

The Cost Benefits of a Hybrid Approach to Security

An Osterman Research White Paper

Published February 2010

SPONSORED BY



Why You Should Read This White Paper

THE PROBLEM

Managing security for any size of organization has never been easy or cheap, but it is becoming significantly more difficult and expensive. The growing use of social networking tools like Twitter and Facebook, as well as the Web itself, are making the potential for inbound threats much worse. In addition, organizations must increasingly be concerned about what leaves their organization – a trade secret sent through a Twitter post, an unencrypted file containing personal health information sent in Webmail, or an employee blog post that does not represent the position of his or her employer can all have serious financial and other consequences.

To manage these threats and ensure compliance with regulatory obligations, legal requirements and corporate best practice, IT departments must deploy the right capabilities to address them. Many solution providers offer a set of single-function solutions, often with their own user interfaces and with standalone policy management capabilities that require significant investments in IT staff time. Many companies require multiple vendors to construct a defense, often resulting in gaps in coverage. Further, small companies and field offices of larger ones typically do not have enough users to support a dedicated IT staff person, meaning they must rely on the office manager, accountant or other non-techie to manage the local infrastructure, perform regular updates, apply patches, manage policies and perform other housekeeping chores for the local appliance or server. As a consequence, many organizations either go without the requisite coverage, or pay a high cost, managing multiple vendor solutions.

The result can be a collection of non-integrated systems that drive up costs to deploy, manage, and support, and that lack the ability to apply consistent security controls across the enterprise with ease of efficiency.

THE SOLUTION

However, these problems can be avoided by using a combination of on-premise systems and cloud-based services that:

- Consolidate security services from multiple vendors, security applications from multiple devices, and leverage cloud-based controls to alleviate the burden of deploying, managing, and supporting infrastructure at the remote or branch office.
- Allow IT staff in the corporate headquarters to manage all policies from a single interface across the entire organization for users served both by appliances and cloud services. This means that policies will be more consistent and less time-consuming to create, monitor and enforce. In short, IT staff can enforce all corporate policies from one console and push these policies to all points on the network simultaneously.
- Replace legacy security technologies with a more advanced and integrated security analysis solution that combines inbound threat prevention with outbound data loss; and coverage across the entire, distributed enterprise so that policy controls are consistent and pervasive, risk is reduced, and remediation costs are diminished.

KEY TAKEAWAYS

In short:

- Organizations of all sizes must protect against the continuing onslaught of email-based malware and the growing threat of increasingly sophisticated Web-based malware that can enter the corporate network.
- They must protect against data loss that can occur from the growing variety of Web and Web 2.0 tools that they use, ranging from ad hoc tools like Twitter and Facebook to IT-sanctioned applications like Google Apps and Salesforce.com.
- They should manage policies consistently and simultaneously, and in a way that minimizes IT's investment of time and people.
- They should consolidate vendors and solutions to improve the performance of their security infrastructure and unify their content security practices.

ABOUT THIS WHITE PAPER

This white paper, sponsored by Websense, discusses the benefits of unified content security, and it provides cost comparisons between conventional and hybrid management of the security infrastructure. The white paper also discusses the Websense TRITON™ system, including the Websense Web Security Gateway and the company's unified approach to content security.

The Web is Both Valuable and Risky...and Becoming More So

SECURITY IS BECOMING MORE COMPLEX

As the Web quickly becomes the new application platform, any organization, regardless of its size or the industry that it serves, is vulnerable to a growing variety of sophisticated threats that leverage its technology. Many of these threats enter organizations through the growing use of Web 2.0 applications, including exploits that are often introduced into a corporate network through no more than simple Web surfing.

However, these are only the newest inbound threats with which organizations must contend. More traditional threats, such as malware that can enter an organization through email or instant messaging systems, or blended threats in which a link to a malicious Web source is sent in a spam email, continue to plague organizations. And, inbound threats are only part of the problem.

While organizations can leverage Web-based tools – such as Twitter, Facebook, LinkedIn, blogs, etc.– for positive business benefits, those tools also pose a growing threat because they can contribute to data loss, non-compliance, and increased risk. For example, an employee can inadvertently attach a confidential memo to an email in their personal Webmail account. An employee can post a company trade secret to

Facebook. An embargoed press release can be sent to a reporter before the company's public relations department wants it to be sent. Customers' credit card information or employees' protected health information can be sent to an outside recipient or posted to the Web without encryption.

