



A Websense® White Paper

Seven Criteria for Evaluating Security-as-a-Service (SaaS) Solutions

Table of Contents

| | |
|--|----|
| Introduction..... | 3 |
| The Security Landscape..... | 4 |
| The Evolving Threat Environment..... | 4 |
| The Dangers of Data Loss..... | 4 |
| The Shift to a Distributed Workforce..... | 5 |
| Lingering Economic Challenges..... | 5 |
| Legal and Regulatory Concerns..... | 5 |
| SaaS for Web and Email Security..... | 6 |
| Reliability: The Buck Stops Here..... | 6 |
| Effectiveness: Protecting Against Modern Threats..... | 7 |
| Performance: Taking It Up a Notch..... | 8 |
| Flexibility: Growing Your Current Solution | 8 |
| Control: You Call the Shots..... | 9 |
| Privacy and Security: SaaS Can Keep a Secret..... | 10 |
| Cost: A Core Benefit of the SaaS Platform | 10 |
| SaaS solutions can significantly reduce total cost of ownership (TCO). | 10 |
| Labor costs. | 11 |
| Non-labor costs..... | 12 |
| Paying the on-premise risk premium. | 12 |
| The price of failure. | 12 |
| The cost of complexity..... | 12 |
| Conclusion..... | 13 |

Introduction

The volume and complexity of Web, email, and data security threats today pose a huge security challenge for organizations, and many lack the resources to address these threats effectively. The growing number of mobile workers, economic constraints, and regulatory compliance compound the security dilemma. Security professionals are left wondering where to turn for the right solution.

One technology that is meeting these challenges head on is Security-as-a-Service (SaaS). SaaS is increasing in popularity as an effective and lower total-cost delivery platform. Organizations of all sizes are now looking to SaaS to reduce the cost of deploying and managing Web and email security across their headquarters, branch offices, and mobile workforce. Advances in cloud computing and the increased capacity and functionality of cloud-based services have led to a significant increase in the adoption rate for SaaS. In an independent survey by Forrester Research, Inc. of IT services buyers, approximately one-fifth said they use SaaS. Of these, nearly one-half said they were expanding their deployment in 2009. An additional 26 percent of respondents were considering or piloting SaaS.ⁱ

Despite this upward trend, some organizations remain reluctant to adopt SaaS due to concerns that it does not provide the same coverage, reliability, and control as on-premise platform-based solutions. But an effective SaaS solution is entirely capable of addressing these concerns. The introduction of a hybrid deployment model that has unified administration is an example of such a solution. This model enables the simultaneous deployment of on-premise and cloud-based services at different points in the enterprise — providing comprehensive protection along with control via a single management interface. (We'll have more on this model later.)

