

SECURITY-AS-A-SERVICE:
HOW SAAS CAN IMPROVE YOUR ORGANIZATION'S SECURITY

A Purewire™ White Paper



CONTENTS

Preface	2
Section I: Security – An End-User Experience	2
Section II: The Administrative Burden of Security	3
Section III: The Disadvantages of Onsite Solutions	4
Section IV: Security Challenges of “In-the-Cloud Security”	5
Section V: The Never-ending Battle	5
Section VI: Protection in a Distributed Environment	6
Executive Summary	6
About Purewire	7

SECURITY-AS-A-SERVICE: HOW SAAS CAN IMPROVE YOUR ORGANIZATION'S SECURITY

Preface

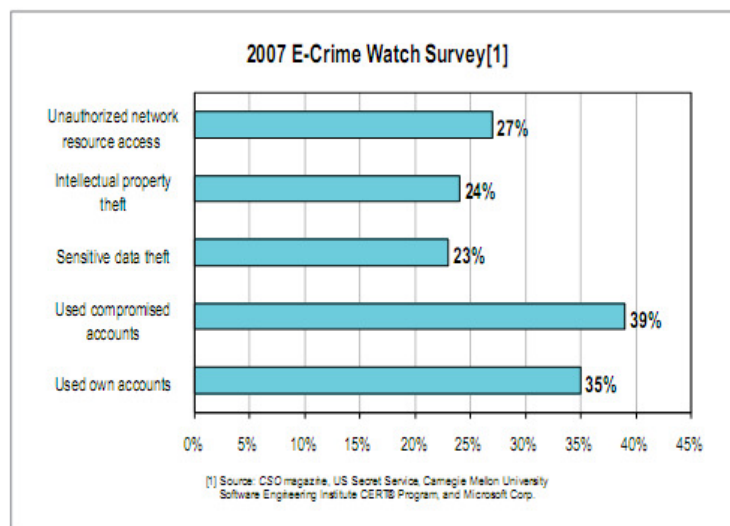
Cloud computing, hosted services and applications on demand have redefined how users interact with data, but security solutions are still stuck in the past, hindered by arcane architecture and localized thinking. The market demands a better way to implement and manage security, while eliminating the liabilities of the past and looking to the future.

The time is now to evolve security to meet the needs of the Web 2.0 world and that evolution will come from the adoption of Software as a Service (SaaS) based security solutions that eliminate the disadvantages of traditional security products. To understand the advantages of new security solutions, one must look at the shortcomings of traditional solutions and pick the path that delivers absolute security in the most cost-effective and palatable fashion for both the administrator and the end user.

Section I: Security – An End-User Experience

55% of online users said they had been infected with spyware, and 82% believed it posed a threat to online privacy, according to Bigfoot Interactive.

Many organizations are finding that the weakest link in the security chain is the endpoint device, or more specifically, the end user. Whether it is through carelessness, ignorance, malicious intent or just plain ignoring the rules, end users introduce all sorts of security ills into a business network. Those security problems can at times go undetected or at the very least, recognized and remediated only after the damage is done. What's more, the biggest problem with end-user security is in fact, the end users themselves.



End users continue to pose a threat to enterprise network security as illustrated by the 2007 E-Crime Watch Survey of IT security professionals.

To fully comprehend how an end user can impact network security, one has to delve deeper into the end user's typical behavior and how that behavior can affect security practices already in use and those that are under consideration. Additionally, the requirements of the business process must also be taken into account to determine if an end user's activity is in line with the operational goals of the business. Of course, monitoring user behavior and correlating that to the business process is a task beyond most IT departments, and many administrators will need to turn to third-party analytics to monitor and evaluate that activity. Never the less, those evaluations are critical for building effective security since most

security problems arise from non-standard behavior and not the tried and true practices set forth by an IT department. The trick here is to use gathered data or industry research to delineate the core issues of the problem.