While inbound threats can be very damaging to an organization, resulting in data loss, financial loss or a network going down, outbound threats can be just as damaging, if not more so. Violation of regulatory obligations to encrypt sensitive data before being sent to external recipients can result in fines or legal sanctions. Posting a trade secret to an external blog can result in the loss of ownership for that intellectual property. Losing customers' financial information can result in loss of business and a damaged corporate reputation.

SECURITY IS BECOMING MORE COSTLY

While security threats are increasing in frequency and severity, so too is the cost of defending against them. Not only must organizations deploy and maintain traditional defenses, they must also guard against new, more modern threats that are designed to evade legacy defenses.

Furthermore, with the traditional approach of adding a variety of discrete security technologies over time, protecting against outbound risks like data loss can easily lead to costs getting out of control due to redundancy and inefficiency. For example, an organization may deploy servers or appliances focused on protecting spam and malware that are delivered through email. They then add servers or appliances focused on real-time communications. Later, as they recognize the threat from use of the Web and Web 2.0 applications, they may add servers or appliances to protect against them. As organizations attempt to solve the problem of data loss and resulting compliance issues, they are investing in even more infrastructure and technology.

THE GROWING COMPLEXITY OF MANAGING SECURITY

The result is a mix of servers, appliances and services that, in most cases, are a set of point solutions designed to address specific problems. This creates a number of difficult and expensive problems, including:

- The need to manage multiple vendors and their varied upgrade cycles.
- The use of multiple consoles and interfaces to manage each system.
- Managing support requirements for each vendor's solution.
- Incomplete and inconsistent security coverage that can arise from less than complete overlap between the various solutions that have been deployed.
- Higher costs for IT staff required to manage the infrastructure, and higher costs because point solutions from a variety of vendors are being used instead of an integrated solution from one vendor.

The Cloud is Growing in Popularity

MANY ORGANIZATIONS ARE TURNING TO THE CLOUD FOR SECURITY

There has been a significant shift to cloud-based solutions for managing security. Many organizations are using hosted services to protect against threats in email. Some are using these systems to protect against instant messaging and other real-time communications threats. A growing number are using cloud-based Web filtering and scanning services to protect against malware and other threats that can enter an organization through the Web or Web 2.0 applications. Cloud-based security services, while growing in popularity, are ideal for branch office and remote locations, where IT infrastructure needs to be lightweight and simple, to supplement the lack of onsite resources and high support costs.

THERE ARE SOME GOOD CLOUD-BASED SOLUTIONS, BUT...

There are a variety of good cloud-based security solutions. While there is variability in the efficacy of various solutions, many are quite good at protecting organizations and their users.

However, it is important to note that many solutions lack sufficient logging capabilities so that IT administrators can understand how their users are employing the Web and Web 2.0 applications. Some cloud-based solutions do not offer highly granular controls for some services, leading to the potential for false positives when sending certain types of content. Some solutions lack sufficient reporting capabilities that can give IT managers insight into how communication and other tools are employed. Plus, some solutions simply are not as serviceable or configurable as others.

The ideal solution is one that combines the efficiency and flexibility of the cloud, with the control and feature-rich capabilities of on premise – a hybrid architecture.

ORGANIZATIONS SHOULD CONSOLIDATE THEIR SECURITY CAPABILITIES

Whether an organization is using on-premise solutions or cloud-based solutions, they should consolidate their security capabilities. Numerous Osterman Research surveys have found that the vast majority of IT decision makers would prefer a security infrastructure that was highly integrated instead of a set of point solutions from different vendors that must be managed independently. By integrating security capabilities, organizations can realize significant economies of scale in the context of both overall expenditures for these capabilities and in the IT staff required to manage them, and in the efficacy of the security they can realize for their users, data and networks.

A UNIFIED APPROACH CAN OFFER THE BEST OF BOTH WORLDS

Not only should organizations consolidate their security infrastructure, they should also use an optimal combination of on-premise and cloud-based solutions where it makes sense to do so. For example, an organization that has a corporate headquarters and a number of field offices might opt to use an on-premise system for the former where they have dedicated IT staff that can manage the infrastructure, and cloud-based solutions for the latter where dedicated IT staff are not available.