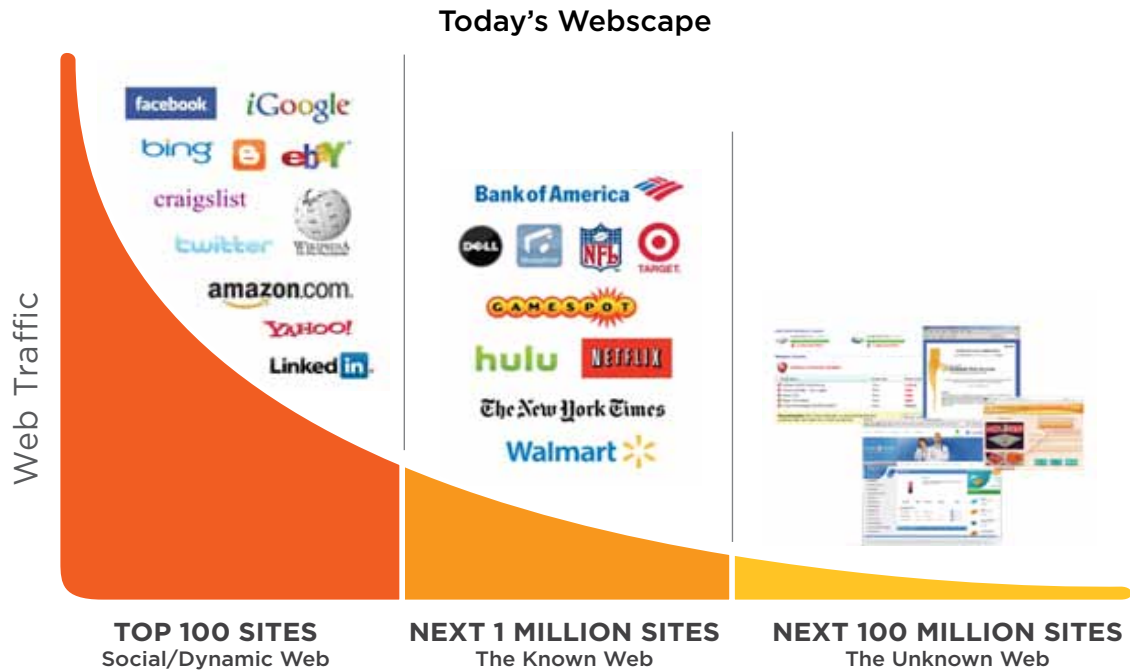
This white paper will examine the security challenges organizations are facing today; address misconceptions about SaaS; and provide criteria to help you evaluate SaaS solutions.

The Security Landscape

The Evolving Threat Environment

Today's dynamic, interactive technologies like email and the Web come with blended threats that are from multiple sources. According to the Messaging Anti-Abuse Working Group, 72 percent of all email traffic in 2005 was spam; that figure is now above 90 percent.ⁱⁱ At the same time, Websense Security Labs™ estimates that 85 percent of all spam contains URLs that often lead to malicious Web sites, the method of choice for delivering malware to unsuspecting users.ⁱⁱⁱ

The Web security landscape looks equally grim. Staying ahead of malicious Web content is a losing game for most companies. The reality is that many of today's threats are even on legitimate Web sites and many security solutions, such as antivirus protection, are no longer adequate. According to the Security Labs report for the latter half of 2009, 71 percent of Web sites with malicious code were legitimate sites that had been compromised, and 95 percent of user-generated posts on Web sites were spam or malicious.



Source: Alexa Internet, Inc., January 2010.

Companies are deploying a growing array of on-premise security solutions to counter these threats. These solutions can be highly effective, but they may often impose additional cost, complexity, and infrastructure requirements that many organizations simply cannot meet. These on-premise solutions also frequently require timely performance updates, system maintenance, and other administrative tasks.

The Dangers of Data Loss

With rapid proliferation of mobile computing devices, widespread use of peripheral devices, and easy access to file-sharing software, the risk of data loss is another growing threat. 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 assets, and result in fines or penalties from regulators. Data loss can occur within an organization from malicious attacks and employee negligence. Many incidents occur via the Web. According to Websense Security Labs, in the second half of 2009, 58 percent of all data stealing attacks were conducted over the Web.

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 a third of the world's work force.^{iv} In addition to business travelers, tens of millions of employees now work from home or from remote offices at least part of the time.

This trend has major IT security implications. Companies with existing on-premise Web and email security solutions must either find ways to extend their security umbrella to protect remote workers or simply accept the risks associated with a distributed and largely unprotected workforce. The second option is clearly unacceptable.

Lingering Economic Challenges

Given the current economic downturn, many IT organizations are under pressure to reduce spending and re-allocate resources to support revenue-generating projects. This means IT staff must do more with less and are likely to value security solutions with streamlined management and reduced maintenance and complexity.

The need to do more with fewer IT resources is especially frustrating when organizations weigh the opportunity costs involved with Web and email security initiatives. These initiatives add no value to a company's strategic business activities, yet it is simply too risky to eliminate them, given the potential consequences of a successful malware attack or data breach incident.

