WHITE PAPER:
BENEFITS OF CHOOSING CLOUD SECURITY

Hosted Solution vs On-Premise

Benefits of Choosing Cloud Security

Who should read this paper

IT Decision Makers, IT Managers, Network Administrators

Symantec.cloud

WHITE PAPER: BENEFITS OF CHOOSING CLOUD SECURITY

Benefits of Choosing Cloud Security

Hosted Solution vs On-Premise

Contents

Combating Advanced Threats with Advanced Security Technology

Email, web, and instant messaging (IM) are among the most pervasive tools for conducting business, impacting arguably every aspect of conducting business for organizations of all sizes. Not only are they used for everyday communications between employees, customers and business partners, they have come to form the backbone of many critical business processes. These “electronic interactions” have become indispensable tools, as critical as any other part of the company infrastructure.

Due to their integral role in conducting business, these tools are favoured points of entry for criminal activity that disrupts operations and exposes businesses to a multitude of threats. Attacks delivered via viruses, spam, Trojans, spyware, phishing and other threats to electronic interactions have become commonplace – and are costly. On May 29, 2009, the United States Federal government issued a report stating that between 2008 – 2009 American business losses due to cyber attacks had grown to more than $1 trillion worth of intellectual property.

Cybercrime remains a very lucrative endeavour. As such, criminals are using increasingly sophisticated tactics; this requires increased investment in resources and expertise on the part of businesses everywhere to combat threats.

Not all threats come from outside the business. The messaging and communication tools that have so much potential to facilitate business also have the potential for misuse that can result in improper use of company assets. If not properly managed, they can even pose a legal risk when misused by employees who operate in avoidance or lack of acceptable use policies.

Today, IT managers from businesses of all sizes find themselves at a crossroads. They must define their approach to addressing security risks, selecting the technology that will help them most effectively:

- Protect their businesses from internal and external threats
- Manage increasing and often unpredictable costs
- Scale as their needs change

This paper examines three solution types that are commonly implemented to address these challenges: onpremise software, on-premise appliances, and hosted security offerings, and provides an overview of their effectiveness in common usage scenarios, as well as a discussion of their impact on overall IT budget. The paper concludes with a discussion of increasing adoption of hosted security services and a summary of the key reasons why many businesses of all sizes are selecting this as a model for protecting their businesses from cyber threats.

Hands-on Security: On-Premise Software

Setup and administration

Licensed security software is installed between the network boundary and email servers and clients. This usually involves configuring firewall ports so that email, web and IM traffic can flow properly. Specific hardware may be required for a management server.

Ongoing management

For the solution to be most effective, an organization must keep its software solution up-to-date with the latest signatures to combat evolving threats across multiple technologies: today's threats not only come in the form of misleading or malware laden email, but can enter your company through unprotected web and IM usage. And, administrators must plan for system redundancy and additional hardware to scale the solution as required.

Staffing

This type of solution typically requires at least one IT resource who will be responsible for deploying agents to endpoint clients and administering any management console deployed on site.

Security in a Box: On-Premise Appliances

Appliances seek to solve the inconveniences and cost of obtaining, deploying and managing custom software packages. An appliance is one or more hardened servers physically installed between the network boundary and internal resources like the email servers and endpoint clients. As the company's mail, internet usage, and security needs grow, additional appliances can be purchased to scale the solution as each appliance has the capacity to process only a finite amount of traffic.

Setup and Administration

As compared to on-premise software which typically must be installed onto a shared or dedicated piece of hardware, appliances come ready "out of the box." Most providers seek to offer customers a plug and play experience where the administrator can simply deploy the hardware, hook it up to power and networking, and then complete some minor setup steps. Administrators then configure the appliance and their network (firewalls, for example) to properly route traffic in and out of the business.

Ongoing Management

With any new piece of hardware comes additional concern for management. Hardware can fail, and that can result in downtime or periods of unprotected electronic interactions. Updates are applied, by either a service contract with the vendor or by customer IT staff, and additional appliances may be needed as the business traffic scales. As with on-premise solutions, IT organizations must plan for redundancy and budget for additional hardware as their requirements grow.

Staffing

An on-premise appliance will generally require at least one IT individual who will manage appliance configuration, interactions with the vendor for repair or downtime issues and the initial unit deployment and upgrades.

Security in the Cloud: Hosted Solutions

A hosted service provider uses a network of data centres located at major Internet hubs to process and monitor electronic interactions for its clients. Hosted solutions are designed to provide protection and efficiency by moving critical operations into provider-maintained facilities and thus have less impact on customer operations.

Setup and administration

Hosted services are simple to set up and administer and generally work with any mail client or server configuration, regardless of geographic location.

Once a customer's specific requirements have been determined, the service is typically enabled through a modification of the client's settings (DNS and mail server settings for email, and/or proxies for web and IM), this set up process can be significantly faster than either packaged software or appliances. For web and instant messaging protection, a policy change or package can be implemented and distributed to endpoint clients. There is often no additional hardware or software required. Once set up is completed, data is routed through secure datacenters and analyzed for malware, viruses and spam before reaching their destinations.

Ongoing management

Administration is typically handled through a web-based portal that provides management information, configuration tools, service statistics and reports in real time, enabling the administrator to monitor how the service is performing. All service updates and upgrades, as well as threat protection, are administered in real-time by the managed service provider, requiring no additional resources from the client.

Although the infrastructure and traffic are moved to the hosted provider, customers retain significant control over configuration, monitoring and management of policies and services.

Staffing

Management of a hosted solution typically requires little IT knowledge or interaction, beyond the initial configuration changes required to direct the business' electronic traffic through the service provider. As a result, these types of solutions rarely require dedicated IT staffing.