Using a combination of cloud-based and on-premise services can yield two important advantages: the efficiency of cloud-based delivery combined with the highly granular control that on-premise systems can offer. Further, such an approach can lower the cost and improve the overall security posture for many organizations.

The Cost Benefits of a Hybrid Approach

WHAT DO WE MEAN BY "HYBRID"?

The hybrid concept is a simple, yet powerful one: it combines on-premise infrastructure and in-the-cloud services within a unified management framework. Hybrid is not a cloud-based lookup – as some vendors purport. The ability to send content back to a cloud-based security infrastructure for analysis has been in use for years and proven ineffective at dynamically classifying content on the fly for both inbound threats and outbound risks. What's more, cloud-based lookup still requires onsite hardware and supporting infrastructure across the enterprise and does not lower the cost of ownership. A real hybrid deployment comes from having multiple enforcement points – on premise and client-based -- that act together to secure different users in different ways. True hybrid offers the flexibility to choose the enforcement point that's most efficient and best maps to the controls an organization needs.

The advantage of a true hybrid architecture is that it:

- Allows remote offices without dedicated IT staff to have the same access to corporate policies as those users that are served by on-premise infrastructure.
- Allows remote users to be served by the same policies at the same time without a lag in policy updates.
- Provides better performance because traffic is not sent back to an on-premise security system, resulting in much lower latency for remote users.
- Provides multiple security services – Web, data, and email, combined into a single solution architecture for greater visibility and control with less management and support costs.
- Allows organizations the freedom to choose the mix of capabilities that work best for them: on-premise infrastructure, cloud-based services or a mix of both in the same environment.
- Can reduce the overall cost of managing a security infrastructure because it reduces the physical footprint at various sites in the enterprise.

The bottom line is that with a hybrid approach to content security an organization can manage security both on-premise and in the cloud simultaneously for different users. For example, users in a headquarters location can have their content secured using on-premise infrastructure while remote users' content is filtered in the cloud. Traffic for the latter does not have to be backhauled to the on-premise infrastructure, resulting in

greater efficiency and lower cost. In addition, a hybrid infrastructure enables policy enforcement from one pane of glass simultaneously for all users.

FOR WHAT TYPES OF ORGANIZATIONS IS THE HYBRID APPROACH IDEAL?

There are a variety of organizational types and scenarios for which a hybrid approach is an ideal solution for managing security. For example, highly distributed organizations are a good fit for the hybrid approach to security because smaller, remote offices cannot afford to maintain dedicated IT staff that can deploy and maintain on-premise infrastructure. However, even organizations that are not distributed can also benefit from the hybrid approach because of its ability to lower the overall cost of managing a security infrastructure. Further, as more of the security infrastructure is deployed beyond corporate boundaries, it is necessary to consolidate the infrastructure to maintain its manageability – the hybrid approach is ideally suited to organizations that need to do this.

ADVANTAGES OF THE HYBRID APPROACH

So, why should you consider deploying a hybrid security infrastructure? There are several reasons why using a hybrid approach to Web security is the optimum method for managing your security infrastructure:

- **Less infrastructure to deploy**
Using cloud-based services as an integral component of an overall security infrastructure means that there is simply less infrastructure to evaluate, specify, deploy and manage. This reduces the amount of time that IT staff must devote to the initial evaluation and specification process, it reduces the amount of infrastructure that they must deploy and manage, and it reduces overall power requirements.
- **The control of on-premise with the efficiency of the cloud**
While there are many cloud-based security solutions that offer highly granular control over how security policies are developed and enforced, some solutions do not offer the level of control that many IT administrators and business decision makers need. In contrast, the use of a hybrid on-premise/cloud security solution combines the best of both worlds: the highly granular and manageable control of an on-premise solution coupled with the inherent efficiencies of the cloud. The result is a security infrastructure that is less expensive to manage and less susceptible to surges in malware and related activity, while still providing the tight control over how the system is managed.
- **IT does not have to absorb the cost of deployment**
The use of a hybrid architecture for managing security also relieves IT of the burden of purchasing new hardware as security requirements increase. Because malware volumes continue to rise, Web 2.0 applications are used increasingly, and there are simply more Web sites visited by users over time, IT must continually add new hardware to a conventional, on-premise infrastructure. This is particularly true when spam volumes, for example, suddenly spike and necessitate unanticipated and unbudgeted improvements to the security infrastructure. By using the cloud as an

integral component of a security infrastructure, however, the burden of adding new infrastructure does not go away – but it does get shifted away from the customer to the cloud provider, freeing IT from having to absorb the cost of new hardware and software deployments.

