

Why Security SaaS Makes Sense Today

TABLE OF CONTENTS

Seven Reasons to Adopt SaaS Security	2
The Savvy SaaS Selector	5
On-Point Security with SaaS	6

SPONSORED BY



Seven Reasons to Adopt SaaS Security

Service subscription takes the headache out of email and Web threat management.

BY SANDRA GITTLEN

Corporate IT teams are waging a significant security battle on two fronts these days: stopping attacks via the Web and through email. They are tirelessly trying to protect their networks against known and unknown viruses, spyware and phishing attacks. However, the more complex these threats become, the more infrastructure companies have to bring in-house, sending capital expenditures through the roof.

It's a battle that Aaron Zuccolin, manager of information systems at the Canadian law firm Watson Goepel Maledy LLP, knows all too well. He estimates that 80% to 90% of his Vancouver, B.C.-based firm's email is spam—a risky proposition when he is beholden to data protection laws in Canada, the United States and Europe.

“Trying to manage that volume day-to-day in-house would be ridiculous,” he says. “Enterprise security is highly variable in terms of the threats you have to deal with, the solutions that are out there to deal with them, and the complexity you want to endure as you scale. That

makes it a fool's game to manage it in-house because you can spend thousands of dollars on hardware, software and personnel and still not lower your risk,” Zuccolin says.

Instead, like many of his peers today, Zuccolin has opted for a software-as-a-service (SaaS) strategy, a software application delivery model where applications are hosted on the Internet and companies pay for usage rather than infrastructure and licensing. By offloading his email security to a provider, Zuccolin says he can focus his team on developing policies and procedures that mitigate the overall data privacy risk.

Chenxi Wang, principal analyst at Forrester Research Inc., says that SaaS offerings will become more prevalent over the next few years as services continue to mature and organizations see SaaS as viable for more than just standard business applications. “Companies are getting more comfortable with SaaS in general—it's becoming more of a norm. They're realizing the benefit of outsourcing commoditized solutions, like security, to specialists so they can stay focused on their core business,” she says.

In fact, companies are seeing drawbacks to owning and managing their own security infrastructure. For instance, on-premise security software and appliances can create a single point of failure. They can also be hard to scale as threats increase, slow to respond to new threats, and a drain on internal IT resources.

Security SaaS solves these problems. Here are the top seven reasons why security SaaS makes sense:

1 Provides improved manageability

In most organizations today, security revolves around building and managing either hardware and software or appliances. IT teams must spend a majority of their time focusing on licensing, updates, performance and availability for a host of security systems strewn about the enterprise. They also struggle with implementation and setup costs, as well as compatibility issues. This leaves little time for managing what's most important—the business processes that mitigate risk.

With SaaS, companies can eliminate the burden of managing infrastructure and focus on developing and enforcing streamlined policies. They can also direct responses to overall threats via a single console, rather than having to tweak configurations at distributed locations. Zuccolin says this holistic view has made it easier and more effective for him to combat spam, spyware, virus and phishing threats.

“We’re more strategic now. We’ve gotten rid of the mundane work so we can focus on our overall security policies such as lowering our risk and disaster recovery,” Zuccolin says. In fact, he says rather than worrying about time-consuming tasks such as deploying and testing patches, he can focus more on business analytics and problem solving.

2 Features guaranteed SLAs

One of the biggest benefits to SaaS is knowing that the provider has promised to uphold a service-level agreement (SLA). SLAs traditionally

[Enterprise security] is a fool’s game to manage in-house because you can spend thousands of dollars on hardware, software and personnel and still not lower your risk.”

**AARON ZUCCOLIN, MANAGER
OF INFORMATION SYSTEMS,
WATSON GOEPEL MALEDY LLP**

guarantee a higher level of performance, availability, uptime and security than IT teams would be able to deliver in-house. And there are penalties to collect on if the provider fails to meet this agreement. Most SLAs offer a way for companies to access reports that feature details on threat mitigation, throughput and response-time performance, as well as other key metrics.

SLAs also offer a clear understanding of the different levels of support customers will receive based on the threat priority level. “With SLAs, you put escalation procedures in place so you know what to expect when an abnormal situation happens. You also know that things will be taken care of, and when they’re not, who to call,” Wang says.

Zuccolin calls SLAs the best way to get comfortable with the idea of SaaS because any concerns IT teams might have can be addressed in writing. “We focused on responsiveness in our SLA because if it takes us a day to have a threat addressed, we lose a lot of lawyer productivity,” he says.

SLAs are also a good opportunity to bring to light potential hidden costs. Wang says it’s important to negotiate fees for scaling and other common SaaS occurrences within the SLA to avoid potential budget busters down the road.

3 Affords flexibility and scalability

Trying to keep up with the demands of protecting email and Web security can be impossible—literally. Consider that in most cases, IT teams must physically build out their networks to handle corporate growth. And as the network expands, so does the need for IT staff to manage it.

