Quest® TECHNOLOGY MANAGEMENT

STRATEGIC ADVISOR

VOLUME XIV, NUMBER 3

Why Multi-cloud Security Matters — and How to Achieve It

How many cloud services does your business use?

"Probably more than last year," says Quest CEO Tim Burke. "And for good reasons. With multiple clouds you can choose services that specifically suit your organization's needs and structure workloads into separate environments that are better aligned with your business goals and policies."

The payoffs include benefitting from best-of-breed capabilities and minimizing public cloud vendor lock-in while boosting agility, availability, and performance.

According to research and advisory firm Gartner,* "Organizations without a cloud-first strategy — where the cloud is primary, prioritized, and promoted — will likely fall behind competitors."

The importance of multi-cloud security

All those always-on devices by which employees access your data anywhere, anytime also capture streams of employee information that are automatically consolidated and made available across environments that include not only public clouds but also company production systems.

"While this interconnectivity eases employees' daily routines and hikes their productivity," Tim explains, "the resulting streams of data can be exploited by people with malicious intent — bad actors who capture those streams to analyze them and model business and user behaviors so they can drive cyberattacks that bridge networks and infect corporate production environments."

Traditional security tools can't help you now

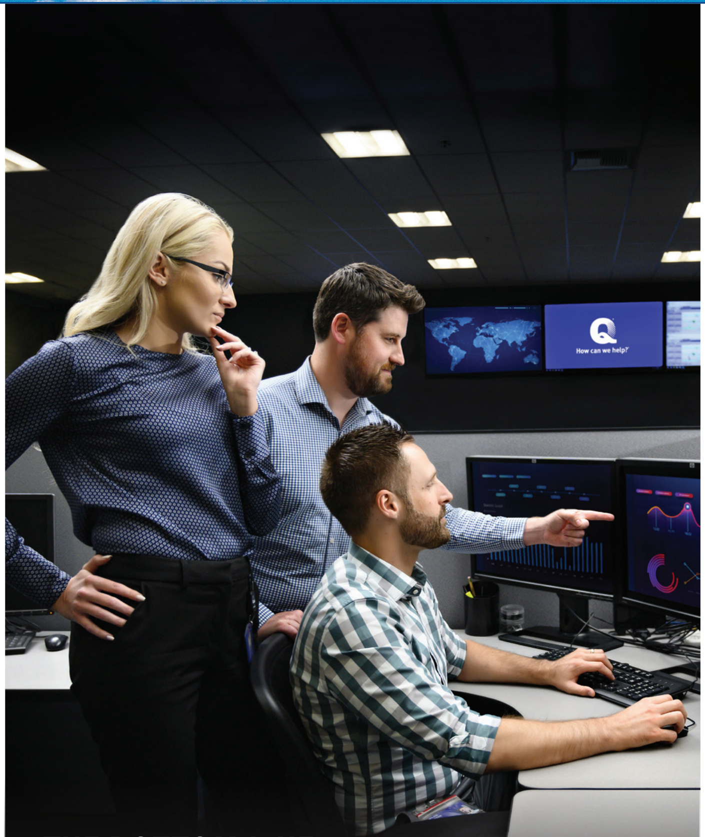
Although cloud providers have appropriate protocols and tools to ensure that their offerings are safe, the responsibility for securing your data, notably during access, remains with you.

So as you harness the benefits of multi-cloud IT, Tim advises that you pay particular attention to several multi-cloud security issues.

"First, understand that traditional security tools aren't designed to protect the enterprise data your employees use," he says.

* https://www.gartner.com/smarterwithgartner/modernize-it-infrastructure-in-a-hybrid-world/

continued on page 2



THE BOTTOM LINE

Ready or not, all those always-on devices that do so much for employee productivity have also ushered in your multi-cloud future — which comes with multi-cloud security challenges you can't afford to ignore. The good news: Quest is ready to help you.

IN THIS ISSUE

Quest's Tim Burke explains why multi-cloud security matters

FROM TIM BURKE...

Focusing on Three Cybersecurity Basics

When you recognize that your business is vulnerable to cybersecurity threats, you may be tempted to acquire fairly complex solutions. But do you genuinely grasp whether or not what you're buying will accomplish what your business really needs?

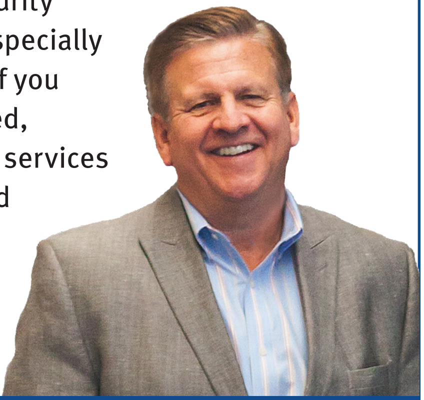
If you hesitate to answer 'yes,' I suggest you gather your IT team and focus on three cybersecurity basics:

First, back up and recover your data. Of course, you ought to confirm that your people are backing up the company's data. But then ask about data recovery — as in, *How often do we test recovery?* It's no accident that this question — *When was the last time you tested your data recovery capabilities?* — is the first thing the FBI asks when you're dealing with a security event, like a ransomware attack.

