lingering economic downturn and the challenges it presents to the majority of businesses worldwide.

> "The average percentage of IT spending that security will comprise in 2010 is 5 percent, down from 6 percent in 2009."
>
> Gartner Security & Risk Management Summit, "Security Spending in Lean Times (Droughts Don't Last Forever, But Budgeting Best Practices Should)," by Vic Wheatman, June 2010.

"The average percentage of IT spending that security will comprise in 2010 is 5 percent, down from 6 percent in 2009."

– Gartner Security & Risk Management Summit, "Security Spending in Lean Times (Droughts Don't Last Forever, But Budgeting Best Practices Should)," by Vic Wheatman, June 2010.

"Despite the enthusiasm for data security in some quarters, however, the majority of North American (59 percent) and European enterprises (51 percent) intend to keep their data security budgets at about the same levels as last year. Moreover, a small minority expects to cut budgets — unsurprising considering the current economic climate." - "Data Security Predictions For 2010," Forrester Research, Inc., December, 2009.

Additional drivers include:

- Total cost versus impact — Many organizations try to evaluate if it makes sense to make an investment by looking at whether the total cost of a security solution is relative to the anticipated total impact of a security problem. But this approach is risky because it's difficult to predict the costs related to impact given the dynamic nature of modern threats and the great number of uncertainties surrounding them and how they might affect an organization.

- A growing sense of futility — An organization may ask, "Will it really happen to me?" And "What are the chances it will?" It may decide to wait until an event occurs before reacting and investing in security solutions if it feels the chances of suffering serious security problems are low.

websense®

"Most new threats attack during periods of emerging technology, such as during the move from mainframes to client/server and Internet connectivity, or the movement from fax to e-mail. However, another important class of threats attacks complacency with, or trust in, technology that comes about after long-term use. For example, e-mail viruses began to attack the trust users had when receiving e-mail that appeared to come from someone they know. The worms attacked complacency in not patching Windows PCs and servers. Phishing attacks exploit trust in popular name brands, and now attacks are beginning to go after users' trust in sites such as MySpace and YouTube." – Gartner Security & Risk Management Summit, "Cyberthreats and the IT Security Market Clock," by John Pescatore, June 2010.

Economic turmoil and the resulting job losses and hardships may also cause otherwise "good" people to make poor decisions, such as removing sensitive data from employers in their efforts to secure new employment or enhance their future in some way.

Point Products Present a Major Problem

With risks on the rise and resources remaining constrained, the bottom line is simple: when it comes to securing their computing environments, most enterprises must find a way to get more done with less. In this regard, the traditional point product approach — still in use by many of them — is an extremely poor fit. Such an approach typically requires:

- Multiple, separate products to account for different security functions (e.g., access control, antimalware, intrusion prevention) or each different domain (e.g., Web, email, data). Note: although there has been some consolidation in recent years, with many functions for a given domain coming together into a single solution for example with Web security gateways and email security gateways — such consolidation is not always available, and neither is it sufficient.

> "DLP policy synchronization is one of the primary reasons for integration of Web and e-mail security gateways; however, this capability is still rare — even among providers with both solutions."
>
> Gartner, Magic Quadrant for Secure Web Gateway, Jan. 8, 2010.

- Multiple, separate instances of each product — typically either in the form of hardware plus software, or perhaps appliances — to account for each site or location where users need to be protected. Note: alternately, organizations can elect to backhaul traffic from remote offices to central ones where they are already deploying appropriate content security solutions. However, this typically incurs a significant latency penalty, results in paying double for bandwidth for all Internet traffic, and, therefore, is becoming less attractive as Security-as-a-Service (SaaS) and other developments continue to drive up the quantity of such traffic.
- One or more software-based security clients for every mobile device, which may be greater than the number of mobile users, and may not even be possible due to the steady proliferation or diversity of such devices and relatively spotty support and coverage provided by vendors of the corresponding security software.