Businesses Like Yours are Moving to Hosted Solutions

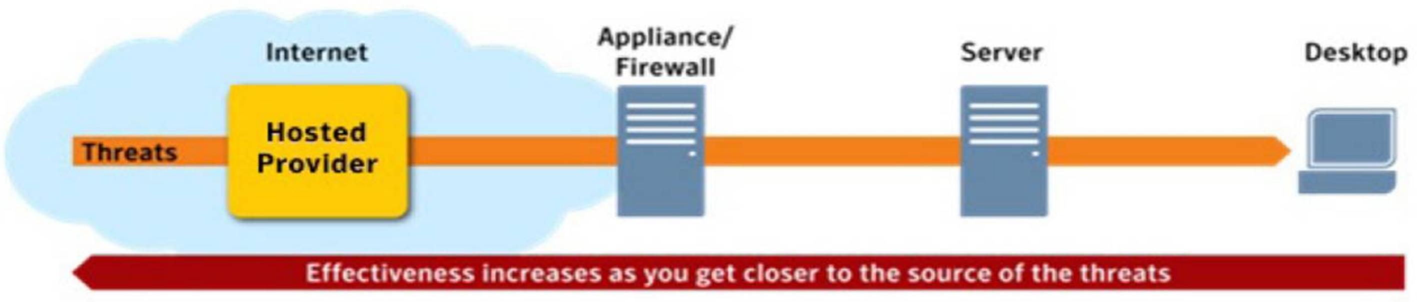
Globally, companies of all sizes are moving to the hosted services model which is also known as Software as a Service.

Companies are making the move to the hosted services model because they benefit from:

- Gaining access to security and management expertise
- The predictable cost of a subscription service, and often have lower startup costs
- The ability to virtually eliminate the need for service-related hardware and software investment

Your security solution needs to always be at the cutting edge.

With new spam and virus techniques emerging almost daily, enterprises have realized that they neither have the core competency nor the financial wherewithal to keep investing personnel, time and money into deploying new countermeasures at a rapid rate. However, dedicated hosted services vendors can devote frontline personnel and massive processing power to fighting emerging threats and can seamlessly implement them to protect enterprise clients in real-time.


Internet
Threats
Hosted Provider
Appliance/ Firewall
Server
Desktop
Effectiveness increases as you get closer to the source of the threats

Because email, web and IM content is scanned and filtered at the Internet level, it helps to prevent malicious code from ever entering the corporate network. Millions of emails and web requests are processed and filtered by the service daily, data is collected, changing threat characteristics are identified, and new signatures are implemented automatically in real-time. While appliance-based solutions and hosted services both quarantine spam, a hosted service houses this data away from the corporate network.

Cost savings can be a large differentiator for a hosted solution.

Hosted services can have a lower startup cost, reduce the need for upfront hardware and software investments, long-term infrastructure commitments, support contracts and the unpredictable cost of dedicated, knowledgeable internal staffing.

By using a hosted service, clients can avoid costs associated with other solutions, such as:

- Complex hardware or software
- Increased storage and bandwidth
- Dedicated technical staff to manage the solution
- Regular software updates
- Routine updates to spam and virus definitions

Important Considerations when Evaluating a Hosted Security Service

Providing metrics for your business: Service Level Agreements
Hosted services are delivered and maintained via third parties, as opposed to on the customer premises. This means customers using hosted services should demand a reliable Service Level Agreement (SLA) as a means of ensuring service accuracy, efficiency and availability.

While all of the solutions discussed so far provide some form of protection against threats, the hosted solution model typically is the only one to clearly enumerate and be accountable for protection levels for services being delivered. This SLA, usually agreed to in the service contract for the service, calls out a series of metrics that the service provider agrees to meet, that can include:

- Accuracy of virus detection
- Accuracy of spam blocking
- Performance levels, such as latency of email and web traffic
- Uptime of the service

If these levels are not met, customers can refer to the Service Level Agreement for some form of redress, such as a money-back remedy.

Expert support available when you need it

Hosted security services can provide excellent protection levels, and some also provide customers with access to a dedicated support team for the solution with high levels of training and expertise on the technologies involved. Potential users of hosted security services should evaluate their security requirements before entering a service contract with a provider. Customers should ensure that they have access to live technical support resources if required, in addition to any ticket or web based systems.

Conclusion

With new virus, malware and spam techniques emerging almost daily, enterprises have realized that they neither have the core competency nor the financial wherewithal to keep investing personnel, time and money into deploying new countermeasures at a rapid rate. However, dedicated hosted services vendors, such as Symantec.cloud, can devote frontline personnel and massive processing power to fighting emerging threats and can seamlessly implement them to protect enterprise clients in real-time. Additionally, a hosted service clears away the concerns over cost of ownership by having a fixed and predictable cost.

About Symantec.cloud

Symantec.cloud, division of Symantec Corporation, offers customers the ability to work more productively in connected world. More than 31,000 organizations ranging from small businesses to the Fortune 500 across 100countries use Symantec.cloud to administer, monitor, and protect their information resources more effectively. Organisations can choose from 14 per-integrated applications to help secure and manage their business even as new technologies and devices are introduced and traditional boundaries of the workplace disappear. Services are delivered on a highly scalable, reliable and energy-efficient global infrastructure built on fourteen datacenters around the globe.

SINGAPORE
6 Temasek Boulevard
#11-01 Suntec Tower 4
Singapore 038986
Main: +65 6333 6366
Fax: +65 6235 8885
Support: 800 120 4415
www.symanteccloud.com.sg

Symantec helps organizations secure and manage their information-driven world with **security management**, **endpoint security**, **messaging security**, and **application security** solutions.