webroot®

PUBLICATION DATE
11 February 2011

Security as a Service: Business Decision Factors

Industry Research

Table of Contents

Introduction

In a companion paper, we show how Security as a Service (SaaS) protects small and midsize businesses from an unprecedented storm of malicious code, while escaping the tradeoff among security, performance, and cost that premise-based security forces on them. This paper looks at the business issues in SaaS: the value it unlocks, the costs—direct and indirect—it avoids, and the corollary benefits like efficiency and agility it supports.

Businesspeople are concerned about the rising number and severity of IT security risks not just because they are dangerous but because of their business impacts: direct financial losses, data theft and inadvertent disclosure, productivity lost to downtime and repair activities, network and system capacity consumed by defenses. And external threats are just part of the story—attempts at premise-based data loss prevention, regulatory compliance and legal discovery introduce costs and risks disproportionate to their business value. Add to those the time, money, and expertise needed to manage barely adequate defenses, and IT security looks like an expensive burden for all but the largest businesses.

Similar concerns have led businesses to adopt SaaS options for e-Learning, CRM, Project Management, ERP, and other complex applications that require specialized tools and knowledge. Security as a Service is a logical next step. Three families of online services—Email Security, Web Security, and Email Archiving—use infrastructure, skills, and processes that are far more effective and economical deployed "in the cloud" and delivered as services.

This paper reviews the business value of IT security, illustrates the business case for SaaS over "do it yourself" premise-based solutions, and outlines what to look for in SaaS solutions you can adopt with confidence and count on as you grow.

Security concerns are business issues

IT security isn't an end in itself—it's valuable because it protects or extends the value that businesses create. And for the small and midsize businesses that create most of the world's economic value, IT security plays a major role.

BUSINESS EXPERIENCE

An August, 2010, Webroot study showed that compared with all firms, small and midsize businesses experienced higher rates of every major class of email and Web attack:

- Virus or worm: 86%, vs. 50% for all firms
- Spyware, including Trojan, keylogger, system monitor, rootkit: 78% vs. 50%
- Hacker attack: 53% vs. 20%
- Phishing attack: 72% vs. 35%

These attacks had significant business impacts, ranging from loss of sensitive data (at 55% of firms), to disrupted business activities (at 81%) and time lost to repair and remediation (at 90%).

BUSINESS PRIORITIES

The Webroot research also showed that the priorities of these firms align closely with their security experience, and reveal a consistent focus on business issues over technology alone:

1. Data security and confidentiality rated "high" or "very high" importance—79% of firms

2. Business continuity/disaster recovery—74%

3. Protecting business email against malware—72%

4. Protecting mobile employees against spam and malware—74%

5. Compliance with regulations and standards—68%

Some of these priorities fall outside what a specialist might call "security"—a fact that reflects both the convergence of email, Web, and data threats, and the business focus on impacts over process and technology issues.

Comparing on-premise security and SaaS

Protecting data, operations, communications and employees rank near the top of surveyed companies' priorities. But on-premise solutions capable of meeting respondents' requirements are often beyond the resources they can reasonably devote to them.

Up-to-date on-premise security requires substantial investments in experienced personnel—employees or consultants—to reach even the planning stage. Once a plan is in place, the business must deploy additional hardware, software, and personnel before the new solution makes any contribution at all—the steps involved are summarized in the diagram below:

