



A Websense® White Paper

Hybrid Messaging Security

How unified hosted and on-premise technology mitigates risk and helps enable your business

Abstract: Increasingly, businesses and analysts are recognizing the value of providing protection where it makes the most sense. Deploying messaging security in layers as a hybrid solution helps achieve greater efficiency and protection while maximizing your network resource investments. A hybrid approach to messaging security combines on-premise and hosted email security into a unified solution. The hybrid deployment model allows you to receive more thorough protection while meeting a wider range of security requirements than is possible in a single deployment model.



Table of Contents:

- Overview..... 3
 - How It Works 3
- Hosted vs. On-Premise Technology: The Right Elements to Leverage 4
 - Hosted Email Security 4
 - On-Premise Email Security..... 4
- The Hybrid Approach..... 5
- Conclusion 6
- About Websense 6

Overview

Today's email threats are more invasive and abundant than ever, and the nature of these attacks is constantly changing. Businesses must deploy security solutions that do more than block spam. A good messaging security solution must provide clear standards for mitigating risk, while also helping align with corporate compliance and governance policies. Many products and services on the market attempt to handle the whole range of inbound and outbound email security threats—in fact, Websense offers two messaging security solutions that provide this range of protection.

Hybrid messaging security is different because it combines the two form factors for email security—hosted and on-premise—and unites them into a cohesive solution that takes advantage of the strength of each delivery platform. By combining the cost savings and network efficiency inherent in a hosted solution with the granularity and easy integration of an on-premise solution, you can customize your messaging security solution to fit perfectly into any existing environment and maximize the elements that will help you meet your security goals.

How It Works

Hosted security filters spam and viruses at the Internet level, while on-premise security resides at the gateway to provide granular inbound and outbound email protection. Figure 1 illustrates this deployment.

In this diagram, Company A is sending a message to Company B. Company B has deployed a hybrid solution: hosted email security blocks viruses, spam, and other threats before they reach the gateway; the on-premise deployment performs a second security screening and also checks outbound email for sensitive content.

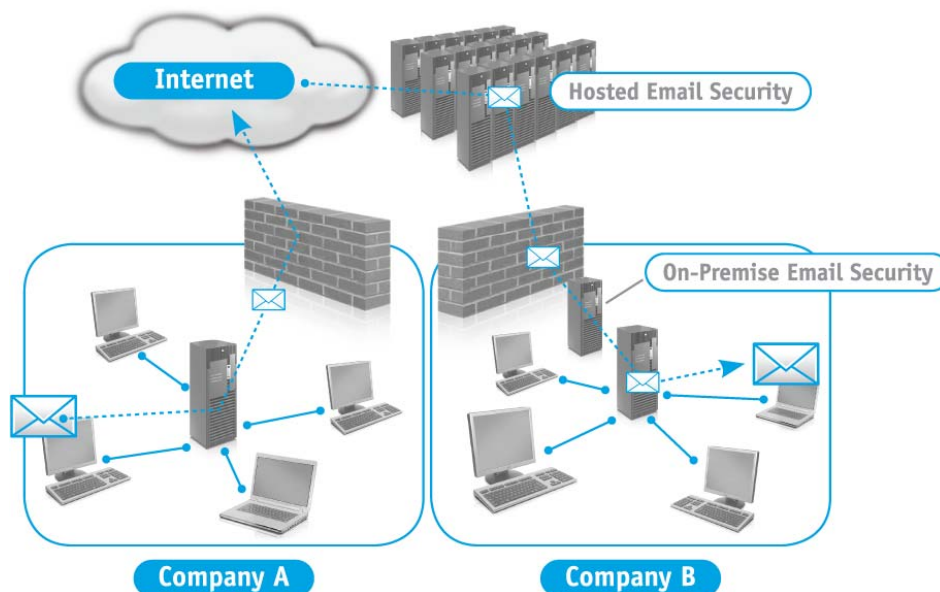


Figure 1: Company B is protected with hybrid messaging security

Hosted vs. On-Premise Technology: The Right Elements to Leverage

The benefits of each deployment option stem from where the solution is deployed. There are inherent strengths to filtering “in the cloud”; likewise, there are advantages that come from managing security in-house.

Hosted Email Security

Hosted email security resides outside the customer’s network and provides excellent bulk protection against threats such as spam and viruses. By blocking these threats at the Internet level and outside your network, you greatly reduce the amount of email and bandwidth you must process at your gateway, lowering business costs. Because a hosted deployment is a service, you benefit from competitive Service Level Agreements (SLAs) that help ensure definitive levels of protection will be met. This mitigates the uncertainty of managing threat protection with your own resources and with dependencies such as available administration time and budget. Only a hosted solution can help mitigate other variable uncertainties such as disaster recovery and capacity planning.

