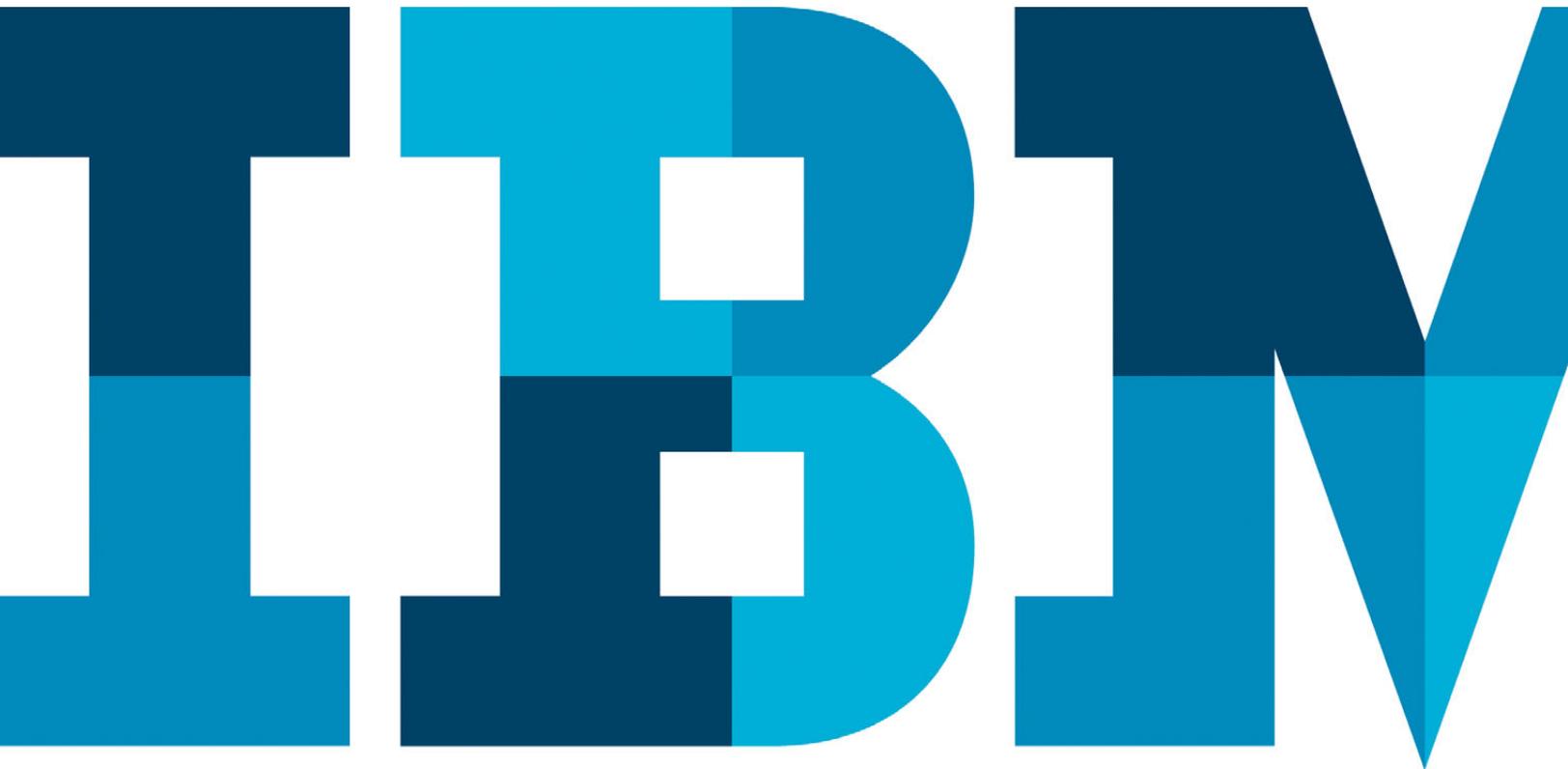


Leveraging security from the cloud

The who, what, when, why and how of cloud-based security services



Introduction

Today's executives understand the need for information security but still struggle to manage the cost and complexity of a myriad of security technologies for everything from threat prevention to email security, vulnerability scanning and security event and log management. While important to a comprehensive security strategy, implementing and managing these solutions can divert IT resources from other critical initiatives. And organizations with smaller budgets may not even be able to consider sophisticated defense-in-depth security solutions. Cloud computing provides a delivery model for security that addresses many of these challenges for businesses large and small.

Cloud computing is a flexible, cost-effective and proven delivery platform for providing business or consumer IT services over the Internet. Cloud resources can be rapidly deployed and easily scaled, with all processes, applications and services provisioned "on demand," regardless of user location or device. As a result, cloud computing helps organizations increase service delivery efficiency, streamline IT management and better align IT services with dynamic business requirements.