- **Less IT staff time devoted to administration**

IT staff time spent managing the security infrastructure is a major expense for most organizations. For example, an Osterman Research study in 2009 found that mid-sized and large organizations spend a mean of 40.5 hours per 1,000 users per week managing messaging- and Web-related security capabilities. At a fully burdened IT salary of \$80,000 per year, that translates to an annual cost of just over \$80 per seat per year just for the labor to manage security. In an organization of 5,000 users, that translates to a cost of more than \$404,000 annually just for the labor to manage the security infrastructure.

A hybrid security infrastructure, on the other hand, can significantly reduce the amount of IT staff time required to manage it. This is particularly true for highly distributed organizations where remote sites do not have dedicated IT staff members. However, even an organization with just one site can also lower their costs of managing security by eliminating the amount of time devoted to patches, upgrades, deploying new appliances, and so forth.

- **A single console to manage everything**

Perhaps most importantly, the advantage of a properly designed hybrid security infrastructure is that every aspect of the system can be managed from a single console. So, instead of managing policies in an email security infrastructure, a data loss prevention (DLP) infrastructure and a Web security infrastructure, each using their own interface and policy applications, all corporate security policies can be developed, monitored and enforced from a single console. This results in not only a lower cost of administration because less IT time is spent managing policies, but also more consistent policy enforcement and the ability to respond more quickly to needed changes in security policies.

COST ANALYSIS

Clearly, a hybrid approach to managing security can offer significant cost advantages over traditional, on-premise approaches. What follows in the next section is a detailed cost analysis with examples of how two types of organizations can benefit by using an optimized, hybrid security system.

Case Studies

For both of the following case studies, we have assumed the following:

- Scenario A: conventional infrastructure
 - A collection of servers and software from several leading security vendors.
 - Annual IT labor cost per user: \$80.90
 - Annual IT wage growth: 5.0%

- Scenario B: hybrid infrastructure
 - One appliance from a leading provider to service users at the headquarters facility and use of a cloud-based service for all remote users.
 - Use of a cloud-based service to push updates to all appliances
 - Annual IT labor cost per user: \$56.63 (assumes 30% less time required because IT can centrally manage all functions from the headquarters location with no involvement by staff members in regional offices.
 - Annual IT wage growth: 5.0%

REGIONAL HEALTHCARE ORGANIZATION

The first case study involves a regional healthcare organization with 1,500 users that has one central headquarters facility with 500 users evenly distributed across 20 regional offices. This type of organization handles a significant amount of confidential data and has significant and growing compliance requirements, not least of which is the updated Health Insurance Portability and Accountability Act (HIPAA) that goes into effect in February 2010. Further, given a less-than-robust economy and escalating costs, the company needs to maximize the efficiency of its IT budget, yet still secure against inbound and outbound threats from its use of email, instant messaging and Web applications.

Based on these assumptions, coupled with costs that have been obtained from verifiable, secondary sources, the costs to manage the security infrastructure at this company are shown in the following tables.

SCENARIO A Conventional Security Infrastructure Costs for a 1,500-User Regional Healthcare Organization

Cost Element	Total Cost
Software	\$189,229
Hardware at headquarters location	\$119,345
Hardware at remote offices	\$169,000
Labor	\$382,561
TOTAL COST	\$860,135
ANNUAL COST PER USER	\$191.14
MONTHLY COST PER USER	\$15.93

SCENARIO B
Unified Security Infrastructure Costs for a
1,500-User Regional Healthcare Organization

Cost Element	Total Cost
Appliances, headquarters	\$7,794
Appliances, regional offices	\$0
Labor	\$267,792
Solution license	\$213,750
TOTAL COST	\$489,336
ANNUAL COST PER USER	\$108.74
MONTHLY COST PER USER	\$9.06
COST SAVINGS	43.1%

The result is a significant savings from the hybrid infrastructure: \$6.87 per user per month, or a total of more than \$370,000 over the three-year lifecycle of the infrastructure.

