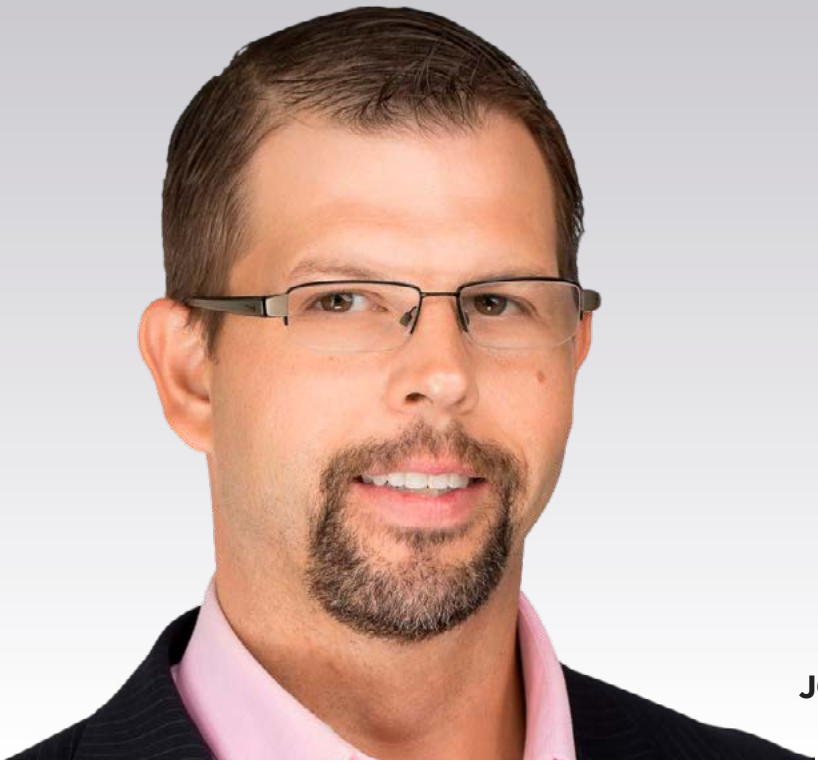
Qualys

SECURITY IN THE CLOUD REQUIRES A NEW MINDSET

CISO of Qualys Shares Strategies to Improve Cloud Security

ISMG
INFORMATION SECURITY
MEDIA GROUP



JONATHAN TRULL

Trull serves as an adviser to several security startups and venture capital firms and supports the broader security community through his work with IANS. He is also an adjunct faculty member at Carnegie Mellon University, where he mentors and coaches those attending the CISO Executive Education Program. Trull is a frequent speaker at industry conferences such as Black Hat, RSA and SANS.

During the accelerated digital transformation of the past two years, enterprises have fully embraced multi-cloud environments. But security practitioners are learning that security in the cloud requires a new mindset and a unique set of skills, says Jonathan Trull, CISO of Qualys.

