WHITE PAPER

CHOOSING THE RIGHT CLOUD PROVIDER FOR YOUR BUSINESS

Four Steps for Evaluating Security and Reliability in Cloud Environments

The appeal of cloud computing for small and medium businesses (SMBs) comes from its power to flexibly and affordably deliver applications and data from anywhere with an Internet connection. The cloud offers as much computing capacity as you need without the expense of owning and managing your own servers. And the cloud's ability to make data available on demand lets you satisfy customer needs better and faster.

With its promise of easy data access through mobile connectivity, it's natural to have some concerns about the security of cloud computing. And with cybercrime regularly making headlines, it's sensible to get informed about your best choices for protecting and growing your business.

In this paper, we'll examine the challenges of managing and securing your own servers. And we'll walk you through some steps to finding the right cloud provider to secure your data while it's in the cloud.

HACKERS DON'T DISCRIMINATE ON BUSINESS SIZE

You may think your business is below the radar of hackers, but that's not the case. Enterprise breaches usually garner the big headlines, but in fact, businesses with fewer than 100 employees were primary targets for hackers in 2010, according to Verizon's 2011 Data Breach Investigations Report (DBIR)[1]. Payment card data and authentication credentials proved to be the most popular targets, but nothing was immune from attack—including personal information, intellectual property, company reports, bank account records, and classified information.

Verizon Business is a global IT, security and communications solutions partner to business and government with one of the world's most connected public IP networks. Our broad range of strategic solutions, services and expertise can help you improve infrastructure and application performance, secure your data wherever it is, create a collaborative environment, and connect with your customers, partners, suppliers, and employees when and where you need to.

Locking down your data is essential to your business operations and to ensuring customer trust. But as many SMBs are now finding—if you don't secure your data, it's just a matter of time before you and your customers pay the price through financial loss, identity theft, reputation damage, and class-action lawsuits. With this in mind, you may be asking yourself whether cloud services can help you better meet business security needs.

THE CHALLENGES OF SECURING YOUR OWN SERVERS

On the surface, operating your own servers may seem like a good way to protect against breaches and secure your company's data. It's logical to think that if you control where the data resides, you won't risk contaminating or exposing data through shared resources, and you can manage your own security settings.

1 "2011 Data Breach Investigations Report," Verizon Business.

Before you go it alone, it may be prudent to take a realistic look at your security and disaster recovery capabilities. Your resources may not adequately update a proliferation of devices and applications or replicate your servers for quick recovery after a cyber attack or natural disaster. Likewise, your ability to remain compliant with industry standards may be too labor-intensive, especially if you can't employ a dedicated security specialist. And revenue losses as a result of reputation damage, along with the cost of trying to restore your business integrity, can be daunting. Here are just a few of the challenges you may be facing:

Keeping up to date with everything: If you have one or two generalists on your IT staff, they may be too busy to juggle all of your security needs with daily administrative tasks and strategic business goals. They may find it impossible to keep up with the evolving landscape of emerging threats, to regularly apply patches to update software, and to monitor all endpoints for intrusion.

Lacking network redundancy and availability: The viability of your company depends on access to mission-critical data. To get back on your feet quickly following a natural disaster or cyber attack requires dispersed data centers, duplicate systems, and real-time backups, but limited resources make these solutions unrealistic for many SMBs.

Inconsistent compliance: Staying compliant with industry security standards and regulations is a strain on companies of all sizes. Yet consistent compliance can contribute to a stronger security profile. The DBIR bears this out with a startling revelation—89 percent of the hacked businesses surveyed were not compliant with the Payment Card Industry Data Security Standard (PCI DSS) at the time of the attack.

Resolving these security issues is a challenge for SMBs, given their size and resource limitations. In many cases, utilizing cloud services can actually improve the overall security of your data while significantly lowering investment in your IT infrastructure. Most cloud providers regularly update their anti-virus programs and apply security patches to software. In fact, many cloud providers invest significantly more in security policing and countermeasures than almost any company—large or small—can afford for itself.

LONG-TERM STABILITY AND PROFESSIONAL SUPPORT

The more you rely on the cloud, the more you need to rely on a committed provider who is financially stable and has long-term viability. Look for these capabilities:

- Security expertise in various security initiatives, such as PCI-DSS, Health Insurance Portability and Accountability Act (HIPAA), and Gramm-Leach-Bliley Act (GLBA)
- Professionals experienced with implementing information security standards such as SAS70 and FISMA (Federal Information Security Act of 2002)
- Audited facilities that meet regulatory standards
- Programs designed to help you build a roadmap to security and compliance
- Security support for do-it-yourself IT groups or companies seeking end-to-end support
- Knowledge of emerging threats gained from sophisticated analytical tools

FOUR STEPS FOR EVALUATING SECURE AND RELIABLE CLOUD COMPUTING ENVIRONMENTS

If the cloud is looking like an attractive option for your business, you'll want to review your selection of cloud providers carefully. The truth is, not all cloud providers deliver the same level of security. You'll need to gauge the stability of each provider and its ability to supply protection and services that meet your standards for security and reliability now and in the future.