One of the biggest considerations for today's users and security is flexibility. Today's knowledge workers have come to rely on the gamut of social networks, Web sites and electronic messaging to gather the information needed to perform their jobs, build business relationships and access external information. Those necessities create a conundrum for security professionals: on one hand, administrators can limit the access to those resources, but productivity will eventually suffer, while on the other hand, opening up a network to external resources can result in myriad security problems. It all comes down to balance and acceptable risk.

- **Some 11% of executives felt more vulnerable to security breaches this year from last year.**
- **25% of CIOs rated preventing breaches, controlling user access to data and systems, and assessing risk as top priorities.**
- **More than half rated managing the complexity of security as their number one challenge.**

(Source: CIO Magazine)

Simply put, all that typical end users desire is unhindered access to the resources they need to perform their duties. For IT to provide that access, a multitude a security services need to be implemented, all without burdening the end user and still offering the highest level of protection. Security must be implemented in such a way that prevents end users from disabling the technology and where adopted policies for access are enforced. If a security problem does occur, remediation must take place with little or no end-user intervention to ensure that an infection does not expand into the network. This is particularly true when it comes to securing the Web browsing experience. Users have little to no tolerance for latency or delays when accessing the Web to conduct business activities. IT departments are challenged with maintaining Web security while remaining transparent to the end user.

These requirements are often beyond what can be done with desktop or endpoint-based security products, forcing IT to adopt highly integrated security solutions which are burdensome, expensive and short of fully reliable. Simply put, any security technology that is wholly reliant on end-user interaction is susceptible to failure.

Best practices for end-user security:

1. Run anti-virus and anti-spyware software
2. Use a firewall
3. Enable automatic computer updates
4. Deploy centralized Web security
5. Use a strong system password

Section II: The Administrative Burden of Security

Businesses today spend approximately 20% of their IT budgets on security (CompTIA Research), but to the chagrin of most CIOs, security costs cannot be budgeted at a set amount. This is because recovery from breaches and exploits is not an exact science and remediation can involve numerous man-hours of IT staff work or require the purchase of new security technologies. Add to that the ever increasing burdens set forth by legislative and compliance issues; it becomes easy to determine why budgets for security products and services are spiraling out of control.

- **IT World has reported that the cost of network security breaches could be as high as \$200 billion a year.**
- **The average total cost for companies is more than \$6.3 million per breach – Ponemon Group.**
- **35 states provide regulations that require that companies or agencies to notify affected individuals, such as customers, employees, citizens, students and alumni, when their confidential or personal information has been lost, stolen or otherwise compromised.**
- **Analysts at Forrester Research predict that the market for security information management tools will continue to grow, with demand reaching \$1.18 billion by 2011.**

This, combined with the increasing sophistication of malware, blended threats, corporate identity theft and intellectual property theft, and it becomes very clear that traditional solutions are no longer capable of protecting important resources in an economical fashion.

- **21% of Forrester survey respondents expect to increase their IT security budgets in 2009, while nearly three-quarters of those surveyed expect no cutbacks in their security spending.**
- **The US managed security services market was valued at approximately \$1.3 bln in 2007, an increase of 19.6% over 2006. This figure is expected to increase to \$2.8 bln by 2012, representing a compound annual growth rate of 17.2%, according to IDC.**
- **The top three priorities for 2008 by IT management are improving IT service levels, improving disaster recovery capabilities, and increasing IT security according to Computer Economics' annual study on IT spending.**

If the overhead costs and demands of security continue to grow at such an alarming rate, most IT departments will find themselves unable to offer the level of protection needed in today's complex environments. This leaves little choice for administrators today – new ways to protect corporate assets are needed. Currently most IT departments focus on the combination of dissimilar technologies to protect heterogeneous networks.