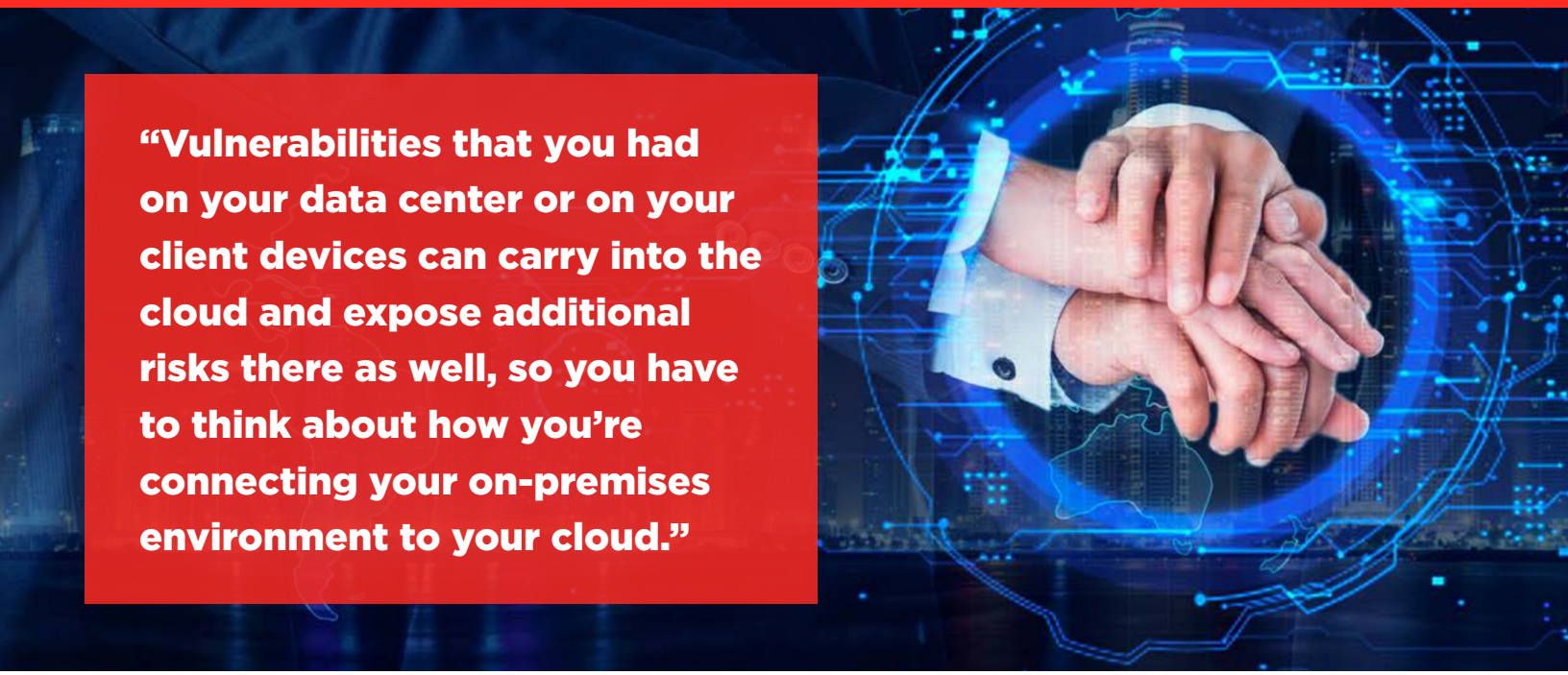
In a video interview with Information Security Media Group at RSA Conference 2022, Trull discusses:

- How organizations are approaching risk as they migrate to the cloud;
- The biggest barriers – technical and nontechnical – to improving cloud security;
- How to measure progress – and gain access to the right talent.

CLOUD MIGRATION AND RISK

ANNA DELANEY: When it comes to cloud migration, how are organizations approaching risk?

JONATHAN TRULL: They have to think about several levels of risk. At a strategic level, you have to decide on the right provider based on evaluation of their controls. You're entering into a partnership with the



“Vulnerabilities that you had on your data center or on your client devices can carry into the cloud and expose additional risks there as well, so you have to think about how you’re connecting your on-premises environment to your cloud.”

company so you have to be confident that the controls that you’re relying on are in place and have been audited. Then you have to start thinking about a new way to architect and work from a security perspective. One of the biggest shifts is that identity becomes a much bigger issue. But at the same time, vulnerabilities that you had on your data center or on your client devices can carry into the cloud and expose additional risks there as well, so you have to think about how you’re connecting your on-premises environment to your cloud.

CLOUD VULNERABILITIES

DELANEY: How should security leaders approach vulnerabilities in the cloud?

TRULL: We’re taking a new approach to vulnerabilities. We’ve been in the vulnerability business for a long time and it’s why we’ve released our new product VMDR 2.0, but the idea is to focus on the true risk that’s associated with those vulnerabilities that you need to patch. The traditional way is: All vulnerabilities are treated equally. And it’s very difficult to triage and approach all of them. You need to focus on vulnerabilities that are known to be exploited in the wild. We have good threat intelligence that the bad actors are trying to attack those cloud workloads. We know they have them in their payloads, because we can see the malware and we can see the different attack frameworks that they’re using. That’s where we need to prioritize our time. That’s where we need to focus. We are trying to shift how people think about dealing with vulnerabilities, whether it’s on-premises or in the cloud.

A NEW MINDSET

DELANEY: What’s the mindset shift that has to happen?