Second, patch your systems. You need to ensure that your organization has an effective patching process in place. Patching might be boring, but unpatched systems create egregious risks. Just ask anybody who suffered at the hands of WannaCry.

Third, monitor your IT environment. Somebody needs to be watching 24/7 so that if, say, an alert comes in at 2 a.m., your people will know and be able to respond quickly and appropriately.

These three cybersecurity capabilities are not especially costly — particularly if you engage an experienced, trusted cybersecurity services provider to deliver and manage them — and they'll go a long way toward reducing your firm's risk exposure.



CHECK OUT MORE OF TIM'S THOUGHTS AT https://www.questsys.com/CEOBlog/

Why multi-cloud security matters *(continued from page 1)*

"Your data streams in and out of cloud apps via infrastructure that your enterprise neither owns nor controls. You must monitor and maintain full visibility and control over those data streams in every cloud your business uses, whether they're hosted, reside on-premises, or are in a public cloud."

And that's not all.

"To protect against cyberthreats like malware in this anywhere/anytime/any device environment," Tim adds, "you need tools that can stop known and unknown threats in real time on any device accessing your data in all of your clouds."

And although many cloud apps offer some degree of visibility and control, Tim notes that you need to be able to consistently apply security policies and make changes across *all* of the cloud services your business uses, regardless of vendor.

> "Traditional security tools aren't designed to protect data your employees use"

"Without security tools explicitly designed for a multi-cloud environment, your IT team gets stuck *manually* adding and/or editing policies in every single application," he says.

This daunting task is made even worse whenever one app's native security control features don't match the feature granularity of other apps. Result: implementing the changes you want becomes enormously cumbersome, if not impossible.

A comprehensive multi-cloud security capability

"We believe," says Tim, "the best approach involves focusing on operational simplicity and implementing end-to-end automation in concert with pervasive cybersecurity."

Perhaps most importantly, this means deploying Security Information and Event Management (SIEM) and Security Operations Center (SOC) capabilities to provide real-time monitoring and analysis of security alerts.

You'll also need to ensure that all operating systems are always up to date; that you can back up and recover your data; that you monitor and manage network traffic with unified threat management devices and deep packet inspection; and that you deploy web application firewalls.

"Comprehensive multi-cloud security involves an array of capabilities that combine software and hardware," Tim advises. "Unless your IT team has significant bandwidth and expertise, you're likely better off engaging a multi-cloud security services provider with a broad range of cybersecurity offerings supported by a Global Security Operations Center."

Quest's Global Security Operations Center:

Cloud-based security services to protect your business

Based in Quest's Network Operations Centers (NOCs), the expert engineers who staff our Global Security Operations Centers (SOCs) support a comprehensive set of integrated security services that take advantage of our extensive experience and proficiency as well as Quest's partnerships with security industry leaders.

Quest's SOC-based cybersecurity services include:

CyberDefense Suite

Using today's most sophisticated tools to monitor your environment 24 X 7 X 365 in real time, CyberDefense Suite capabilities, which you can choose in whole or in part, incorporate...

Endpoint device protection monitoring/updating that monitors your IT security environment 24 X 7 X 365.

Spam and anti-malware protection monitoring/alerting/updating that monitors your anti-spam and anti-malware platform.

Firewall/IDS/IPS monitoring/alerting that enables you to quickly identify and respond to potential threats filtered by your firewalls.

Quarterly vulnerability scan that helps you systematically document regulatory and policy compliance.

SIEM as a Service

Our state-of-the-art Security Information and Event Management technology monitors your IT activity patterns to spot threats and deliver the actionable intelligence necessary to prioritize response.

Patch Management as a Service

Quest provides patch automation and compliance across apps and platforms.

Data Loss Prevention as a Service

Discover, monitor, control, and secure your sensitive data.

Penetration Testing

Our security experts use a wide variety of tools and methods to conduct internal and external penetration tests that can identify your organization's security vulnerabilities.

Quest's Incident Response Team

Just a phone call away, Quest's Incident Response Team moves fast and effectively to address cybersecurity incidents of all kinds.

Security Training and Compliance

This online cybersecurity training solution teaches your employees to recognize and handle front-line cybersecurity attacks and meet compliance requirements.

Security Workshop

Find out about the state of your organization's cybersecurity with a Quest assessment of your current security posture and vulnerabilities.

Protect your business with comprehensive, layered digital security provided by an experienced, SOC-based expert team of specialists who use leading-edge, cloud-based tools and resources.

DID YOU KNOW?

