

Quest[®] STRATEGIC ADVISOR

www.questsys.com

Quest | CLOUD SECURITY BRIEF

Staying Secure in the Cloud: It's a Partnership

As you reap the benefits of Cloud computing's flexible infrastructure capacity and speedy provisioning, don't forget about the steps your IT crew needs to take to keep your use of Cloud computing secure.

Cloud environments face all the security issues of any complex networked system — plus the added challenge of protecting huge amounts of diverse customer data that live in Cloud datacenters.

"Fortunately, a well-designed Cloud infrastructure that properly isolates customer data addresses many of the security issues that often fall through the cracks in traditional IT environments," says Quest CEO Tim Burke.

Cloud security: Why it has to be a partnership
Even so, Cloud security is impossible without a partnership between the Cloud provider and the customer.

"Consider, for example, the role of web browsers, which both providers and customers rely on as a Cloud interface," Tim says. "Browser security failures can quickly lead to Cloud security breaches. And while providers can watch over their admins' browsers, customers have to do their part, too, and continually make sure customer browsers stay secure."

Three customer Cloud security must-dos

So what should a Cloud customer do when it comes to Cloud security? Tim points to three must-dos:

Minimize your device vulnerabilities. Whether it's PC-resident web browsers or road-warriors' smartphones, use your firm's security policy to reduce exposure to malicious websites, and apply best practices for securing and hardening employee devices. This is especially important if you allow BYOD (bring your own device).

Encrypt. "Strong encryption should always be used for any network communications involving confidential Cloud app interaction or data transfer," Tim says. "And stored confidential data should be encrypted, too."

Benchmark your application performance. This starts with benchmarking your apps and establishing key performance requirements before deploying those apps to the Cloud — so you can make sure your performance requirements (e.g., response time, bulk data transfer rates) are met in the Cloud environment you choose. Should your apps suffer performance degradation in

CLOUD SECURITY (Cont. on p. 2)



THE BOTTOM LINE

Cloud security is a partnership between you and your Cloud services provider. Here's what you need to know to keep that partnership strong and effective.

IN THIS ISSUE

Keeping Cloud security strong — with partnership

2 From Tim Burke:
Pay attention to the chain of control

3 Profile:
Quest's many and varied security offerings

3 Did You Know?
Glancing at the future of IT security

4 What's New...
Mobility on the march

CLOUD SECURITY (Cont. from p. 1)

the Cloud — perhaps from a malware attack — you'll know it.

"The good news is that Cloud service providers with depth and breadth of capability can help you get these must-dos done," notes Tim, "with services like mobile device management, encryption, and app performance monitoring."

"Cloud security is not an add-on. It has to be a built-in. And when it is, it can exceed the security of traditional in-house IT environments."

Assessing Cloud provider security

In addition to securing your devices, encrypting your data, and benchmarking your apps, Tim recommends you scrutinize your Cloud provider in five key ways:

Taking security seriously. Does your Cloud provider have appropriate security certifications and a willingness to be externally audited? Check your Cloud provider's operating policies for their incident response and recovery procedures/practices, vetting of privileged users (e.g., the provider's system/network administrators), and internal investigation processes regarding illegal/inappropriate use of IT resources.

Cloud infrastructure visibility. Look for a provider who has mechanisms — such as virtual firewalls, virtual intrusion detection/prevention systems, and network segmentation techniques like VLANs — that protect their Cloud's virtual machines (VMs) from attacks by other VMs residing on the same physical host, by the physical host itself, or by the network.

Identity/access management visibility. Know about your provider's authentication/access control mech-

FROM TIM BURKE...

Pay Attention to the Chain of Control

These days, you can buy Cloud services from just about anyone.

Some of these providers do it all themselves, from initial needs assessment through design, integration, customization, and implementation all the way to post-deployment support. Even if they provide capabilities via reselling products and services from others, they have deep technical knowledge of what they've provided and can stand by it.

So as a customer, your chain of control is unbroken — when you want help or information about your service, you'll get what you need.

Others do Cloud in bits and pieces. These Cloud brokers often buy and resell in the time-honored ways of white-labeling. Which is fine — as long as you, the customer, still have an unbroken chain of control.