Given these characteristics, it's not difficult to see that this approach is extremely costly and, in most cases, unsustainable. Practically every new technology, type of threat, corporate office, and mobile user that comes along leads to the purchase of another product. Not only that, but the enterprise has to juggle numerous vendor relationships, train its security staff across a plethora of products, and deploy, operate, maintain, support, and ideally integrate all of those disparate products and systems as well.

websense®

Enterprises incur further costs based on having to manage around steadily mounting infrastructure or system complexity and inevitable gaps in functional capabilities (or that are introduced by inconsistent and non-overlapping policies). Add to that the costs of having to manage a relatively brittle "solution" that is difficult to adapt to changing conditions — such as greater user mobility, adoption of cloud computing, or geographic expansion.

"As the case with many security technologies today, content filtering as a standalone solution is becoming an increasingly difficult sale. Customer expectations are trending towards the view that content filtering is part of a larger picture, and should be an integrated part of a holistic security offering." – Frost & Sullivan, World Content Filtering Markets, Jun 2009.

"We have been advising buyers to consider secure email gateways (SEG) and secure Web gateway (SWG) purchases together to save costs and improve DLP and communications policy reuse across these two critical channels. As more and more communication traffic moves to Web-based channels, such as social networking, instant messaging, voice over IP (VoIP) and Web conferencing, managing and securing these channels will necessitate improved convergence between these tools."
– Gartner, Magic Quadrant for Secure Email Gateways, April 27, 2010.

"DLP policy synchronization is one of the primary reasons for integration of Web and e-mail security gateways; however, this capability is still rare — even among providers with both solutions."
– Gartner, Magic Quadrant for Secure Web Gateway, Jan. 8, 2010.

websense®

Introducing the Websense® TRITON™ Solution

The Websense® TRITON™ solution is the first and only solution to combine industry-leading Web security, email security, and data loss prevention security technologies into one unified architecture. The TRITON solution delivers increased content security and cost savings, helping organizations efficiently defend their computing environments from aggressive, fast-moving threats and enabling them to leverage all the benefits of Web 2.0 — unlike point solutions that rely on redundant, multivendor management tools.

Compared with such limited and restrictive solutions, the TRITON architecture also enables superior control and flexibility, providing unrivaled visibility into an organization's security operations, and protects remote office and mobile workers just as effectively as it would protect workers at corporate headquarters. The result: the TRITON solution provides today's enterprises with the best security for modern threats at the lowest total cost of ownership (TCO).

But how exactly is this possible? In particular, how does the TRITON solution achieve the lowest TCO? The answer lies in the TRITON solution's strengths and capabilities in four specific areas: security effectiveness, infrastructure consolidation, operational efficiency, and overall flexibility or adaptability.

In addition, two key points to keep in mind as we explore each of these areas are that:

- It's not a matter of some competitor's solutions having some of the same features and capabilities; rather that none of their offerings have all of them, like the Websense TRITON solution does.
- Initial purchase price is only one small piece of the TCO equation.

Security Effectiveness

One of the greatest contributing factors to TCO is a security solution's effectiveness or the visibility, control, and stopping power that it provides. Products that are unable to consistently prevent both known and unknown threats with a high rate of success will ultimately cost an organization dearly. Each negative outcome entails the need for "cleanup," including identification and remediation or restoration of all systems that were impacted. Major incidents can also lead to substantial costs in the form of customer notifications, lost data, regulatory fines, punitive damages, loss of customer confidence, and loss of competitive advantage.