With the constant shift in attacks and engineered breaches, it may be difficult to pick the importance of one technology over another, forcing IT departments to create overlaps of protection. In theory, overlapping security products or hierarchical layers of protection prove to be the best way to protect network resources and end-users from security threats. But in practice, many IT Managers are finding that the costs associated with integration and training are starting to far outweigh the perceived benefits, creating another, more serious problem – gaps in coverage. Many are discovering the inevitability of integrating dissimilar products in complex environments to be the lack of addressing every possibility. In other words, the more complex the solution, the more likely it is to encounter unforeseen problems.

A Yankee Group survey of 404 "decision makers" at medium-to-large companies found that half of respondents see security budgets increasing over the next three years. In addition, 40% of the Fortune 500 plan to purchase Web services security products.

Administrators are finding that security products must evolve quickly to keep pace with new threats and attacks, yet that evolution is limited due to incompatibilities, multiple vendor requirements and technical knowledge. For security to succeed, the burden has to be shifted from the IT department to others better equipped to deal with change and the rapid evolution of the threat environment. Further complicating the issue is the fact that businesses of all sizes face the very same threat environment, ranging from the largest of enterprises to the smallest of local businesses. For enterprises, increasing budgets for security solutions and support are becoming less tolerable, while small businesses do not have the capital to deal with the problem in the first place.

Section III: The Disadvantages of Onsite Solutions

Most businesses have come to rely on boxed security solutions, all of which require some level of integration into an existing infrastructure. Those point solutions may consist of appliances, firewalls, software security products and so on. When integrated properly, that mixture of solutions can offer what may be the best in defense, yet can still suffer from a common weakness: the need for constant monitoring and updating by IT professionals. What's more, the impact of those weaknesses grows exponentially as an IT environment grows and starts to spread out over multiple locations.

Once an organization grows beyond a single location, centralized security becomes an almost impossible task. Multiple branch offices spread out over geographical areas all need their own set of solutions that can operate independently, yet still be centrally managed. This results in a situation that is often contradictory and impossible to resolve easily with onsite solutions.

For single site locations, onsite solutions may be somewhat easier to manage, but can still fall prey to "security solution creep" where circumstances dictate that new solutions be added to the mix to combat new and previously unidentified threats. The problems caused by that unplanned product growth range from budgetary to technical. After all, new features often cost more money and then must be integrated into an existing infrastructure quickly and without problems.

Furthermore, a process to validate the effectiveness of those new solutions must be performed to remove all doubt from the protection equation. That process may dictate the need for extensive testing of new products, the testing of existing products for integration issues and then testing how users and network resources are affected. This is a time consuming and expensive process, which also delays the launch of new protection features that may be needed immediately. Currently, onsite solutions are not able to promise a level of effectiveness that can guarantee the protection of data systems and users, or the elimination of security issue remediation. The reasons for that are numerous – ranging from the failure to protect from zero-day threats to effectively deploying patches before breaches occur.

Online attackers are increasingly using zero-day flaws and targeting a wider array of applications, according to the annual “Top 20 Security Attack Targets Report” from the SANS Institute.

Much like a modern day army, security benefits from strength in numbers. In other words, the larger the security force, the less likely a breach is to occur. While strength in numbers is a simple concept, it is almost impossible to accomplish using onsite solutions with today's IT budgets and staff levels. The strength needed for IT security (hardware and personnel) is beyond most corporate entities, especially so for small and medium enterprises.

For those enterprises attempting to resist information technology threats, a new methodology must be considered, one where the strength of the many can be leveraged by the smallest of corporate entities. Currently, the only way to accomplish that objective is to leverage security solutions offered in the cloud, or security SaaS solutions. A security SaaS offering provides the protection of the many by spreading the burden of cost out among the subscribers. In other words, businesses can benefit from a high-end solution, without having to pay the full costs of that solution.

Section IV: Security Challenges of “In-the-Cloud Security”

Businesses are encountering an ever-increasing number of security threats. That increase is an unintended side effect of Web 2.0 technologies, such as cloud computing, SaaS and hosted applications. Each of these technologies require connections via the Internet, which in some cases start out with an unsecure, unencrypted connection to the Web.