Sadly, however, this is not always the case. Too often, those who actually deliver the brokered services you've bought are several times removed from you. Your Cloud broker, meanwhile, may understand much less than you'd like about what they've sold you.

Worse, you may not even know whose services you've ended up with. This can create situations in which you get shuffled along from provider to provider, never quite getting the help or the answers you need.

So when you're moving to the Cloud, ask those chain-of-control questions. A capable, trustworthy Cloud services provider will always be eager to answer them.



CHECK OUT MORE OF TIM'S THINKING AT www.questsys.com/CEOBlog/

anisms as well as the tools available to you for provisioning authentication data and inputting/maintaining authorizations for both users and apps.

Authentication. Look for Cloud services providers who use advanced authentication techniques to lower the risk of account hijacking, impersonation, etc.

Operations affecting your data. Insist on visibility into any of your Cloud provider's operating services that impact your data. You want to make sure the Cloud apps you use run securely

and can be integrated with existing security mechanisms and enforced by security policy. You want to be able to determine the physical location of your stored data, to administer access control over your data, to verify how your data was securely erased, and to track how hardware storing your data was securely deleted.

"Cloud security is not an add-on," Tim points out. "It has to be a built-in. And when it is, it can exceed the security of traditional in-house IT environments."

Quest's Security Solutions:

Getting What You Need to Keep Your IT Secure

Quest understands that to be effective, your security measures need to work together in awareness of each other. That's why we offer a full range of security capabilities that can be customized, integrated, and fine-tuned to precisely fit the needs of your organization.

Whether you want to boost the security of your Cloud services, need a comprehensive information security plan, or simply wish to plug a few holes, we'll deliver what you require from our remote Network Operations Centers (with full 24/7 management) or right at your site.

Quest's free security-related assessments

Our no-cost scans, assessments, and reviews can show you where you're vulnerable and how we can help. These free offers include:

- ▶ *Malware Assessment* — find out how well you'd weather a malware attack,
- ▶ *Application Security Scan* — one application scanned to help identify any security gaps or vulnerabilities,
- ▶ *Firewall Review* — a remote scan via secure communication followed by recommendations, and
- ▶ *Security Review/Security for the Half-Day* — a vulnerability scan followed by discussion and Quest recommendations.

Quest's security-related Managed Services

Our Managed Security Services include:

- > Security Posture Assessment
- > Managed Unified Threat Management Services
- > Enterprise Firewall Design/Management
- > Intrusion Detection/Prevention
- > Vulnerability Scanning
- > Application scanning
- > Managed Antivirus Services
- > Email Virus Protection/Spam Detection
- > Managed Web Filtering
- > Data Loss Prevention Solutions and Services
- > Wireless Security
- > Mobile device management
- > Quest's Security Response Team (SRT)
- > Computer Security Incident Response Planning and Management
- > Computer Forensic Data Collection and Analysis
- > Managed Network Services

- > Client VPN Design
- > Managed Site-to-Site VPN Service.

Quest's security-related Professional Services

Our teams of expert security professionals can help you develop or adapt your corporate security policy to changing times and technologies as well as prepare you for audits, forensics, compliance analysis, and MasterCard/VISA certification processes.

We can also help implement and manage security-related projects, including infrastructure security, intrusion detection/protection systems, correlation analysis, and log monitoring.

DID-YOU-KNOW?

Glancing at the Future of IT Security

Analyst firm Gartner's Symposium/ITxpo in October produced some insights about the state of IT security, current and future*:

- ▶ *Over the next five years, investments in security will grow a dramatic 56%, with investments in Cloud security almost tripling*, chiefly because the pervasiveness of IT across business operations will spawn a new wave of government interventions and regulation.
- ▶ *Through 2013, 80% of Cloud security incidents will be caused either by Cloud service provider administrative error or by problems in user management of Cloud services.*
- ▶ *In high-security environments — about 20% of the market — security will be kept separate from private or public Cloud infrastructure* via mechanisms that require all security-relevant flows to be externalized so that existing and separate security processes can examine them and enforce security policies.
- ▶ *In low-security environments — another 20% of the market — relying on the security built into infrastructure will be sufficient.*
- ▶ *For the 60% in the middle, there will be compromise:* As long as sufficient separation of duties and audit/visibility can be provided, security workloads will run in private Cloud and public Cloud environments.