Consider these related statistics:

- The costs associated with a malware infection are approximately $60 per endpoint for remediation and another $50 per user in terms of lost productivity.[iii]
- The average cost of an ordinary security breach is approximately $49,000.[iv]
- For security breaches involving the loss of customer records, the average total per-incident costs in 2009 were $6.75 million (or approximately $204 per compromised customer record).[v]

The TRITON solution helps organizations minimize and avoid such costs by delivering unmatched security effectiveness in the following ways:

- **Broad and comprehensive threat and domain coverage.** With the TRITON solution, Web security, email security, application control, *and* data loss prevention are all provided in a single, unified solution.
- **Comprehensive and uniformly strong capabilities for each domain**. Each module or component of the TRITON solution is a market-leading, enterprise-class solution in its own right, providing essential scalability across a full set of protection mechanisms. For example, Websense

websense®

Web Security incorporates integrated antivirus, real-time security scanning, Web filtering with advanced reputation analytics, real-time content classification for Web 2.0 employee productivity, extensive application control, SSL visibility, enterprise-class data loss prevention, protocol and bandwidth controls, and full proxy/caching capabilities.

- **Cross-domain analysis/integration**. With Websense TruContent™ intelligence, information gained from one domain or discipline is effectively used to benefit the others. For example, organizations can create DLP policies that account for the reputation of an intended Web destination. Similarly, they can make the email security module aware of URLs that lead to sites hosting malicious code. This way, the solution as a whole is better able to counteract blended threats and achieves a higher level of effectiveness, especially compared to the point-product approach.

- **Real-time scanning and analysis**. The Websense Advanced Classification Engine (ACE) includes real-time analytics that enable detection of zero-day threats by identifying malicious content "on the fly," without the need to reference databases for previously known attacks.

- **Real-time content classification**. ACE further incorporates the ability to accurately extend acceptable use policies to dynamic Web 2.0 sites by classifying content elements within each Web page "on the fly." If an individual content element violates policy, it can be stripped from the page while compliant information is allowed. The result: organizations can leverage Web 2.0 sites and services for business purposes while maintaining productivity and compliance with corporate policies.

- **Real-time threat intelligence**. Websense ThreatSeeker® Network, a collection of over 50 million systems, continuously analyzes potential security threats through the use of advanced, real-time reputation analysis and behavioral analysis techniques. Newly discovered findings are automatically distributed to all Websense Web, email, and data security modules.

- **Consistent policy enforcement**. Websense TruHybrid™ deployment helps eliminate gaps in an organization's security coverage by ensuring that policies and other configuration details are uniform across the different platforms a customer chooses to implement.

As for the impact of all of these features and capabilities, the following independent test results clearly demonstrate that the TRITON solution provides unmatched levels of security effectiveness.[vi]

Averages of Percentage Blocked Values for Malware Threat Types
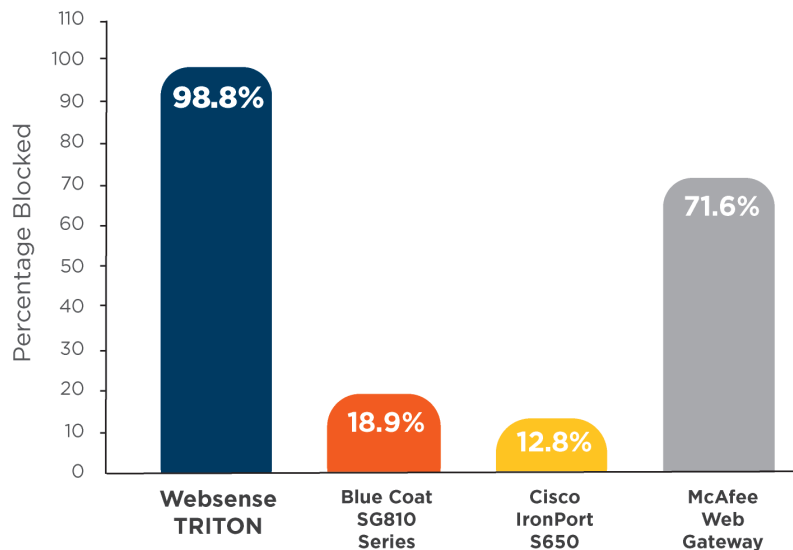
Source: Miercom, May 2010

websense®

Comparing the Websense TRITON solution to the Cisco IronPort solution in this case, the resulting financial impact is essentially incalculable (for every 1.2 pieces of malware the TRITON solution misses, Cisco IronPort misses 87.2, resulting in the potential for infection that is approximately 73 times greater with the Cisco solution).