FINANCIAL SERVICES ORGANIZATION

The second case study is a 10,000-seat financial services organization with 4,000 users in a headquarters location and 6,000 users evenly distributed across 100 nationally distributed field offices. As with the healthcare organization discussed above, this company must comply with a large and growing number of regulatory obligations, including those imposed by the SEC and FINRA. Communications must be monitored closely so that registered representatives are not making inappropriate claims, conducting business via social networking tools and the like. Further, the financial services has been in a state of flux since Fall 2008, and so there is a significant need for persistent policy controls that can help the organization manage its use of communication, social networking and other tools efficiently. This is an industry that is accustomed to the use of outsourced service providers.

Based on these assumptions, coupled with costs that have been obtained from verifiable, secondary sources, the costs to manage the security infrastructure at this company are shown in the following tables.

SCENARIO A
Conventional Security Infrastructure Costs for a
10,000-User Financial Services Organization

Cost Element	Total Cost
Software	\$604,044
Hardware at headquarters location	\$119,345
Hardware at remote offices	\$2,325,000
Labor	\$2,550,404
TOTAL COST	\$5,598,793
ANNUAL COST PER USER	\$186.63
MONTHLY COST PER USER	\$15.55

SCENARIO B
Hybrid Security Infrastructure Costs for a
10,000-User Financial Services Organization

Cost Element	Total Cost
Appliances, headquarters	\$20,800
Appliances, regional offices	\$0
Labor	\$1,785,283
Solution license	\$1,275,000
TOTAL COST	\$3,081,083
ANNUAL COST PER USER	\$102.70
MONTHLY COST PER USER	\$8.56
COST SAVINGS	45.0%

Here, too, the result is a significant savings from the hybrid infrastructure: \$6.99 per user per month, or a total of more than \$2.5 million over the three-year lifecycle of the infrastructure.

Summary

Conventionally managed application security is becoming more complicated with the increasing use of new tools like Twitter and Facebook, and it is becoming more expensive. The results are higher IT costs, more cumbersome and less timely policy management, and greater potential for violating regulatory, legal and corporate policies.

By using a unified approach that combines the optimum combination of on-premise infrastructure with cloud-based services, organizations can reduce their overall cost of ownership for managing security, increase the effectiveness of their policy management, and free IT staff for tasks that will provide more value to the enterprise.

About Websense

The Websense TRITON architecture with the Websense Web Security Gateway is a unified content security solution that combines email security, data security and Web security in a single offering. The solution offers enterprise-class DLP capabilities for Web 2.0 applications. Websense TRITON is a unified architecture for Web, email, and data loss prevention that delivers the market's leading technology to protect employees and their essential information, ensure compliance, and reduce risk. TRITON is the first and only solution to provide unified content security to reduce deployment and administrative costs while providing superior security. The 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 allows for efficient solution delivery across the global enterprise by combining high-performance appliances at the headquarters with security-as-a-service at the branch or remote office.

Websense, Inc. (NASDAQ: WBSN), a global leader in integrated Web, messaging and data protection technologies, provides Essential Information Protection™ for more than 42 million employees at more than 50,000 organizations worldwide. Distributed through its global network of channel partners, Websense software and hosted security solutions help organizations block malicious code, prevent the loss of confidential information and enforce Internet use and messaging security policies. For more information, visit www.websense.com.

© 2010 Osterman Research, Inc. All rights reserved.

No part of this document may be reproduced in any form by any means, nor may it be distributed without the permission of Osterman Research, Inc., nor may it be resold or distributed by any entity other than Osterman Research, Inc., without prior written authorization of Osterman Research, Inc.

Osterman Research, Inc. does not provide legal advice. Nothing in this document constitutes legal advice, nor shall this document or any software product or other offering referenced herein serve as a substitute for the reader's compliance with any laws (including but not limited to any act, statute, regulation, rule, directive, administrative order, executive order, etc. (collectively, "Laws")) referenced in this document. If necessary, the reader should consult with competent legal counsel regarding any Laws referenced herein. Osterman Research, Inc. makes no representation or warranty regarding the completeness or accuracy of the information contained in this document.

THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.