Economic turmoil is also a major driving factor behind many Web- and email-based attacks, such as phishing schemes in which the attacker masquerades as a trustworthy entity in an attempt to acquire valuable data like credit card information. Attackers are becoming highly sophisticated in not only who they target but also in the social engineering tactics they use to trick their victims into disclosing credentials, running a malicious file, or visiting an infected Web site.

Legal and Regulatory Concerns

Another challenge facing IT decision makers is the expansion of regulatory compliance requirements. Health care data privacy legislation requires even firms that do business with health care providers to meet rigorous data security and privacy requirements. (See the Websense white paper "Using Data Loss Prevention for Health Care Compliance" at www.websense.com/assets/white-papers/using-data-loss-prevention-for-healthcare-compliance-en.pdf.) And while industry standards such as the Payment Card Industry Data Security Standard (PCI DSS) may not carry the force of law, they can still have a major economic impact on businesses that do not comply. Companies that fail to protect sensitive information such as customer records or third-party intellectual property are increasingly likely to run the risk of negligence lawsuits.

SaaS for Web and Email Security

Security solutions using a Security-as-a-Service platform offer a number of features that allow organizations to address these and other pressing concerns. Quite a few companies are already aware of the advantages of a SaaS solution. Many other organizations, however, continue to resist the idea of outsourcing their Web and email security requirements.

Decision makers generally have the most serious concerns about the following seven items and often have misconceptions about how SaaS addresses each one. IT decision makers should evaluate a SaaS vendor's effectiveness in dealing with each of these criteria and the vendor's ability to offer a truly compelling alternative to an on-premise security solution.

- Reliability
- Effectiveness
- Performance
- Flexibility
- Control
- Privacy and Security
- Total Cost of Ownership (TCO)

Reliability: The Buck Stops Here

What upsets IT managers more than unplanned downtime? Unplanned downtime that they are powerless to remedy.

In a nutshell, this explains why so many organizations are reluctant to trust a SaaS provider. If the provider's service goes down, they will find themselves cut off and unprotected. Their email won't arrive, or perhaps it *will* arrive as a torrent of spam, malware, and phishing scams. Such a failure could quickly overwhelm a company's on-premise mail servers and network infrastructure, and it will open the door to a host of Web-based security threats and internal data loss risks.

It is not enough to minimize these risks — an effective SaaS solution must *eliminate* them. In order to accomplish this task, a SaaS vendor's data center infrastructure must be:

- **Geographically dispersed and physically redundant.** Even if a disaster destroys an individual data center, the remaining sites have the capacity and functionality to provide uninterrupted service.
- **Physically secure.** Each data center must employ redundant power and cooling systems, physical access control, server clustering, multiple Internet uplinks, and other security measures.
- **Designed for maximum efficiency.** The provider should be capable of routing customer traffic to the most appropriate data center, based on geographic location and Internet traffic conditions. This is an especially valuable capability for companies that must secure remote offices and mobile workers.

Websense® Security-as-a-Service for Web and email illustrates the reliability benefits of a carefully designed data center infrastructure. Websense maintains 10 redundant, load-balanced data centers spread around the globe. Email traffic is routed to multiple data centers, each of which provides enough capacity to meet customer demand. Websense SaaS customers also gain all the benefits of market-leading Web and email security, while eliminating the need to deploy and support on-premise or remote clients.

By shifting all management and enforcement processes to these data centers, Websense is able to reduce operational costs for its customers. Other benefits of Websense data centers include redundant power with gas-fired generators and redundant cooling, separate wiring paths, multiple high-speed Internet connections, and fault-tolerant equipment clusters with automatic fail-safe capabilities.

Effectiveness: Protecting Against Modern Threats

Legacy email and Web security solutions are highly effective when they address known threats. Today, however, these types of threats represent just the tip of the security iceberg. An avalanche of zero-hour threats, including new malware variants and compromised malicious Web sites, will quickly overwhelm software solutions designed to incorporate regular, periodic updates to their antivirus definitions or URL databases.