Effective Consolidation

TCO is also driven in large part by the number of disparate products needed to fashion an overall solution. With *effective* consolidation, organizations can *safely* reduce this number, thereby generating savings in several ways (e.g., by having fewer physical systems to purchase, implement, integrate into the network, power, cool, provide space for, integrate with each other, and manage). And to be clear, the distinction being called out here is absolutely critical: *Simple* consolidation — where multiple capabilities and products are mashed together into one physical device and the "combining" only takes place on the surface — is only partially helpful. In comparison, *effective* consolidation, characterized by "combining" that takes place at the software and management layers as well, is what allows organizations to achieve maximum gains.

> The annualized TCO of Websense Hosted Email Security at a typical midsize company is less than one-third the cost of a comparable on-premise email security solution.[vii]

The TRITON solution delivers a high degree of *effective* consolidation by providing:

- **Unified enforcement infrastructure**. Enterprises are relieved of the burden of having a separate device for each part of their content security solution. For example, Websense Web Security Gateway Anywhere, part of the TRITON solution, incorporates Websense enterprise-class DLP technology as an embedded component. The impact: IT can implement Web security and Web DLP with half as many devices.

- **Unified management infrastructure**. The TRITON Console currently combines management for Websense Web Security and DLP solution modules, and in the future, will combine Websense email security too. The impact: IT can reduce the number of management systems that are required.

- **A Security-as-a-Service (SaaS) option**. With the TRITON solution, customers have a choice of platform: on-premise, SaaS, or a hybrid approach (which combines both on-premise and SaaS options, but effectively manages them as one). One of the cost savings benefits of the SaaS approach in particular is the relief it can provide for Internet bandwidth and other related infrastructure. For example, filtering spam and other email-borne threats in the cloud can easily trim inbound email traffic by 80 percent or more, thereby reducing bandwidth and capacity requirements for devices and systems that would otherwise need to process all of this traffic when using an on-premise solution. Even more significant, is that the SaaS approach unburdens enterprises of numerous tasks and investments, shifting ownership and responsibility to the service provider — who can accomplish them in a manner that results in substantial savings (primarily due to the economies of scale they can achieve). For example, with SaaS, enterprises can:
  - Eliminate the distribution, deployment, and ongoing maintenance of on-premise hardware, which is especially attractive for shops with numerous branch offices.
  - Eliminate the need for associated networking infrastructure (e.g., switch ports), rack space, power, and cooling capacity.
  - Eliminate the need to invest in "overhead" capacity (for bandwidth, content security devices, and related infrastructure) to account for spikes in activity.

websense®

- Eliminate the need to invest in additional hardware or systems to achieve high availability and disaster recovery objectives.

The last item from this list, the availability of a SaaS option, is particularly powerful from a cost-savings perspective. As the following graphic illustrates, the annualized TCO of Websense Hosted Email Security at a typical midsize company is less than one-third the cost of a comparable on-premise email security solution.[vii] The difference in labor costs alone is sufficient to justify the use of SaaS, although other factors, including the virtual elimination of hardware costs, also play a major role.