SaaS enables IT teams to easily and transparently scale security to match business needs. For instance, they can quickly add a group of users that resulted from a corporate merger or beef up scanning to protect the organization from unwanted Web content. They can also make sure that mobile users have the same security on- and off-network—a difficult challenge with on-premise solutions.

Zuccolin says he relies on the flexibility of his security SaaS to allow him to adjust group and user policies on the fly to match new legislative mandates.

4 Provides high-quality security by security experts

It would take a larger IT team than the majority of companies have to address the security challenges most organizations face, according to Wang. As an example, she points to the fact that

711,912 new malware threats were reported in 2007, which translates into 1,950 new malware attacks each day.

She adds that the Web is becoming increasingly more dangerous, with growing numbers of search queries resulting in at least one malicious URL.

To adequately combat most of these threats, IT teams need immediate and detailed knowledge of emerging attack vectors. One or two staff members devoted to security can't possibly detect and mitigate these risks quickly enough to ward off serious damage.

Wang says that less than half of respondents to a 2007 Forrester survey reported using any kind of real-time protection such as behavior-based detection, outbound content protection, heuristics detection, content inspection, reputation filters or URL filtering.

With SaaS, companies don't have to be security experts. Instead, they can depend on the expertise of a provider that is constantly monitoring and combating new threats to the network. Using signature, behavior and heuristic analysis in tandem with access and policy controls, a SaaS provider can quickly thwart spam, virus, spyware and phishing attacks within email as well as detect inappropriate content and malware on Web sites that users visit.

And since this protection is in the cloud, providers can eliminate the threat before it impacts the network. For instance, companies avoid the slow system performance, reduced employee productivity and other business disruptions that spam causes. Cloud-based protection also gives providers a holistic view of potential threats so they know how to protect customers from attacks that

[Companies] are realizing the benefit of outsourcing commoditized solutions, like security, to specialists so they can stay focused on their core business."

CHENXI WANG
PRINCIPAL ANALYST,
FORRESTER RESEARCH INC.

have affected other organizations.

Zuccolin says security SaaS gives him immediate access to updates without having the typical delay required to download and test a patch. He considers it the fastest response to zero-day threats.

5 Reduces bandwidth requirements and improves network performance

SaaS is not only a cost-saver, but also a resource-saver, according to Wang. She says that offloading email and Web security takes a lot of pressure off the enterprise to handle traffic generated by spam.

For instance, if a company builds its network to support 15 million inbound email messages per day and 14 million are purely junk, that's a lot of money wasted trying to deal with the volume on-premise. "After you move to an in-the-cloud offering, you only need to support a million messages per day on your own network so bandwidth consumption is drastically reduced," she says. By

ridding the network of that extra burden, companies could also see a boost in performance.

6 Plays a critical role in defense-in-depth security

Security experts recommend that companies have a multilayered approach to security, but buying and managing the infrastructure required to do that can be cost-prohibitive.

Security SaaS enables IT teams to have a layered approach without all the headaches. For instance, Wang says Web security SaaS can handle fast processing of connection-level filtering and an on-premise solution to perform the more in-depth content analysis. That first layer lightens the load the on-premise solution has to inspect, enhancing the network's speed and overall security.

Zuccolin says he uses his email security SaaS as an additional layer to ensure outbound email is free of unwanted content and intellectual property so his company is seen as a good corporate citizen.

7 Enhances cost savings surrounding security

One of the biggest issues for many organizations is determining if security SaaS adds to the bottom line. As mentioned previously in this report, by eliminating the need for infrastructure and the personnel to manage that infrastructure, SaaS offers immediate savings. In a 2007 study, market research firm Gartner Inc. found that SaaS secure Web gateway solutions cost as much as \$40 less per user than

appliances. Companies realize these savings by having a subscription model with predictable costs.

Companies can also see cost benefits from needing less storage and bandwidth since a lot of spam and other false content is handled off-network. SaaS lowers help desk costs as well because IT teams spend less time fixing damage

caused by spam, viruses, malware and other attacks.

By using a comprehensive security SaaS solution, organizations can avoid the incurred costs of a data breach. A survey by the Ponemon Institute LLC found that 74% of respondents reported a loss of customers, 59% faced potential litigation, 33% faced potential fines, and 32%

experienced a decline in share value.

As these seven reasons prove, SaaS is definitely the best option for tackling even the toughest Web and email security challenges. Not only do IT teams get to hand off routine security infrastructure tasks, but they also get instant and scalable access to top-notch security protection across the entire organization. ▶

THE SAVVY SAAS SELECTOR

Five simple steps to finding a SaaS partner that meets your business needs.

Handing over the management of Web and email security is a big step for most organizations. To ease that anxiety and ensure the success of your SaaS adoption, you need a solution that matches your business requirements. Here are some tips for finding the perfect SaaS partner.

1. Dig deep into the provider's service-level agreement. You're agreeing to move your operational burden to the SaaS provider, so you will need an inside view into their operations. Also, get a commitment to guarantee the availability and uptime of your security service as well as its effectiveness, accuracy and security. The provider should offer you a way to track, record and audit these performance benchmarks.