Truly effective Web and email security solutions provide unified content security that addresses a real-time threat environment with real-time threat detection and assessment tools as well as including data loss prevention (DLP) capabilities. They should also provide a unified platform with unified management for on-premise and SaaS platforms so security policies can be applied and enforced equally across dispersed enterprises.

These tools, in turn, rely upon three important capabilities:

- **A scalable threat assessment infrastructure.** The ability to recognize zero-hour threats depends largely upon a provider's ability to collect, classify, and correlate massive quantities of security intelligence data. This includes data gathered from existing customers, automated Web scanning tools, "honeypot" systems, and human security researchers. Given very large statistical samples and advanced analysis tools, a provider can detect under-the-radar threats and deploy suitable countermeasures.
- **Real-time threat response capabilities.** Intelligence-gathering efforts are an exercise in futility unless a provider can deliver the results to its customers before zero-hour threats breach their internal networks and threaten their users.
- **A single management interface.** A single interface will result in greater efficiencies, visibility, control, and management over combined Web, data, and email security technologies and will deliver unified content analysis and management.

The first capability is essential for any successful SaaS security solution. The second capability is where the SaaS platform truly demonstrates its value. The third capability unifies policy management and reporting infrastructure across SaaS, on-premise, and hybrid deployment models and allows organizations to set persistent security policies across geographically dispersed offices and remote workers.

Every Websense Web and email security product, including those using both on-premise and SaaS platforms, takes advantage of the Websense ThreatSeeker® Network, the company's underlying threat assessment infrastructure. Currently, up to 60 percent of the daily threats that the ThreatSeeker Network detects are not yet associated with antivirus signatures — representing a total of 250,000 new threats each month that legacy antivirus products cannot catch.^v

In terms of sheer volume alone, these figures give a new meaning to the term "real time." No matter how effectively an on-premise solution automates the security update process, the process of pushing out updates may represent a significant IT management burden and a potential source of risk for customers. Websense SaaS Web and SaaS email security solutions, by comparison, speed and simplify the process of turning real-time threat assessment capabilities into real-time protection.

For the best security against modern threats at the lowest total cost of ownership, Websense offers the Websense TRITON™ Solution, which combines Websense Web, data, and email security technologies into a single architecture with unified content analysis and management. This includes real-time content classification for analyzing content "on the fly," along with real-time content scanning that can identify unknown zero-day threats missed by antivirus solutions. With the TRITON solution, Websense customers also have the option of choosing hybrid deployment combining SaaS and on-premise platforms with unified management of all deployments. This provides effective protection across the enterprise without incurring the cost of managing multiple systems.

Performance: Taking It Up a Notch

Concerns over SaaS reliability can extend to a company's perceptions about the quality of Internet performance or lack thereof. Why should an IT administrator compound his company's existing bandwidth and network latency worries by routing email or Web traffic through a third-party data center? The answer is that moving security into the cloud can actually improve performance and the ability to scale a security solution with demand.

First, consider the fact that SMTP traffic can consume up to one third of a company's total Internet bandwidth^{vi} and as noted previously, up to 90 percent of that traffic is spam. Also, keep in mind that temporary spikes in spam traffic can drive a company's bandwidth usage off the charts and, in some cases, can even take down a network.

At this point, routing both email and Web traffic through a SaaS solution begins to make a lot of sense, especially solutions that deliver high reliability and performance. Spam, malware, and unwanted Web traffic never reaches a customer's local network and never impacts its bandwidth or network integrity.

Websense SaaS Web security and SaaS for email deliver both of these capabilities. In addition, the company's global, distributed data center infrastructure is designed to minimize network latency by routing email and Web traffic based upon both geographic proximity (which data center is closest to a particular customer) and intelligent traffic analysis (how the Internet backbone traffic impacts latency). With SaaS, organizations have unlimited scalability. Processing isn't limited by on-premise equipment and subject to degradation during high usage periods. Processing through SaaS automatically scales with demand.