In summary, the hosted delivery platform:

- **Eliminates viruses, worms, Trojan horses, etc. before they reach your gateway.** According to Gartner, this amounts to about 6% of all email traffic.¹ Blocking viruses in the cloud eliminates certain and predictable threats before they reach your network.
- **Eliminates spam before it reaches your gateway.** According to Gartner, this amounts to about 90% of all email traffic, which is a serious and significant percentage that continues to grow each year.² By eliminating spam at the Internet level, you yield tremendous cost savings on hardware, bandwidth, electricity, storage, support, and administration time.
- **Provides clearly defined and certain levels of protection.** Because a hosted solution is a service, it comes with SLAs that provide clear levels of protection (providing SLA-backed uptime, virus blocking, etc.). Only a service can provide this type of contractual reliability.
- **Includes built-in business continuity features.** A hosted solution can provide spooling and disaster recovery, allowing your business to continue even in the face of a network failure. This can be an important part of your network contingency plans, and it ensures that even if your mail server goes down, you won’t lose your email.
- **Enables growth and capacity planning.** The hosted platform is infinitely scalable—providing predictable costs and consistent protection as your business evolves.

On-Premise Email Security

On-premise email security’s strength is in its residence inside the customer’s network, allowing for tight policy integration with directory services. Its gateway location is a prime spot for performing a deep-dive interrogation as messages attempt to leave the network. On-premise technology lends itself to a more granular policy framework and can provide detailed visibility and trend analysis not always achievable through a hosted solution.

¹ Benchmarking Anti-Spam Effectiveness. Gartner, 2007

² Benchmarking Anti-Spam Effectiveness. Gartner, 2007

In summary, the on-premise delivery platform:

- **Provides comprehensive email security through a flexible policy interface.** On-premise security tends to be more granular and can be finely tuned to meet a wide range of messaging security needs. Policies can be applied based on a number of triggers in addition to blocking spam and malicious threats.
- **Performs deep message interrogation.** On-premise messaging security is less concerned with bulk processing and can often be configured to perform very deep content inspection on each message.
- **Can be configured for in-depth content analysis.** On-premise technology tends to offer multiple ways of examining the content of both inbound and outbound messages, including granular dictionaries and image analysis. In fact, many smaller customers use on-premise outbound email security as a beginning step toward blocking data leaks.
- **Provides granular reporting.** Depending on the solution, on-premise security can obtain a more detailed view of the email. For example, Websense Email Security provides reports that show not just spam and virus statistics, but per-user or per-department trends for outbound email usage.

The Hybrid Approach

According to IDC, approximately 20% of small businesses and 40% of large businesses have a hybrid messaging security solution deployed today.³ The flexibility of a hybrid deployment allows you to choose which elements from each form factor is the best fit for your organization's unique needs.

Below are three example scenarios, each of which illustrates a specific reason your organization may want to think about hybrid messaging security.

Benefit #1: Hybrid messaging security improves network and cost efficiency.

Most customers use hybrid messaging security to improve the efficiency of on-network processing. By eliminating 90% of your inbound email traffic (since roughly 90% of all email is spam), the burden of what you process, filter, and archive on-premise is greatly reduced. The second benefit is that once all that junk is gone, your on-premise solution can perform a second screening of the email, ensuring through multiple technologies that the email is clean.

In this scenario, you will improve the efficiency of email processing as well as ensure greater protection through multiple layers of messaging security.

Benefit #2: Hybrid messaging security mitigates the risks of inbound and outbound email.

There is a logical benefit to keeping certain types of email where they belong: harmful email should stay outside your network; sensitive and confidential email should stay inside your network. Hybrid messaging security keeps potentially harmful messages in their place.

In this scenario, hosted security eliminates viruses, malware, worms, spam, and other threats before they reach your network. On-premise security prevents sensitive data from leaving your network via email. For many customers, especially in the SMB space, this provides a good first step toward implementing a data leak prevention solution.

³ Security's Troublesome Twins, Crime & Compliance, Ride the Web and Drive 2008 Trends. IDC, 2008

Benefit #3: Hybrid messaging security is best from a single trusted vendor.

A hybrid deployment does not require both solutions to come from a single vendor. In fact, adding hosted security to an already existing on-premise implementation can help improve performance and efficiency while allowing you to continue using a solution that is familiar and effective.

However, there are specific benefits that can only be obtained when a single vendor supplies both the on-premise and the hosted technology. For example, customers can benefit from a strategic layered approach, ensuring that layered security is not redundant but complementary. Support is centralized, ensuring best practices for the hybrid as a holistic solution, not as two simultaneous and independent solutions.

It is also important to consolidate hybrid messaging security through a vendor that is a leader in threat expertise AND data leak prevention. This will ensure that you truly are using the best solution for inbound and outbound protection, and if you need to develop a more thorough and strategic solution for data loss, your vendor will be able to help you make that transition.

Conclusion

Hybrid messaging security provides greater protection and allows you to meet a wider range of security requirements than you can with a single deployment model. Deploying messaging security as a hybrid solution helps you achieve superior efficiency and protection, while maximizing your network resource investments.

About Websense

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 security policies. For more information, visit www.websense.com.