Cost of Ownership (On-Premise vs. Hosted)
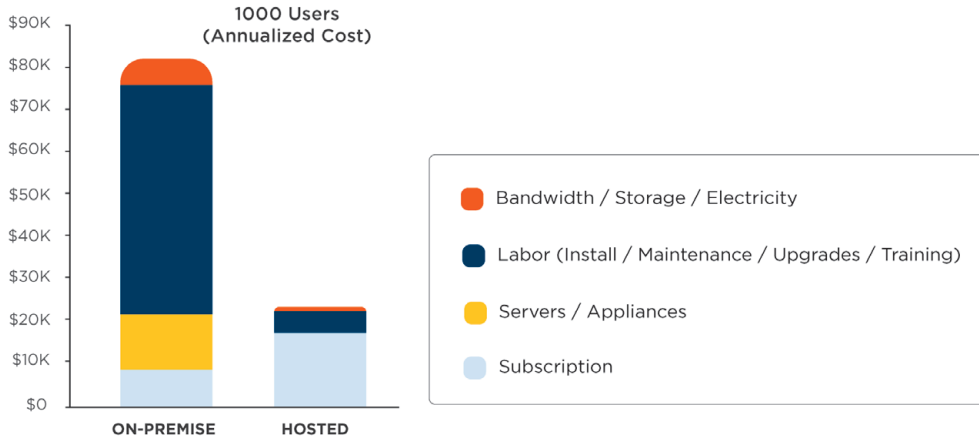
Source: "The Advantages of a Hosted Security Model," Osterman Research, July 2009.

Organizations can also achieve major savings by adopting a hybrid approach, where they employ an on-premise appliance to service users at a headquarters facility and engage a complementary cloud-based offering to support all remote users. As illustrated below, compared to an all on-premise solution, a hybrid approach can yield a savings of 43-45 percent over a period of three years, depending on the size of the organization.[viii]

Hybrid Web Security Cost Comparisons
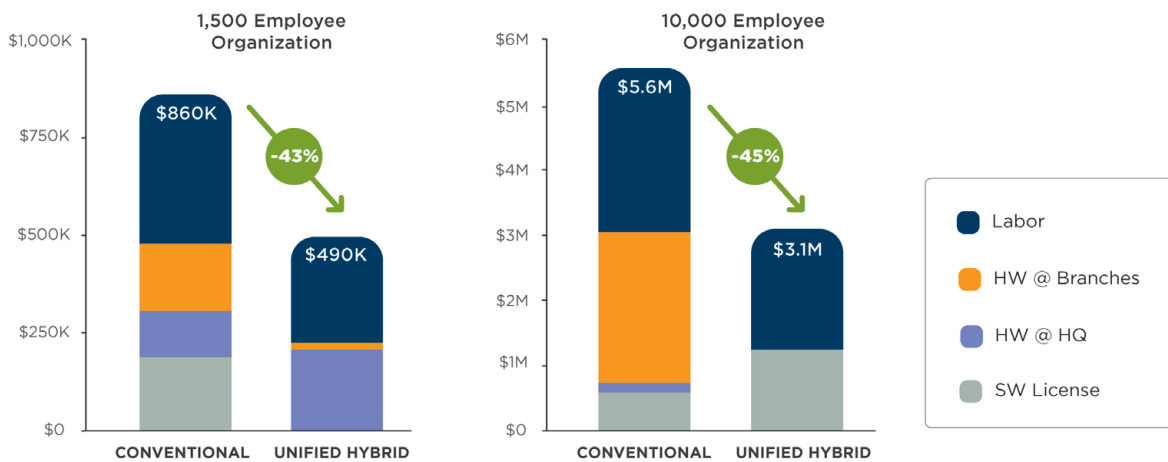
Source: "The Cost Benefits of a Hybrid Approach to Security," Osterman Research, February 2010.

websense®

Operational Efficiency

Whereas consolidation involves making do with fewer physical resources, operational efficiency is all about reducing the burden on and need for personnel. The primary aspects of operational efficiency center on ease of managing the overall solution and its capacity for automation.

The TRITON solution delivers exceptional operational efficiency by providing:

- **Unified administration**. Availability of the TRITON Console means that operators can seamlessly manage Web, email, application control, and data loss prevention policies and reports from a single interface, without having to bounce between numerous different management applications. Moreover, TruHybrid deployment means that management tasks are also unified across whatever combination of platforms customers choose to use, on-premise or SaaS or a combination of these deployment options. This greatly simplifies operational tasks, ensures consistent and thorough implementation of policies, and contributes to even greater levels of overall security effectiveness by enabling superior visibility and control compared to multivendor point solutions.