Flexibility: Growing Your Current Solution

Even when organizations are favorably disposed towards SaaS, they may be inclined to avoid making any decisions that could impact their on-premise solutions earlier than planned. Companies are understandably eager to squeeze every last dime from their current IT capital investments. However, a SaaS platform-based security solution doesn't have to replace an on-premise solution. A hybrid solution, such as adding SaaS email security to an existing on-premise implementation, can result in benefits such as off-loading the processing, reducing bandwidth, and protecting against traffic spikes, thereby eliminating the need to replace or augment on-premise email servers due to periodic spikes in unwanted email traffic.

Organizations should also consider these two ways that SaaS can complement on-premise Web and email security solutions:

- **Expanded reach.** An on-premise solution is often ill-suited to meeting the demands of remote and mobile workers. Given the nearly universal trend towards distributed workforces, this creates an obvious opportunity for SaaS solutions to step in and address this coverage gap.
- **Extended capabilities.** Many companies currently employ on-premise security products that lack important functionality. A well-rounded SaaS solution can add missing pieces to the security puzzle or offer a smooth transition to an integrated suite of security products.

The current Websense SaaS Web and SaaS email security offerings illustrate how this process can work. Organizations with on-premise antivirus and antispam solutions can implement the Websense Hosted Web Security offering, which provides protection against unwanted and malicious Web content. They also have the option of graduating to Websense TruHybrid™ deployment, which adds real-time virus and malware scanning, and implementing the Websense antispam solution with Security-as-a-Service.

Websense TruHybrid deployment, available with the Websense TRITON solution, offers the flexibility to select a mix of on-premise and SaaS deployment platforms, while managing the entire environment with the unified management capabilities of the TRITON Console. Organizations can extend security to

branch offices or mobile users by leveraging the SaaS platform. At the same time, they can deploy high-performance appliances at corporate, large branch, or data center locations. Regardless of the mix of SaaS or appliance options chosen, they define a single enterprise-wide policy in one place. This unified approach not only cuts the cost of managing hybrid on-premise/ SaaS deployments but also ensures consistent security coverage across all environments.

Organizations with on-premise email solutions can implement the Websense Hosted Email Security solution. Websense Security-as-a-Service for email integrates best-in-class Web security and data security technology with email security to achieve unparalleled visibility into emerging threats and one of the highest levels of protection from inbound and outbound email security risks. Websense SaaS email security is tightly integrated with Websense SaaS Web security, providing centralized, cloud-based policy management and reporting for both Web and email security.

These Websense solutions provide many of the features associated with far more expensive, on-premise DLP solutions, such as pre-defined content dictionaries and deep content inspection to detect inappropriate or unauthorized outbound communications, while retaining the cost, integration, and management benefits associated with solutions using SaaS.

Control: You Call the Shots

When it comes to SaaS platform-based security, worries about “losing control” typically boil down to two issues: performance and manageability.

As noted earlier, SaaS performance depends largely upon a provider’s data center infrastructure and upon its willingness to back up its infrastructure claims with a meaningful service-level agreement (SLA). Websense backs up its SaaS Web and SaaS email security with an SLA that promises 99.999 percent minimum availability. This represents about the same amount of time required for a single on-premise server reboot, and it gives organizations a level of uptime assurance that very few companies of any size can attain with an on-premise solution.

When it comes to manageability, an organization will benefit by choosing a SaaS provider that provides administrative tools needed, so that the organization isn’t dependent on a third party. With Websense SaaS solutions, organizations use a Web browser to manage their systems in much the same way they might manage an appliance on their network. In addition, they get SLAs which provide contractual commitments to a specific level of performance — something on-premise solution providers aren’t typically able to provide.

In practice, a customer’s ability to manage Security-as-a-Service for Web and email depends upon the following features:

- **Administrative tools.** This includes integrated Active Directory and LDAP synchronization, fine-grained user and group policy definitions, and the ability to adjust spam-scoring criteria manually if desired.
- **Accessibility and integration.** The SaaS solution should offer a Web-based management interface with single-console access to *all* of the Web, email, and content security services that an organization uses.
- **Ease of use.** End-users should have easy-to-use administrative features, such as security dashboards; intuitive policy controls; granular search criteria; the ability to perform tasks appropriate to their organizational role and level of access; the ability to delegate administration; and a full audit trail of administrative actions.
- **Reporting features.** Administrators should have access to the information they need to make accurate decisions and to evaluate the effectiveness of a SaaS solution.