Warning: Microsoft Legacy OSs at Risk from BlueKeep

In May, Quest sent the following notice to our customers, which we reprint here in the belief that this dangerous potential threat continues (see page 4 for more information):

Quest's Global Security Operations Center (SOC) is working closely with industry leaders, tracking Microsoft's recent advisement that certain legacy Windows operating systems contain a vulnerability that can compromise devices. The vulnerability could be used as a cyber-weapon similar to the WannaCry worm that was a global threat in 2017.

Microsoft has identified Windows Server 2003, Windows Server 2008, Windows XP, and Windows 7 as high-risk operating systems. This vulnerability is significant enough that Microsoft has put a patch out for Windows XP, which went end-of-life as of April 2014.

It is recommended that companies review patch management processes and continue to practice safe computing habits before opening/downloading documents and attachments from untrusted data sources.

In the event that you need assistance in reviewing and remediating this vendor-identified vulnerability, or to discuss any other security concerns, please reach out to our 24/7 SOC support services at 800-443-5605 or submit a ticket to performance@questsys.com.

What’s New...

Ransomware Watch: How Protected Is Your Business?

Microsoft’s May announcement that a now-patched computer bug (indexed as CVE-2019-0708) could be used as a “wormable” WannaCry-like cyber weapon signals the continuing — and unrelenting — presence of ransomware threats.

As with WannaCry, Microsoft has issued patches to fix the vulnerability — called BlueKeep —in the Remote Desktop Services component of several legacy versions of its Windows operating system, including Windows 7, Windows Server 2008 R2, Windows Server 2008, Windows Server 2003, and Windows XP. More recent versions of Windows are not at risk.

“Highly likely” to be exploited

Nevertheless, Microsoft believes this self-replicating, code-execution vulnerability — which can allow an unauthenticated, remote attacker to execute arbitrary code on a targeted system — is “highly likely” to be exploited, since all an attacker has to do is send specific packets over the network to a vulnerable system in which the Remote Desktop Protocol (RDP) service is available.

The good news: because a malicious request must be sent to the targeted system, networks that restrict access from untrusted sources can make exploitation more difficult. And network firewalls and other defenses that block the RDP service would effectively stop a BlueKeep attack from occurring.

However, as the WannaCry attacks in 2017 so vividly illustrate, even when patches are readily available, too many systems remain unpatched and thus vulnerable. In the case of BlueKeep, researchers have estimated that some three million RDP endpoints are directly exposed, while 16 million are exposed to the internet through TCP ports typically reserved for RDP.

You *can* protect your business from ransomware

These days, wormable ransomware attacks come via a widening range of vectors — from phishing emails to Microsoft’s RDP, even Microsoft Office — and too many businesses are unprepared to deal with them.

Ransomware horror stories abound, but you *can* protect your business by preventing attacks and by developing and enforcing policies that enable you to limit the effects of a successful attack and recover from it quickly with minimal disruption and cost. Contact Quest to learn how.

I NEED TO SET SOME GOALS FOR YOU.
MY JOB IS TO MAINTAIN THE LEGACY SYSTEM.
@ScottAdamsSays
Dilbert.com
MY ONLY GOAL IS TO AVOID ACCIDENTALLY UPGRADING IT.
© 2017 Scott Adams, Inc./Dist. by Andrews McMeel
2-25-17
AND HOW'S THAT GOING?
I DON'T LIKE TO BRAG, BUT I WAS BORN FOR THIS JOB.

DILBERT: © Scott Adams. Used by permission of ANDREWS MCMEEL SYNDICATION. All rights reserved.

FIND, FRIEND, FOLLOW QUEST

https://www.facebook.com/QuestTechGlobal
https://twitter.com/QuestTechGlobal
youtube.com/QuesTechUSA
https://www.linkedin.com/company/quest-media-&-supplies-inc-/

QUEST ASSESSMENT SERVICES

Test drive our services, evaluate our expertise.

For a complete listing, go to: https://www.questsys.com/assessments/

Disaster Recovery Workshop
https://www.questsys.com/assessments/disaster-recovery/

Security Workshop
https://www.questsys.com/assessments/security-workshop/

Risk Management Workshop
https://www.questsys.com/assessments/risk-management-workshop/

Network Health and Infrastructure Check
https://www.questsys.com/assessments/network-health-infrastructure-check/

Backup and Data Recovery Review
https://www.questsys.com/assessments/backup-and-data-recovery-review/

IN THE MEDIA ROOM

VISIT QUEST CEO TIM BURKE’S BLOG
(https://www.questsys.com/CEOBlog/)

NEWSLETTERS
Get current and back issues of our popular newsletter at https://www.questsys.com/resources/.

Manage your newsletter subscrition at https://www.questsys.com/subscription-preferences/.

Quest STRATEGIC ADVISOR
Publisher: Tim Burke
Editor: Barbara Klide
Contact the editor at: barbara_klide@questsys.com