When it comes to delivering information security, cloud computing provides several advantages relative to on-premise security software and appliances. Cloud-based security services (otherwise known as hosted security or security software as a service) provide security functionality over the Internet. The customer does not take ownership of security applications but rather subscribes to a total solution that is delivered remotely. There are no hardware/software licenses to purchase and no associated maintenance fees. The cloud delivery model also helps reduce security complexity as organizations will not be faced with a proliferation of security devices and technologies to manage, configure and patch. In many ways, consuming

security from the cloud offers customers the best of both worlds. They gain access to sophisticated security technology and up-to-the-minute security intelligence without the capital expense, overhead and management responsibility associated with on-premise solutions.

Discovering the "who, what, when, where, why and how" of cloud-based security services reveals how security can be used to reduce risk, optimize resources, improve flexibility and address regulatory requirements—without breaking the bank.

Who benefits from security delivered via the cloud?

Security threats and weaknesses do not recognize vertical industry boundaries or discriminate between small and large companies. However, advanced security technologies are usually confined to larger organizations with the budget and expertise required to install, manage and monitor advanced enterprise solutions. As a result, many organizations lack protection against new threats based on a shortage of resources, not for intent or negligence.

Cloud-based security services benefit the largest enterprises, as well as small and medium-size businesses. Relative to on-premise security software, cloud security requires little to no up-front capital investment and deployment costs; and the cloud delivery model lowers ongoing operational management costs. It also satisfies risk management needs across industries—from government to retail to manufacturing.

In addition to reducing costs and addressing risk management requirements, cloud security services help to enable a customer's limited operational resources to direct their efforts towards more strategic initiatives that drive real business

value. Compared to traditional, on premise security implementations, organizations leveraging the cloud spend less time managing systems, troubleshooting technical problems, and responding to the most recent security threat.

What are cloud-based security services?

Cloud-based security services are delivered remotely to provide security functionality and intelligence from a remotely located provider. They combine managed services, technology and security intelligence to integrate security with existing business processes, prevent attacks and misuse, address key stakeholder demands, and meet environmental changes. Cloud-based security services enable clients to perform routine security activities more efficiently and cost-effectively by utilizing technology and infrastructure provided by a trusted third party. They help clients contain costs with flexible pricing based on usage. The cloud security service provider takes responsibility for application functionality, deployment, performance and maintenance, liberating the client from these burdensome activities.

Cloud-based security services offer the following advantages over traditional security deployments:

- No expensive, on-premise security hardware to purchase, install and maintain
- No stand-alone software to constantly update and patch
- Rapid deployment and self-service through a web-based portal
- Ability to scale and expand security coverage quickly, without investing in additional infrastructure
- Flexible, service-oriented pricing and service level agreements

Traditional approaches to security require the purchase of multiple security technologies and management systems, along with manpower for integration, configuration and patching. Cloud-based services reduce those expenses and provide an ideal delivery method for many external security functions, including:

- Vulnerability scanning
- Web/URL filtering
- Security event management
- Security log management
- Email security

In addition to security functionality, cloud-based security services also provide up-to-the-minute security intelligence and analytics to keep all security technologies patched and up-to-date. For example, a company that purchased an email security appliance three years ago may face challenges keeping the security software updated or risk making the software obsolete. By using cloud-based security, the service evolves over time, always up-to-date with the latest functionality and software content.

When do cloud-based security services provide a real advantage?

The flexibility of cloud-based security services can transform the way businesses operate, aligning security with evolving business requirements like never before. The cloud-based advantage becomes clear whenever organizations experience a change causing them to reassess, reprioritize and reconfigure security. For example: it provides security and business process advantages in the event of new government regulations, an acquisition, or the addition of a new business unit and/or system. In such cases, cloud security services work fluidly in a changing IT environment without requiring the customer to divert valuable IT and security resources from other critical initiatives.

Where do cloud-based security services work best?

Wherever businesses have Internet connectivity and want to protect information assets, cloud security services will work. Whether applied globally, at corporate headquarters or only for remote locations, the choice is driven by business requirements. Companies don't have to commit to a large-scale deployment with cloud security services. Instead, they can selectively test the delivery model by starting with hosted security at a particular location or for a certain segment of the IT infrastructure, while still managing other aspects of security internally. Regardless of whether a business chooses cloud security services to protect a single data center or the entire IT infrastructure, it will have access to all cloud security service capabilities, including advanced analysis and correlation, artificial intelligence, industry-leading security expertise and a web-based management portal.

Why do organizations need cloud-based security services?

Cloud security services provide protection in a simpler, more efficient and inexpensive manner that empowers customers to focus resources on their primary business. The cloud-based delivery model can transform an organization's approach to security, making security decisions more strategic and aligning security technology with evolving business requirements like never before. With a centralized portal view of security that also provides integrated security intelligence, customers can

make better educated business decisions about how to reduce risk. The cloud security service provider does the heavy lifting and the day-to-day busy work, but the customer maintains control of security posture.