- **Delegated administration**. Granular, role-based administration capabilities allow selective delegation of management functions and their scope of coverage. Organizations can use these to improve security team efficiency by enabling certain tasks, such as dealing with misuse violations, to be offloaded to local administrators or business unit managers.

- **Numerous ease of use capabilities**. The TRITON Console includes numerous time-saving features that support both initial implementation and ongoing operation of a unified content security solution, such as deployment wizards, configuration templates, pre-defined policies, an intuitive user interface with guided help throughout, dashboards with integral drill-down functionality, structured workflows for common processes, advanced forensics capabilities, and a library of pre-defined reports.

- **Automated content updates *and* feature enhancements**. Security updates pertaining to new threats, site classifications, application signatures, and so forth are automatically delivered as they become available. With the SaaS option, the same benefit also applies for new features and upgrades. The impact: a reduction in administrative effort at the same time that security effectiveness is bolstered even further.

- **Automated, granular response and remediation**. The TRITON solution can be configured to automatically respond to content security events in a myriad of ways, including notification, encryption, quarantining, blocking, removal of offending material, logging, and enforcement of time quotas, bandwidth limitations, or time-of-day restrictions. The impact: rather than simply restricting "business," IT can securely enable it, in a low-impact, low-effort manner.

- **Automated reporting**. The creation and distribution of all types of reports — whether to support ongoing operations, detailed analysis of activities, periodic compliance checks, or high-level oversight — can be fully automated, enabling a set-and-forget model without sacrificing visibility.

- **An adaptive and automated feedback loop**. Administrators can save time by quickly and easily logging misclassified content (e.g., URLs, data) in the management GUI. Not only will their system account for the change going forward, but the corresponding information will automatically be sent to Websense for review and reclassification.

Another major advantage for the TRITON solution that helps deliver even greater operational efficiency — among its many other advantages — is Websense Global Technical Support. With **Global Technical Support**, TRITON solution customers are assured of getting the assistance they need when they need it, without having to make numerous calls to numerous vendors, particularly since the entire solution is provided by a single vendor, Websense. Websense provides top-quality support to help resolve all technical issues. Websense technical support personnel have expertise spanning all life cycle phases, from architectural design to physical deployment, integration, policy development, and all aspects of ongoing

websense®

operations. Not only that, but by delivering complete control over case management and easy access to tools like Knowledge Base, support forums, and the MyWebsense portal, the award-winning Websense eSupport makes it even more efficient for customers to deploy and manage the TRITON solution.

Flexibility and Adaptability

The flexibility to seamlessly support a wide variety of use cases and different network configurations and the adaptability to remain applicable despite changing conditions or requirements are the keys to having an excellent level of investment protection. In contrast, solutions that are anchored to a given platform, difficult to upgrade, or unable to accommodate step-function increases in demand and changing operational models (e.g., the adoption of cloud computing or greater workforce distribution) will ultimately drive content security expenditures higher due to their significantly shorter period of usefulness.

The TRITON solution delivers extensive flexibility, adaptability, and solution longevity by providing:

- **Extensive breadth of user or scenario coverage.** The TRITON solution's hybrid deployment architecture enables best-fit coverage across the global enterprise, combining high-performance appliances at corporate headquarters and other highly populated facilities with SaaS. It provides coverage for remote and branch offices, telecommuters, and road warriors. The impact: IT avoids costly alternatives, such as employing a collection of different products to establish complete coverage, implementing appliances at each corporate location, or backhauling remote traffic to a central site for inspections and policy enforcement purposes.

- **An extensible architecture.** The TRITON architecture, particularly with its SaaS platform, can accommodate major upgrades and the addition of entirely new capabilities, as new requirements and types of threats arise, without the need for forklift upgrades, replacements, or having to deploy additional devices.