As noted earlier, Websense TruHybrid deployment enables full management on premise, with SaaS in the cloud as an enforcement point. So for organizations that want to retain greater control, such as longer log and reporting retention, they can manage on premise but use the cloud to deliver the policy to the end-user.

Ultimately, there is absolutely no reason for any organization to lower its expectations when it comes to the level of control it will have using a SaaS solution. If a SaaS provider cannot deliver all of the management capabilities that a customer expects from its Web and email security tools, then other aspects of its solution offering are also unlikely to meet the customer's expectations.

Privacy and Security: SaaS Can Keep a Secret

A common concern many organization have is that a provider will expose sensitive data to unauthorized users or that the provider's systems will fall prey to the very attacks it is supposed to prevent.

One of the best ways to assess a SaaS vendor's privacy and security measures is through the use of third-party certification procedures. Perhaps the most relevant certification, known as ISO 27001, is designed specifically to "provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an information security management system."^{vii} This rigorous certification process focuses on a number of key requirements, including:

- The use of best practices to ensure the privacy, integrity, and availability of customer data.
- A provider's willingness to submit its data center and related operations to periodic certification audits.

A security certification is one piece of the puzzle, but there are others. A SaaS provider should mandate standards for protecting the physical security of its data centers, including around-the-clock staffing, access control, and multilayered monitoring systems. It should also submit its facilities to regular vulnerability testing, preferably in conjunction with a third-party security assessment organization.

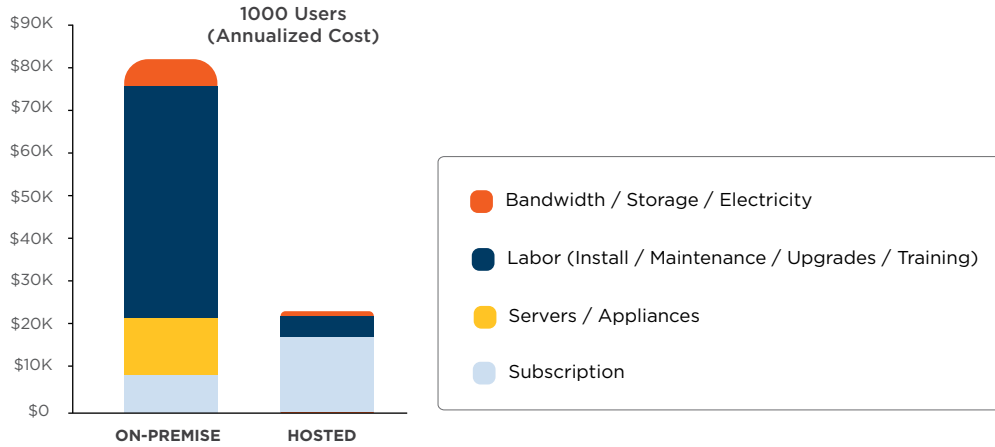
The process of evaluating a SaaS provider's privacy and security measures should never involve a leap of faith. Websense, for example, has certified its SaaS Web and email security solutions to ISO 27001 standards and is externally audited every six months to ensure its compliance. Websense also enforces the strictest physical security standards for its data centers, ensuring both the reliability of its solutions that use SaaS and the security of its customers' data. As a result, customers that adopt Websense SaaS solutions can count on a level of privacy and security that many enterprise data centers are not even capable of matching.

Cost: A Core Benefit of the SaaS Platform

SaaS solutions can significantly reduce total cost of ownership (TCO). With a SaaS solution, organizations can reduce costs by eliminating the distribution, deployment, and ongoing upgrade of on-premise hardware. In addition, no electricity or cooling is required. Bandwidth costs are lower, and built-in fault tolerance further eliminates the need for additional servers. Labor costs are also reduced, because instead of paying for training, installation, management, and ongoing maintenance, the labor costs associated with a SaaS solution are focused on minimal staff training and administrative functions.