With cloud security services, customers have a consolidated view of business security posture, and a central resource (a security portal) for security-related information. Security event data is only valuable if businesses can analyze it in order to take corrective action. With a consolidated view of security posture delivered via the cloud, businesses now have the flexibility to report on the number of remediation tasks assigned and completed, the number of vulnerabilities reduced, and the cost savings associated with cleaner traffic and more efficient use of bandwidth.

The flexibility and robustness of a cloud security services portal also improves regulatory compliance efforts. The information needed for annual audits—vulnerabilities, security events, log files, etc.—is captured and maintained in a forensically sound manner. For auditing and investigation, the information can be accessed from the central portal faster and easier than having to pull from various management consoles.

The cloud-based delivery model leverages existing technology investments such as routers, application servers and security software. Cloud security services scale for growth, staff changes and shifts in business focus. This approach speeds time to protection, reduces demands on internal resources, enhances profitability and increases focus on operational excellence.

How to select a cloud-based security service provider?

An effective service provider possesses the right combination of service delivery experience, managed services, technology and security intelligence. Cloud security services should be delivered by security-focused experts that offer:

- Proven experience delivering security functionality via the Internet
- A central portal where customers can view their security posture at any time
- A complete managed security services platform including device management and cloud-based security services
- A full suite of security technology for the entire IT infrastructure
- Real-time, proactive security intelligence on threats and vulnerabilities
- The ability to work with existing infrastructure and security technologies
- An understanding of how risk management affects business processes like application deployments, compliance management, supply chain and more
- A strong audit and compliance posture that ensures alignment with your organization's needs
- A global delivery footprint that provides global geographic coverage and continuous service availability

Cloud-based security services from IBM Managed Security Services

IBM has been at the forefront of cloud computing since its inception. And IBM is a proven provider of cloud security services with nearly a decade of experience using this delivery model. As the trusted security advisor to thousands of the world's leading businesses and governments, IBM has been at

the forefront of security technologies like vulnerability assessment, intrusion prevention and virus prevention. And IBM was a pioneer in offering cloud-based vulnerability management, security event and log management and in providing clients with a web-based centralized customer portal for all their cloud-based services as well as their device management managed security services.

This portal, called the IBM virtual security operations center (Virtual-SOC) customer portal, gives clients better visibility and control over their entire security infrastructure. Customers use the Virtual-SOC portal as their single command and control center for all their IBM cloud security services as well as their device management managed security services. The secure web-based portal empowers clients with the intelligence, tools and capabilities necessary to make real-time decisions to improve their security posture. This feature-rich portal provides organizations with a centralized command center for monitoring and controlling their security operations across the entire enterprise. Available anytime, anywhere, the Virtual-SOC portal integrates security intelligence from the IBM X-Force® security intelligence team, early-warning threat analysis services, customized reporting and interactive client/security operations center communications enabling collaboration between clients your organization and their team of the IBM security experts.

IBM security products and services are based on the proactive security intelligence of its X-Force research and development team—the unequivocal world authority in vulnerability and threat research. In addition, IBM has the business expertise to help customers align security and risk reduction with existing business processes.

Cloud-based security services from IBM Managed Security Services include:

- **Hosted Security Event and Log Management** – compiles event and log files from network applications, operating systems, and security technologies into one seamless platform; includes integrated workflow and analysis capabilities, and seamless off-site storage.
- **Hosted Vulnerability Management** – combines managed scanning service for discovery and remediation with expert workflow and case management; helps demonstrate compliance.
- **Hosted Email and Web Security** – provides 24x7x365 cloud-based protection against spam, worms, viruses, spyware, adware and offensive content
- **IBM X-Force Hosted Threat Analysis Service** – delivers customized security intelligence based on threat information from the X-Force research and development team.

The cloud-based security services offerings from IBM are also complimented by a comprehensive portfolio of traditional managed security and professional services solutions.

For more information

To learn more about cloud-based security services from IBM Managed Security Services, please contact your IBM sales representative or IBM Business Partner, or visit the following website:

ibm.com/services/us/index.wss/offerfamily/iss/a1026954

Additionally, financing solutions from IBM Global Financing can enable effective cash management, protection from technology obsolescence, improved total cost of ownership and return on investment. Also, our Global Asset Recovery Services help address environmental concerns with new, more energy-efficient solutions. For more information on IBM Global Financing, visit: ibm.com/financing



© Copyright IBM Corporation 2010

IBM Corporation
New Orchard Road
Armonk, NY 10504
U.S.A.

Produced in the United States of America
July 2010
All Rights Reserved

IBM, the IBM logo and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at ibm.com/legal/copytrade.shtml

Other company, product or service names may be trademarks or service marks of others.

The customer is responsible for ensuring compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the reader may have to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law or regulation.



Please Recycle