2. Consider the data center footprint. If you're a distributed or global company, look at the map of your provider's data center sites. Make sure that you can not only connect to the closest data center, but that you also have failover capabilities to alternate sites in case of an outage. Test-drive these connections during the evaluation phase.

3. Plot out your integration needs. With Web and email security, it's critical to detail what part of the existing infrastructure will need to be integrated with the SaaS solution. For instance, you should determine whether the provider will have to handle LDAP directories, Microsoft Exchange and other security infrastructure. The goal is to have a tightly integrated network that includes SaaS, not a set of siloed applications.

4. Ask about the size of existing customers. It's too easy to get into a situation where your provider only has experience with small businesses, so make sure you ask about customers that have a similar scale as your organization. In addition, inquire about their deployment scenarios for larger customers for future expansion. If you are in an industry with strict security and privacy restrictions, such as medical or financial, gather references for customers in similar situations.

5. Don't overlook customer support. If something happens to your Web and email security during crunch time at your organization, you're going to want your provider at the ready. It is standard for SaaS providers nowadays to say they have 24/7 support, but it's up to you to make sure that's true. Evaluate whether their response times are the same or better than what you'd be able to do in-house. Also, look carefully at the different tiers of service the provider offers based on the severity of your issues. Your provider, no matter what your SLA, should be closely monitoring the network in order to detect problems before you or your users do.

It's important for IT teams to compare service providers based on these five criteria. If they pass in all these areas, you can rest assured that your Web and email security are in good hands.

—Sandra Gittlen

On-Point Security with SaaS



Keeping up with Web and email security threats can be a daunting challenge for today's busy IT executives. Writer Sandra Gittlen spoke with Michael Irwin, chief operating officer at Webroot Software, to discuss how SaaS can help organizations offload the security burden without risking data protection.

Q: What is the state of security surrounding email and Web applications today?

Irwin: It's not good. There is a massive explosion of new malware variants. The browser is the main gateway for malware. In fact, the Web is making up about 80% of new infections because users are increasingly landing on infected sites. There has also been a sharp increase in spam and a proliferation of malware in email. Existing Web and email security technologies cannot handle this increase in outbreaks—especially when you consider that new malware is constantly being generated on the fly.

At the same time, demands on IT groups are increasing but your budgets are not. So you have to deliver a higher level of protection with lower costs.

Q: How are IT organizations accomplishing this goal?

Irwin: What you're seeing is an evolution. First, IT teams used a combination of software and hardware. But this required going out and buying a bunch of infrastructure, configuring it and making tweaks that were specific to the organization. Then those configurations had to be locked down so that they weren't open to manual error.

Next were appliances, which were a significant improvement over the software/hardware option, because they weren't as error-prone. However, they still needed ongoing management and updating. Also, it can be hard to plan where to put your appliances depending on your network topography. While they should be close to your users, you don't want them in a spot where IT can't reach them.

In both of these cases, you also have to spend a lot of time trying to predict and budget for future spends. What if you get a denial-of-service attack? Do you have enough hardware and software or appliances to handle that event or do you have to plan for a tenfold increase in traffic?

Q: How does software as a service solve these problems?

Irwin: SaaS is the next logical iteration to help secure the perimeter. It takes out the ongoing management piece and puts it in the provider's hands. The subscription model eliminates capital expenditures on infrastructure and appliances. There is no doubt that spam will continue to increase and that denial-of-service attacks will happen. SaaS ensures you don't feel the strains of those inevitabilities.

With SaaS, you get higher levels of protection as threats expand and morph. Software and appliances tend to become more specialized and complex as attacks evolve. Because of the time it takes to discover vulnerabilities, create a signature, test patches and deploy them, you've always got a gap in security. SaaS puts the onus for all this on the provider, who employs heuristics and behavioral analysis in the cloud to detect a majority of new variants before they even affect your network. You're essentially moving the protection much closer to the source of potential problems and gaining a holistic view of malware

threats. Therefore, you can make mitigation decisions quickly and intelligently.

You also gain the wisdom of crowds. If your provider detects and fixes a threat to another customer, your service will be updated immediately as well.

Finally, SaaS affords a much better management model because you can oversee multilocation implementations and enforce granular policies from a single console.

Q: What about the belief that most IT organizations want security to be managed in-house?

Irwin: That view has changed pretty

significantly since email security SaaS first started in 1999. IT teams realize this is a viable model because the alternative economics are so disruptive. You have a list of things to get done with a very small staff and budget, so you need these types of solutions.

Q: In what type of or size of organization does SaaS security thrive?

Irwin: This delivery is applicable to the entire marketplace. Everyone from Fortune 50 companies down to individual users is struggling with the same problem—stopping spam and protecting Web applications. SaaS fills that need. ▶

Sandra Gittlen is a Massachusetts-based technology writer and former senior editor at Network World.