- **Dynamic scalability.** Processing through SaaS automatically scales with demand, and can even be used to augment on-premise implementations that are at or near capacity — all without having to purchase and implement additional hardware. Seamless application of policies and management capabilities across the different platforms ensures uniform protection and a consistent experience for users and administrators alike.

- **Compatibility with existing solutions.** Websense SaaS offerings can be used to complement the functionality of existing on-premise content security solutions, thereby allowing organizations to squeeze every last dime from investments that have already been made. Extensive integration capabilities further ensure maximum leverage and value is derived from existing infrastructure and solutions (e.g., for user authentication, security management, compliance management).

- **Support for future enterprise initiatives.** As enterprises evolve their IT solutions to take advantage of new technologies (e.g., virtualization) or operating models, such as full-on migration to a cloud computing or Security-as-a-Service approach, the choice of platform provided by the TRITON solution ensures continued applicability of the Websense solution, obviating the need for additional content security investments. This holds true for business initiatives as well, such as geographic expansion or mergers and acquisitions, where Websense SaaS enables organizations to rapidly establish coverage for new offices and locations without having to distribute, deploy, and maintain a bunch of on-premise hardware.

websense®

The Right Solution at the Right Time

"In Gartner's 2010 annual survey of 1,586 CIOs from 27 industries and 41 countries, CIO respondents reported that their CEOs and the business expect IT to place a higher emphasis on raising productivity in 2010 (see Figure 4). The combination of business process, information and workforce changes influences enterprise operations, raises productivity and produces business results. These three productivity levers are also key to enhancing the capabilities needed in a recovering economy."

- Gartner, "The 2010 Gartner Scenario: The Current State and Future Directions of the IT Industry," by Ken McGee, June 14, 2010.

Figure 4. Business Expectations for 2010:
Greater Productivity and Continued Cost-Efficiencies

Business Expectations	Ranking of business priorities CIOs selected as one of their top five priorities in 2010, and projected for 2013						
Ranking	2010		2009	2008	2007	2013
Improving business processes	1	↔	1	1	1	2
Reducing enterprise costs	2	↔	2	5	2	8
Increasing the use of information/analytics	3	↑	5	8	7	5
Improving enterprise workforce effectiveness	4	↑	3	6	4	7
Attracting and retaining new customers	5	⇩	4	2	3	3
Creating new products or services (innovation)	6	↑	8	3	10	1
Managing change initiatives	7	↑	6	12	*	12
Expanding current customer relationships	8	⇩	7	9	*	9
Consolidating business operations	9	↑	11	13	*	16
Targeting customers and markets more effectively	10	↑	9	7	*	10
Supporting regulation, reporting and compliance	11	⇩	12	14	13	15
Creating new sources of competitive advantage	12	⇩	13	11	8	4
Expanding into new markets or geographies	13	⇩	10	4	*	6

*New question

Source: Gartner (June 2010)

The Websense TRITON solution helps address all three of these priorities, delivering the right solution at the right time.

[i] Gartner Security & Risk Management Summit, "Email Hygiene – Don't Forget to Floss," by Peter Firstbrook, June 2010.
[ii] "Worldwide Mobile Worker 2009-2013 Forecast," IDC Research, #221309, February 2010.
[iii] "Cloud-Client Enterprise Security Impact Report," Osterman Research, January 2009.
[iv] ibid.
[v] "U.S. Cost of Data Breach Study, Ponemon Institute," January 2010.
[vi] "Detailed Competitive Testing of the Websense Web Security Gateway 7.5," Miercom Lab Testing Detailed Report DR100412D, May 2010.
[vii] "The Advantages of a Hosted Security Model," Osterman Research, July 2009.
[viii] "The Cost Benefits of a Hybrid Approach to Security," Osterman Research, February 2010.

websense®