Your provider should offer physical security at the data center and apply recognized standard protections at gateways. You'll need to check your provider's offering for availability guarantees and a layered defense that secures data as it rests or travels in the cloud. The following four steps can help guide your decisions:

1. Utilize a data center that protects against break-ins	2. Protect your data from remote attack	3. Maintain high levels of availability	4. Secure your data whether it's static or on the move
The first step in defending your data is defending the data center. According to the DBIR, the lack of physical security at the actual data center was a factor in almost one third of all breaches investigated. • Look for tight physical security, such as 24x7 human guards and biometric screening, to positively identify visitors, and video cameras for facility monitoring. These safeguards will help protect against hardware theft and software tampering, and unauthorized access data. • Find out where your data will be stored. Will your provider use its own secure facility or farm out processing and storage functions to a third party that may add risk?	Locking down all ports and remote connections is an essential step in protecting against external attacks. • Ask your provider to verify that all software patches, anti-virus signatures, anti-malware, and security policies are up to date and applied consistently. • Your provider should require access credentials and strong authentication for secure log-ins. • Ask about cloud-specific firewalls for virtual machines and intrusion.	If your provider's infrastructure fails, you risk an interruption in service that could impact sales and reputation. • Find out about your provider's backup practices. • Learn if your provider replicates data and application infrastructure across multiple sites. • Ask your provider if a complete restoration is possible and how long it will take. • Look for a provider who can contract for the level of availability you require. • Ask about uninterruptible power supplies, climate control, and fire prevention and suppression at the data center.	Data in the cloud is typically in a shared environment, which means that data from multiple companies may reside on the same server. Your cloud provider needs to provide strong isolation and compartmentalization at every layer of the multi-tenant architecture to protect against unauthorized access. • Your expectations should include tested encryption methods for file transfers, support for customer pre-encrypted file storage, and strong authentication. • Find out if the provider complies with standards designed to control access by the people who manage your data. • If you foresee specialized requirements not met by shared resources, seek a provider who can offer additional protections through dedicated systems and private IP networking options, such as application log monitoring, virtual private networks, and migration strategies and services.

LAYERED DEFENSE IN VERIZON CaaS

Physical security: We protect our data centers from physical intrusion with 24x7 security guard protection, surveillance cameras, and biometric scanners.

Encryption: We preserve the integrity and confidentiality of your data with file transfers that use SSL and AES 256-bit encryption.

Multi-tiered network: CaaS stops attackers with virtual firewalls and load balancers that keep data highly available while controlling the exposure of your applications to the Internet.

Patching: We thwart cyber attacks before they bring down the network through regular software patching and consistent updates of virus signatures.

Intrusion detection: CaaS audit trails enable you to identify who has accessed your computing environment and what operations they have performed.

Strong authentication: Our multi-tenant file system requires at least three types of credentials and governs what any given user can access.

Standards-based security: We operate in a PCI-compliant environment that's been certified by our own Security Management Program and SAS70 Type II-audited.

Professional services: We offer optional security services you can use to tailor your cloud security, such as identity and access management, host intrusion detection, application vulnerability assessment, network application assessment, and migration service.

VERIZON MAKES THE CLOUD A SAFER PLACE

As experts in cloud computing, we make it our business to build a cloud computing platform that protects businesses of all sizes. We build security into every layer of our Computing as a Service (CaaS) infrastructure so that you can confidently exploit the cost and capacity advantages of cloud computing.

Our security controls, policies and procedures have been validated against a stringent set of Cybertrust best practices. You'll be able to demonstrate to your customers and partners that you use cloud computing services that meet the stringent standards of one of the largest wholly-owned, facilities-based networks in the world.

SUMMARY—PROVEN SECURITY EXPERTISE MAKES ALL THE DIFFERENCE

A cloud provider with proven security expertise can make the cloud a safer place to conduct your business and secure your data. The right cloud provider makes security its business, so that you can concentrate on using the cloud's speed, efficiency, and cost savings to gain an edge in today's business climate.

Verizon stays abreast of the latest security threats and devotes powerful tools and the expertise of its global team to maintaining the safety of your information in the cloud. You can grow your business with Verizon and know that when your security and availability standards change, we'll be there with the advanced options you require. Give your business a boost with pay-as-you-go cloud services from a world leader in security and communications.

Next Steps

For more information about how Verizon can help you transition to cloud computing, contact an account representative or visit us online at verizonbusiness.com/medium/.

Verizon is a global leader in driving better business outcomes for mid-sized and large enterprises and government agencies. Verizon combines integrated communications and IT solutions, professional services expertise with high IQ global IP and mobility networks to enable businesses to securely access information, share content and communicate. Verizon is rapidly transforming to a cloud-based 'everything-as-a-service' delivery model that will put the power of enterprise-grade solutions within the reach of every business. **verizonbusiness.com**

Verizon Communications Inc. (NYSE, NASDAQ:VZ), headquartered in New York, is a global leader in delivering broadband and other wireless and wireline communications services to mass market, business, government and wholesale customers. Verizon Wireless operates America's most reliable wireless network, serving more than 93 million customers nationwide. Verizon also provides converged communications, information and entertainment services over America's most advanced fiber-optic network, and delivers innovative, seamless business solutions to customers around the world. A Dow 30 company, Verizon employs a diverse workforce of more than 195,000 and last year generated consolidated revenues of $106.6 billion. **verizon.com**