TRULL: It’s about: What is the true risk based on the context of the workload and the asset. Is it processing critical data or not? Honestly,

naturally, most security professionals are going through this thought process. They're thinking: "Is it exposed directly to the internet? How many control points are between the internet and an attacker and that vulnerability? How fast do I need to move?" The problem is: You can do that with one, two or maybe up to 100 or 1,000 assets. But some large enterprises are trying to protect 1 million cloud assets and workloads, so they have to build in a lot of automation.

I recommend zero-touch patching for certain workloads where you have a high level of confidence that you can patch and protect those vulnerabilities. We always used to wait and do testing; it was slow. It would take 30 days, sometimes three months, to get to a vulnerability. Unfortunately, as we all know, the attackers don't care about breaking things, so they move fast. They exploit vulnerabilities within 24 hours, eight hours after they are released, so we have to move faster.

MANY THREATS TO CLOUD SECURITY

DELANEY: What are the cloud security threats of most concern to you?

TRULL: When we see cloud workloads being attacked, usually it's through identity – poor passwords or APIs that are exposed to the internet that aren't protected with multifactor authentication. That's one mechanism. We also see a lot of misconfigurations because there's a huge shortage of cloud security professionals. The ones working are not malicious, but they do configurations very quickly because there's demand and pressure to get work done. Unfortunately, things aren't protected with firewalls. Storage containers are open for the internet to access. Oftentimes, it's not a very sophisticated attack. It's people crawling cloud services and finding very weak passwords and exposed vulnerabilities. The last piece is traditional exploitation, which is: You're running a server in the cloud. It has a vulnerability. It's attacked with some type of payload and, if you're not patching quickly, the attacker gets a foothold and begins to move laterally throughout that cloud environment.

STEPS TO GOOD CLOUD SECURITY

DELANEY: What should cloud security look like, and how does it differ from on-premises security?

TRULL: Good cloud security starts at the fundamental, early stages. You need to set guardrails, which can be set in policy through technology that is part of the cloud frameworks.

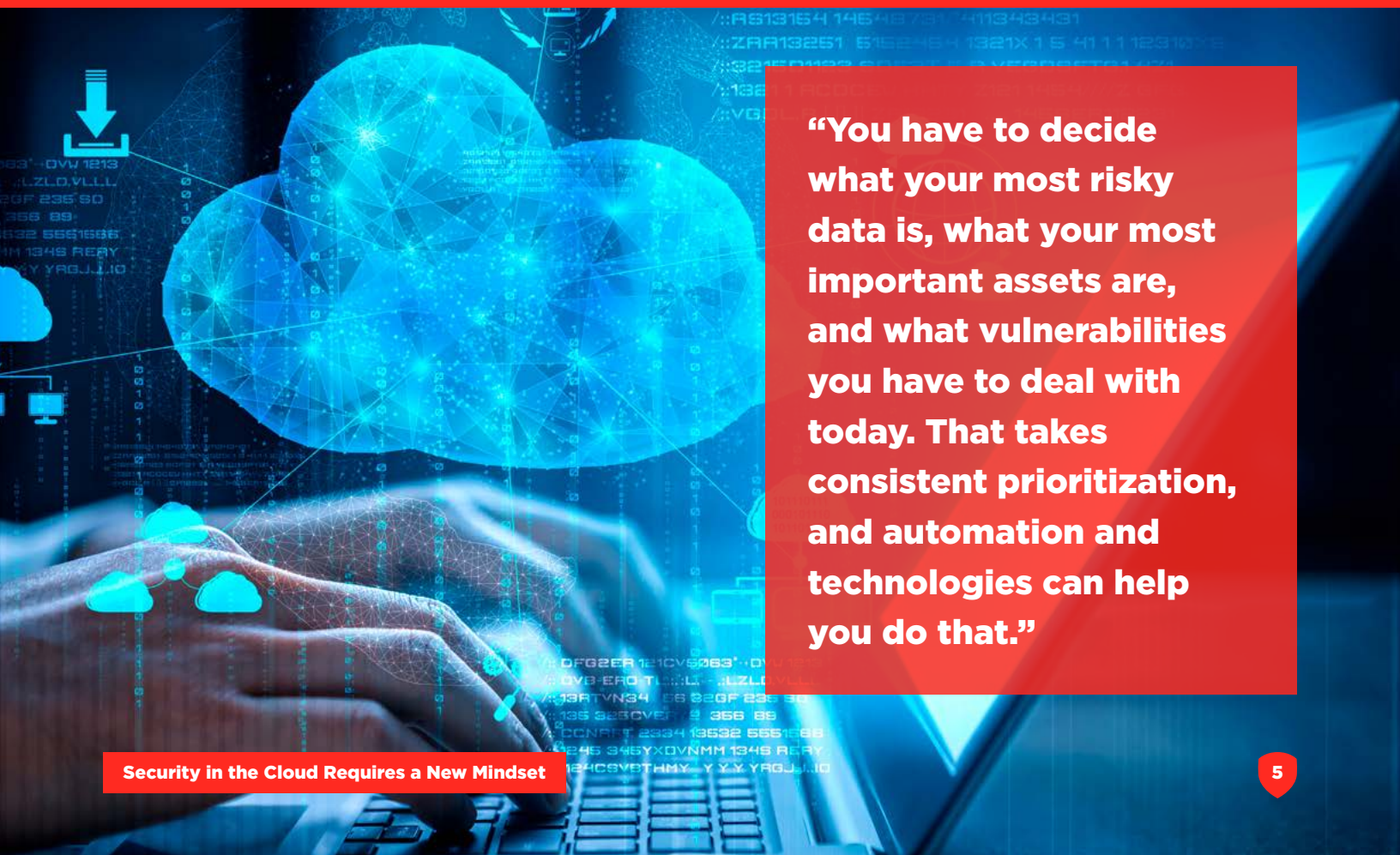
Guardrails help you say: "I only want certain types of workloads that I've trusted and certain versions of operating systems." Certain storage containers can't be exposed, because they're blocked at a policy level. You also need to use Terraform or functions as code to orchestrate the spinning up and spinning down of workloads. Then your security team can evaluate all of those, test those functions, and get a lot more granular security over the specific work that's being done.