The graph below, with data from Osterman Research, compares the costs associated with on-premise email security to Websense SaaS email security. The difference in labor costs alone is often sufficient to justify a move away from an on-premise solution, although other factors, including the virtual elimination of hardware costs, also play a major role.

Cost of Ownership (On-Premise vs. Hosted)

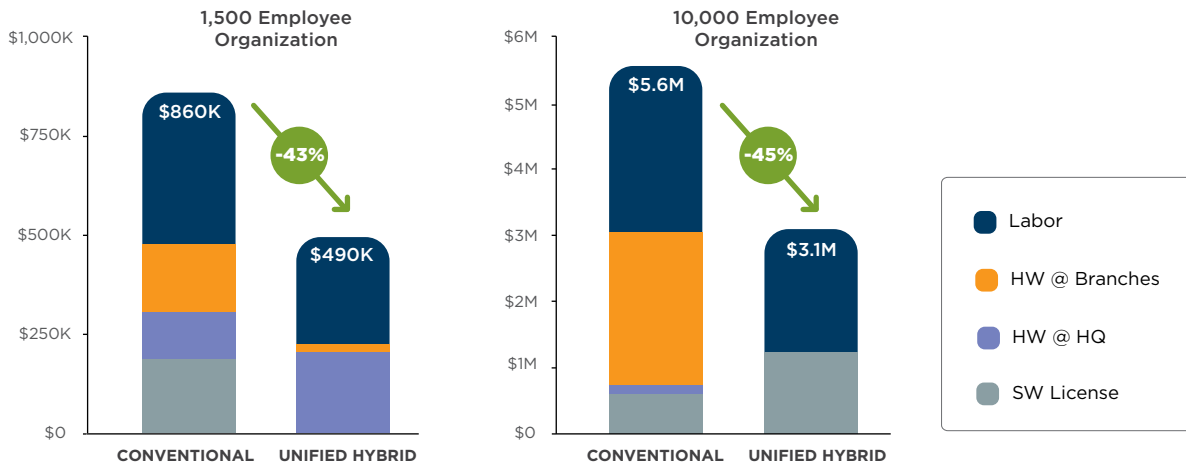


Source: "The Advantages of a Hosted Security Model," Osterman Research, July 2009.

Osterman Research concludes that 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.^{viii}

For those who prefer a hybrid approach, Osterman Research found that the cost benefits of a hybrid solution for Web security were substantial when compared with conventional on-premise solutions, as shown in the following cost comparison between the two.

Hybrid Web Security Cost Comparisons



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

Since cost is such an important factor in determining whether many organizations decide to pursue a SaaS solution, it's important to accurately compare costs between SaaS and on-premise products. A number of incorrect assumptions exist that initially appear to stack the deck in favor of on-premise solutions but a closer look reveals the reality behind these assumptions.

Labor costs. Let's take another look at labor costs. Many companies tend to underestimate the labor costs associated with managing and maintaining on-premise solutions. Decision makers may, for example, fail to consider the cost of assigning IT staff to perform patches and software upgrades, deal

with unplanned outages or system failures, and conduct capacity-planning exercises to address future security infrastructure requirements. Companies that include all of these costs in their TCO estimates are likely to draw some surprising conclusions. According to a 2008 Osterman Research study, a complete accounting of IT labor costs for an on-premise email security solution results in a total annual cost of \$103 per email user.^{ix}

This estimate does not include the impact of another, closely related cost: training for the IT staff members assigned to administer an on-premise solution. According to the same study, companies should assume an average training cost of around \$3,000 per IT staff member involved, and this figure does not include the opportunity cost of taking staff members away from their daily duties in order to receive training.^x