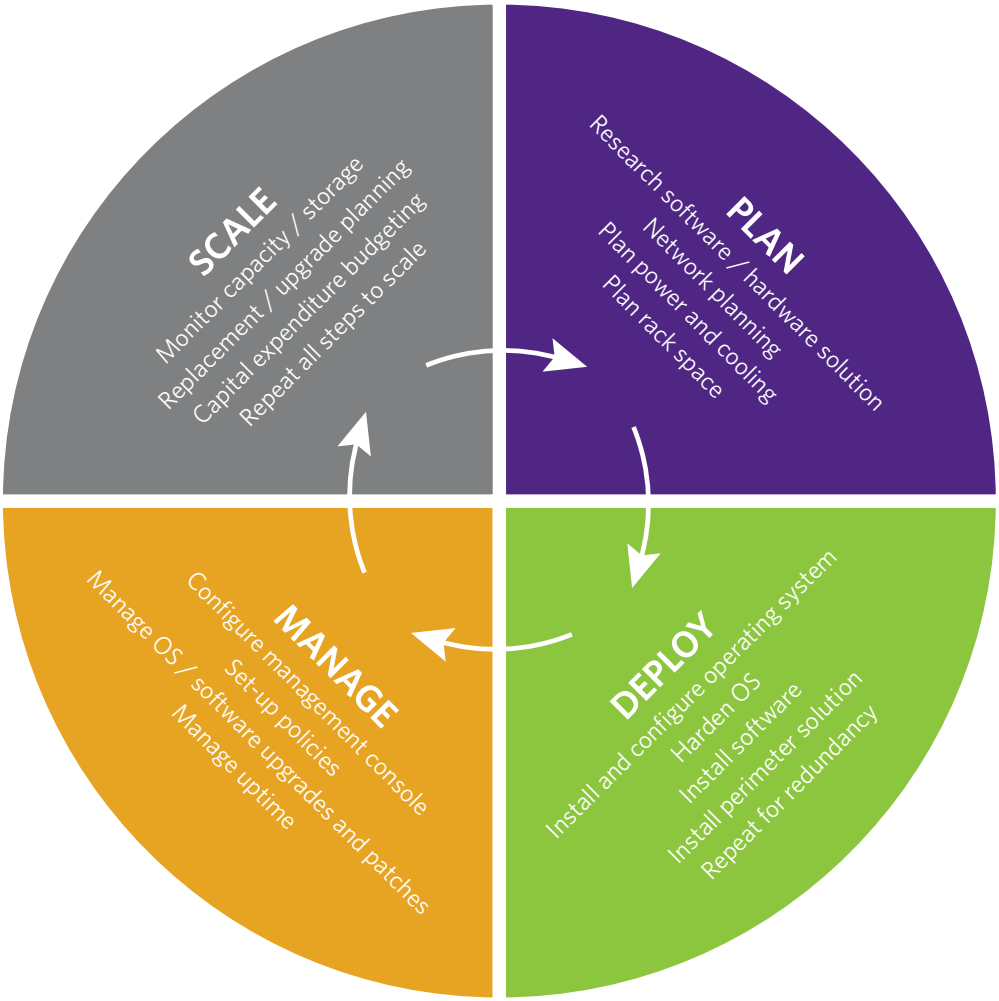

Figure 1: The steps involved in on-premise deployment

> "On-premise solutions capable of meeting companies' requirements are often beyond the resources they can reasonably devote to them.

Costs remain high even after deployment—as the left side of the diagram suggests, management is a significant burden, and scaling or adapting the security solution to meet new business or security demands requires reiteration of the entire process. Business and IT managers understand these challenges: in addition to cost, they rank staffing, maintenance and management among the top benefits they expect from Security as a Service.

SaaS—key business factors

High-end Security as a Service operates from a global network of security centers backed by advanced threat research and analysis, and is delivered through state-of-the-art infrastructure. Regardless of how providers package and promote their SaaS offerings, businesses should carefully review them to secure the advantages outlined here. SaaS complements and extends past premise-based security, adding an extra layer of protection, keeping some threats completely outside company networks, and managing premise-based solutions remotely.

REDUCED COST

SaaS applies significant economies of scale—the ability to give many smaller clients the infrastructure, specialized skills, and service levels only a few large companies can afford for themselves. Compared to on-premise solutions, SaaS economies include:

- Reduced burden on company IT staff and resources
- Lower maintenance requirements
- Simplified management: less time, fewer errors
- Rapid deployment, reconfiguration, and upgrade
- No capital expense, maintenance, power, or cooling for hardware
- Consolidation of security solutions with one vendor and support team
- Quick scalability with no capacity ceiling
- No software to purchase or licenses to manage

REDUCED RISK

Much of the value of SaaS comes from routing business email and Web traffic through the provider's networks and data centers instead of directly to the Internet. This approach lets security specialists analyze, filter, and correlate inbound and outbound traffic in depth using the latest technologies.

Broad protection—inbound Web and email protections should include the ability to block targeted and blended threats including spam, virus, spyware, and phishing attacks. Omitting spyware and phishing exposes businesses to multi-pronged attacks and advanced persistent threats, both of which are on the rise. Both signature-based and non-signature or heuristic analysis should be applied in depth to protect against known and unknown malware. Outbound protections should include Web and URL filtering, Internet access controls, as well as inspection for sensitive company or personal content, followed by blocking/quarantine, encryption, and alerting according to company policies.

In-depth protection—SaaS clients should expect more comprehensive analysis at their provider's data centers than they could implement using on-premise solutions. In addition to threat signature scanning and basic heuristics, look for multi-layer antivirus, reputation analysis, blacklisting by server and IP address, spam backscatter protection, zero-hour protection, and more. Sophisticated URL filtering with multiple categories and quota and time controls helps maintain user productivity as well as security.

BETTER CAPACITY AND PERFORMANCE

SaaS delivers protection without big loads on business gateways and networks. Today, that's a big improvement: filtering out spam alone cuts traffic through email gateways up to 90% during a busy month. So when evaluating threat protection, consider both the quality of protection and the performance impact:

Throughput and latency—while SaaS solutions add a "hop" to email and Web traffic and run extra scans and tests, SaaS providers use high-performance infrastructures and offload scanning requirements from clients' slower on-premise solutions. As a result, most clients see net throughput improvement as well as bandwidth savings. In order to maximize your solution's performance, look for SaaS data centers in the same geographic regions as your largest offices, and performance guarantees.