Forrester Research reports the adoption rate of Web 2.0 technologies by IT is actually stronger in enterprises than it is in SMBs, with 42% of enterprises utilizing Web 2.0 technologies like AJAX, Flash, etc. to 32% of SMBs.

While Web 2.0 technologies can be a boon to productivity, there is an increased administrative burden in the form of security. Most Web 2.0 services allow users to bypass corporate controls and access applications directly, leaving only local (PC-based) security and possibly the corporate firewall between the end-user and the application. The problem worsens when mobile users and remote offices are added to the equation. Simply put, premise-based security solutions cannot scale beyond the corporate edge and can completely fail with remote, mobile or branch office users.

One way to address the problem is to use some of the very same technologies that enable the problem. In other words, use hosted security solutions to protect users from the security problems created by hosted applications. That concept completely changes the dynamic of dealing with security. In practice the user is always protected, regardless of what they are connecting to on the Internet. Ideally, a fully implemented security SaaS suite will handle and control all Web traffic between the user and their destination, regardless of the user's location and connectivity methods.

Security SaaS adds multiple layers of protection and offers the additional benefit of protecting users while they browse the Web, preventing the spread of malware, intrusions or other serious threats from beyond the edge of the network.

Section V: The Never-ending Battle

One of the biggest problems with security solutions is the administrative overhead and the need for constant updating. Anti-malware applications need daily or more frequent security signature updates to be effective, while filtering applications need constant category refreshes and URL database updates. With a new domain coming online every second, traditional URL filtering solutions can't keep up. Operating systems and applications also need frequent patching and security fixes to prevent compromises. When the administrative burden is added up, it becomes evident why premise-based security becomes so expensive and demonstrates very little ROI. What's more, if a particular security vendor is not

on the ball, an organization can become exposed to zero-day threats, where the threat goes active before the security vendor has had time to analyze it and create a patch or signature update to combat it. In many cases, the new threat may last beyond a single day because vendors may be slow to react or administrators may be slow to update their onsite solutions.

The simplest way to resolve these issues is to switch to a security solution that is updated automatically, frequently and effectively. Security SaaS solutions meet all of those requirements, maintaining a 24x7 staff and advanced technologies to keep security on the cutting edge of protection and ahead of the zero day threat dilemma. A security SaaS solution offers an additional advantage in the form of effective integration. An administrator no longer has to keep track of multiple solutions and multiple updates; the burden is shifted to the security services provider, which actually has the staff, security expertise, and advanced technology to keep an integrated solution up to date and effective.

51% of IT decision-makers surveyed said their companies have been infected by a Web-based virus such as the Bagel Worm or JS Scob. Furthermore, 16% said the virus took a week or more to remediate. - Web@Work survey conducted by Harris Interactive.

Security SaaS solutions also offer identifiable ROI in the form of analysis and reporting. Administrators can correlate protection with traffic and demonstrate to management how a SaaS solution has protected the enterprise from harm. Common criteria reports such as virus interceptions and filtered sites offer proof of productivity, while reports on signature and patch updates demonstrate the hours saved by shifting the administrative burden out to the service provider. Additional reports on breaches prevented, intruders detected and stopped and overall network traffic further solidify the value of a fully managed SaaS solution that is completely budget-able and where costs are kept predictable.

Section VI: Protection in a Distributed Environment

As IT infrastructures grow more diverse, administrators have to consider how they will protect a distributed environment. Generally speaking, the more distributed an environment, the more difficult it is to secure, which translates to increased expenses for security. That is not to say that a distributed environment is not without its advantages – distributed systems are often more resilient, provide a better path to business continuity and offer efficiencies not achievable in a large data center. Distributed environments excel at bringing data processing closer to the user, both physically and virtually, but they also can be hard to control and secure.

The ideal security solution for the distributed environment can place the security services as close as possible to the distribution point and the end-user. The best practice is to create that distributed security solution by using a centralized solution virtually. In other words, by relying on a security SaaS platform where security is both distributed and centralized at the same time – virtually, the best of both worlds – enabling administrators to set policies once and automatically apply and enforce them across multiple distributed locations.