* As reported by *Network World*: <http://www.networkworld.com/news/2012/103012-gartner-critical-trends-263793.html?page=2>

Coming in the next issue of *Quest Strategic Advisor*:
Case Study of: MOCSE CREDIT UNION

What's New...

Mobility on the march

Analysts at IT trend-watcher Gartner used the firm's recent symposium to offer predictions about the future of mobility and bring-your-own-device (BYOD)*:

- > *In 2016, 40% of the workforce will be mobile and two-thirds of these workers will own a smartphone.* Also in 2016, half of all non-PC devices will be purchased by employees; by decade's end, half of all devices in business will be purchased by employees.
- > *The emergence of Apple iPads has made BYOD a near-term priority* — even though iPads are tough for most users to justify as an essential computing tool. While IT organizations do not want to increase the cost per user for computing resources, most enterprises want employees to use whatever tools may help them perform their jobs better or are likely to aid in retention of high-value employees.
- > *Over the next five years, 65% of organizations will adopt mobile device management* to address security concerns triggered by use of smartphones and tablets.
- > *By 2016, 60% of large enterprises will implement limited access network zones* to restrict the connectivity of personally owned mobile devices.

* As reported by *Network World*: <http://www.networkworld.com/news/2012/103012-gartner-critical-trends-263793.html?page=2>




Quest STRATEGIC ADVISOR

Publisher: Tim Burke
Editor: Barbara Klide

Contact the editor at
barbara_klide@questsys.com

All contents copyright © 2012 by Quest® Media & Supplies, Inc., unless otherwise noted. *Quest Strategic Advisor* is published bimonthly by Quest Media & Supplies, Inc. Information contained in this newsletter is believed to be reliable but cannot be guaranteed to be complete or correct. Quest Media & Supplies, Inc. assumes no liability for any use of this newsletter and/or the information or opinions it contains. *Quest Strategic Advisor* and questsys.com are trademarks of Quest Media & Supplies, Inc. Other product, service, and company names mentioned herein may be servicemarks, trademarks, or registered trademarks of their respective holders. To the best of Quest's knowledge, cited data and research findings belong to the organizations to which they are attributed and Quest Media & Supplies, Inc. asserts no claim to them. Quest® is a Registered Trademark of Quest Media & Supplies, Inc.

FRIEND, FOLLOW, FIND QUEST

 facebook.com/QuestTechUSA
 twitter.com/QuestTechUSA
 youtube.com/QuestTechUSA

IN THE MEDIA ROOM

VISIT QUEST CEO TIM BURKE'S BLOG

[\(www.questsys.com/CEOBlog/\)](http://www.questsys.com/CEOBlog/)

THE QUEST YOUTUBE CHANNEL

www.youtube.com/QuestTechUSA

Master Your Disaster, parts 1-4
DR for the Day ... and much more

QUEST WEBSITE VIDEOS

www.questsys.com/media.aspx

Who We Are: Colleagues describe how Quest helped them.

Service Delivery Centers: They're why you can count on Quest.

Business Resumption Center Online Tour: Secure, seismically-stable 24x7x365 availability — Quest's BRC is the ultimate in disaster preparedness.

Business Continuity Planning/Disaster Recovery: More than 25% of businesses damaged from natural and/or man-made disasters never recover. Ensure your future.

DR for the Day®: Find out if you're ready — at NO CHARGE.

Data Security: The FBI, security experts, and your peers on today's security issues and how Quest can help protect you.

Overview of our Infrastructure Services

QUEST EXECUTIVE BRIEFS

Getting the Most from Cloud Computing (3-part series):

Learn what it is and how it can help your business thrive (<http://www.questsys.com/getMostCloud/>).

10 Strategic Essentials for Boosting Business' IT Security:

Key strategic security steps every organization should take (<http://www.questsys.com/BoostITSecurity/>).

Protecting Your Critical Business Data: The Data Loss Prevention Payoff: How data loss prevention (DLP) technology can protect corporate data from misuse, malicious or otherwise (<http://www.questsys.com/PowerofDLP/>).

NEWSLETTERS

Get current and back issues of our popular newsletter.

Manage your Newsletter subscription:

Let us know how you want your newsletter sent at <http://www.questsys.com/SANpreference.aspx>

Choose an emailed PDF or hard copy via USPS.