Location of coverage—endpoint protection and remediation will need to be done at the endpoints themselves, and endpoint vulnerability assessment is highly recommended to make sure software is running at current patch levels. But these solutions can be lightweight, update efficiently, and run very fast.

> "In most cases, on-premise deployments simply **cannot match the level of security** provided by most hosted providers.

EXTENDED COVERAGE

An upgrade from premise-based to SaaS security should be more than a haphazard application of security solutions. Look instead for a framework of coherent security policies, consistently applied and enforced, with the option to extend and customize them where your business circumstances require it:

Mobile user protection—premise-based solutions struggle with mobile security, but SaaS doesn't. Direct support of mobile and remote Web users by the nearest SaaS data center protects mobile and fixed systems in exactly the same way, regardless of platform and without intermediate "backhaul" connections between users and on-premise VPN routers, for example.

Content filtering—outbound email data loss prevention can recognize critical words, phrases, and data patterns. Inappropriate content filtering for both Web and email should cover images, including thumbnail images in search engine results. And Web filtering should be effective against "anonymizer" proxies, even user-created one-off proxies.

Application Control—unauthorized use of peer-to-peer (P2P) "sharing" software can be a significant threat to data security. SaaS providers give clients a way to block P2P and other suspect applications, with options to deny applications by default and exempt or authorize individual users.

Customization—default or "starter" policies already in place at SaaS providers cover most requirements, but clients can customize policies with:

- blocking or whitelisting of individual URLs or IP addresses
- custom content dictionaries of terms that are sensitive or suspicious for their individual business or market
- specialized applications that offer opportunities for misuse in specific industries

EFFECTIVE COMPLIANCE

By concentrating infrastructure, processes, and expertise, SaaS services simplify compliance with regulatory and legal requirements:

Data Loss Prevention (DLP)—clients in regulated industries apply content dictionaries relevant to their requirements: HIPAA for medical and insurance companies, PCI for payment-card issuers and processors, EU-US Safe Harbor for companies with customers in Europe, and so on.

Encryption—data loss prevention policies may require encryption of messages that contain sensitive phrases or data as an efficient method for protecting content without blocking messages outright. Encryption is particularly important for clients in professional services, finance, and healthcare, or others who routinely handle confidential or proprietary information.

Archiving—while not strictly a security feature, automated offsite email archiving makes sense from both operational and compliance points of view. It reduces storage waste and clutter, enforces retention policies, maintains a protected, accessible, encrypted record of communications, and supports efficient legal search and discovery.

EFFICIENT MANAGEMENT

With offsite specialists shouldering the bulk of day-to-day security management, IT staff has more time to devote to strategic initiatives, without sacrificing the visibility essential to effective security management.

Management portals—client managers receive instant and continuous access to policies and rules, email and Web traffic flows, and threats, backed by continuously available telephone support to handle questions, issues, or exceptions.

Reports—administrative and management reports should include email and Web traffic, bandwidth use, and activity by department down to the individual user level. Reports should also include objective measurements of performance that are directly related to SLAs.

SaaS providers differ along many criteria in addition to these, and feature-based comparisons can't tell the whole story. But using the framework above will help potential clients uncover key differences among providers, illustrate their business philosophies and approaches, and help guide clients to a confident decision.

Effectiveness and expectations

Industry analyst Aberdeen Group compared on-premise and cloud-based security models at 58 companies in depth for a year—using both objective measures and subjective evaluations—and found that companies using cloud-based solutions enjoyed:

- 58% fewer malware infections
- 78% fewer Web site compromises
- 45% fewer instances of data loss or exposure
- 45% less security-related downtime
- 93% fewer audit deficiencies

And although both groups reduced Help Desk calls, companies using cloud-based SaaS reduced them at a 42% faster rate.

As decentralization, mobility, and cloud computing continue to dissolve the perimeters companies once relied on to protect their information and infrastructure, more companies will turn to cloud-based SaaS. Beyond the logical appeal of moving protection to where the threats are, basic economies of scale will improve companies' security posture. Cloud-based SaaS offers:

- Consistent, industry-proven policies and practices
- Higher-performance technologies and resources deployed against threats
- More consistent, effective management
- More experienced, better-trained staff, and less "churn"

- Threat research integrated into protection
- Rapid, almost unlimited deployment and scalability

Decisions about SaaS involve technology, but they are fundamentally business decisions. SaaS providers make them easier by keeping their services *transparent* and *accountable:* offering business-relevant, objective metrics and SLAs backed by performance guarantees.

Why Webroot?

Webroot is a leading provider of IT security solutions for businesses and consumers worldwide, with a network of fully-staffed, specialized security data centers throughout North America, Europe, and Asia. Our powerful suite of hybrid and cloud-based Software as a Service (SaaS) offerings integrate security, data-protection, archiving, management, and compliance solutions designed, implemented, and priced to match the requirements of small to midsize businesses. We guarantee our performance, and give you the tools you need to measure it.

> Decisions about SaaS involve technology, **but they are fundamentally business decisions.**