Non-labor costs. In addition to upfront hardware and software licensing costs, companies must also consider the ongoing financial burdens associated with maintenance contracts, licensing renewals, bandwidth, networking infrastructure, and power and cooling requirements. According to Osterman Research, annual non-labor costs amount to more than \$19 per user.^{xi}

Paying the on-premise risk premium. Other costs are more difficult to quantify, yet they should play a role in the assessment process:

- **Overhead overkill.** Given the risk of occasional “spam spikes,” companies that manage an on-premise antispam solution must also plan for bandwidth and server capacity far in excess of their normal operating requirements. Since this capacity serves no useful business purpose, it represents an especially wasteful use of scarce IT resources.
- **Strategic sacrifices.** As we have already pointed out, companies with fixed IT budgets and limited resources must make a choice: Continue to manage in-house Web and email security solutions or focus on strategic business IT objectives. In the current economic climate, it is often impossible to accomplish both of these tasks at the same time.

The price of failure. In a study by IDC, only 11 percent of organizations surveyed reported spam blocking effectiveness of 99 percent or above, which is the rate offered as part of the Websense Hosted Email Security SLA.^{xii} Given the risks associated with zero-hour Web and email threats, this performance gap could cost an organization dearly. Websense SaaS solutions are also backed by a 100 percent SLA for protection from known viruses.

The cost of complexity. Inevitably, complexity breeds complexity; as Web, email, and data loss threats morph and evolve, the tools required to address these threats must keep up the pace. This imposes two major burdens on an IT staff: It must stay abreast of the latest threats, and it must ensure that its on-premise security infrastructure is capable of addressing those threats. A SaaS solution can relieve a company of these burdens, shifting the responsibility for staying ahead of the curve from the customer to the provider.

Companies should also consider the costs associated with maintaining multiple Web and email security solutions versus a single, integrated solution with unified management that addresses both their Web and email security needs. The unified and integrated Websense email and Web security solution using SaaS, for example, can deliver significant savings by reducing the IT labor costs and indirect opportunity costs associated with multiple point solutions, each of which typically requires its own management console, administrative procedures, maintenance and upgrade procedures, and associated IT training requirements.

Conclusion: Seven Reasons to Use SaaS

The right Security-as-a-Service solution can perform reliably and effectively and deliver the flexibility and control associated with on-premise solutions — at a significantly lower cost — without compromising privacy and security. Whether as the sole deployment platform or part of a hybrid on-premise/SaaS solution, SaaS helps provide a greater return on an organization's security investment through coverage that scales to meet an organization's needs and by reducing costs associated with maintaining on-premise solutions.

When choosing a SaaS provider, consider the market-leading capabilities provided by Websense solutions. Websense SaaS customers gain all the benefits of the industry's leading content security, while eliminating the distribution, deployment, and ongoing upgrade of on-premise hardware. With Websense TruHybrid deployment, customers receive unified management of hybrid on-premise/SaaS deployments across the enterprise, along with all the benefits of the Websense TRITON solution including enterprise-class data loss prevention and real-time content classification and scanning.

ⁱ "SaaS Valuation Criteria," Forrester Research, Inc., February 22, 2010.

ⁱⁱ "Secure Email: Make It Someone Else's Problem," InformationWeek Analytics, December 2009.

ⁱⁱⁱ "Say Yes! Hosted Security De-myth-ified," Websense Webinar, July 2009.

^{iv} "Worldwide Mobile Worker 2009-2013 Forecast," IDC Research, #221309, February 2010.

^v "Say Yes! SaaS Is a Security Muse," Websense Webinar, September 2009.

^{vi} "The Advantages of a Hosted Security Model," Osterman Research, July 2009.

^{vii} "An Introduction to ISO 27001," www.27000.org, retrieved February 1, 2010.

^{viii} "The Advantages of a Hosted Security Model," Osterman Research, July 2009.

^{ix} *ibid.*

^x *ibid.*

^{xi} *ibid.*

^{xii} IDC, "Messaging Security Survey: The Good, Bad, and Ugly," #216781, February 2009.