Executive Summary

The Security SaaS model has several advantages over traditional onsite solutions, making the technology the choice for today and the future for securing networks of any size. This is especially true for securing the Web browsing experience. Web security SaaS provides enterprises with:

- **Improved Policy Definition, Distribution and Enforcement:** Security SaaS offers a natural path to integrated management. For Web security SaaS specifically, policies can be set once in the management interface and automatically be distributed to multiple locations, offering centralized policy setting and enforcement. Premise-based solutions rely on sometimes problematic policy rollouts and management element synchronizations, making premise-based security less than reliable when it comes to policy enforcement and changes.
- **Improved Distributive Security Technology:** A SaaS solution enforces security at the endpoint regardless of the location, equipment deployed and infrastructure environment. Security SaaS solutions allow any connected device to be fully protected and controlled by policies, even if those devices are not located in static environments. Physical location no longer plays into the effectiveness of security, because the analysis and security decisions take place in the

cloud. Premise-based solutions rely on physical connections between the endpoint and the premise security device, complicating the ability to protect mobile or remote workers who might be accessing the Web from a laptop or other.

- **Reduced Cost of Ownership:** SaaS solutions shift the burden of expense from facilities to operations, where costs can be budgeted based upon the level of service needed and not the physical devices put in place. While premise-based solutions require expenses for hardware, software, integration and maintenance, SaaS solutions are budgeted based upon a single line item encompassing service. What's more, SaaS solutions are priced based upon capacities needed (or in use) and not upon anticipated but unidentified growth potentials. In other words, the SaaS model encompasses actual usage, while premise-based solutions must be budgeted to handle possible maximum usage scenarios.
- **Reduced Operational Costs:** SaaS solutions are priced based upon a service model, where a set fee is completely inclusive of all services desired. Security SaaS eliminates the need to budget for additional support, technical training, upgrades (software and hardware), enhanced support contracts, administrative overhead and the many other hidden costs associated with premise-based or traditional solutions.
- **Enhanced Deployment:** SaaS solutions are designed for instant deployment, needing little or no administrative involvement. Most of the incidental costs of implementing software and hardware are eliminated by the SaaS model. The burden of integration becomes associated with the SaaS provider and not the in-house IT department. Premise-based solutions require extensive administrative and IT department involvement, which increases costs and slows deployments, perhaps leaving a larger window open to security problems. SaaS solutions allow employees and IT personnel to focus on their core responsibilities, instead of being sidetracked by the management and remediation requirements of premise-based solutions. Where premise-based solutions can add hours, if not weeks, to the security deployment process – SaaS solutions accomplish the same goals with efficiencies that are measured in minutes.

About Purewire

Headquartered in Atlanta, Purewire™ secures business and social interactions on the Web. Founded by veteran security industry entrepreneurs, the company offers Web security-as-a-service to increase ROI and lower the total cost of security for businesses. Purewire is the only vendor that addresses the complete Web security threat landscape, providing unique algorithms and scalable services to protect users from malicious People, Places and Things on the Web™. For additional information, please visit www.purewire.com.

Comprehensive Security for Today's Enterprise

The Purewire Web Security Service is a multi-tenant Web security SaaS that protects users as they browse the Web, regardless of location or physical device.

- (1) Purewire Enterprise™ protects users when they are in the office,
- (2) Purewire Remote™ protects employees who are on the road using a laptop or other public computer,
- (3) Purewire Mobile™ protects employees accessing the Internet via mobile devices, and
- (4) Purewire Research™ provides access to anytime, anywhere data and information via a Web portal.

For a free trial evaluation of the Purewire Web Security Service, please contact us today and mention this white paper:

Purewire, Inc.
14 Piedmont Center NE, Suite 850
Atlanta, GA 30305
404-963-9000
info@purewire.com