Finally, there's data protection and encryption. Key management is a very big focus for cloud security. Depending on how you view risk, you need to determine whether you want to store your keys and if you're comfortable with the cloud provider storing the keys. Finally, you need to bring the technology that you use to protect your on-premises into the cloud and push your vendors to provide solutions that support and work in any of the major clouds out there. Most of the time, you don't want to adopt and use new technology; you want to use something your team is trained on and comfortable with.

FILLING THE TALENT GAPS

DELANEY: You mentioned the talent shortage earlier. What other barriers exist to improving cloud security maturity?

TRULL: We talk a lot about working with higher education institutions and universities. Traditional computer science programs are really good at teaching coding and some of the basics, such as C++ languages and how to write different data structures. But they



"You have to decide what your most risky data is, what your most important assets are, and what vulnerabilities you have to deal with today. That takes consistent prioritization, and automation and technologies can help you do that."

haven't always evolved and kept up with how you do some of the more practical tasks around cloud and cloud security. Similar to cybersecurity programs, often the focus is very heavily on on-premises.

We have a very small pool of candidates that we're all competing for. We have to work with universities and help improve their programs. At Qualys, we give our technology away to universities for free so that they can use it to train their students. That's because we want to hire them, so we want them to be trained and know how to do the job.

Finally, we need to look at being a little bit more forgiving of people. In the industry, we tend to always want the best – someone with 15 years of experience who is an expert. We need to take more junior people. We need to mentor them and grow them into this space over time. It's not a short-term solution. It's a big industry solution that we're all trying to work to make better.

TECHNICAL BARRIERS TO CLOUD SECURITY

DELANEY: What about the technical barriers?

TRULL: There are a lot of new services that cloud providers spin up all the time. Hundreds and hundreds of services exist. Trying to keep up to speed is very difficult. On the technology side, you have to focus on true risk perspective. You can't boil the ocean. You can't focus on all of the technologies and issues. You have to decide what your most risky data is, what your most important assets are, and what vulnerabilities you have to deal with today. That takes consistent prioritization, and automation and technologies can help you do that.

MEASURING CLOUD SECURITY MATURITY

DELANEY: How do we measure progress in cloud maturity?

TRULL: There are some great frameworks out there. The Cloud Security Alliance has a cloud security maturity model. It's got five levels and based on the level, you can assess how you're doing. It starts with foundational controls – things that, no matter what control you look at, it should be done. It then moves to structural, which is around how you do network security, protect data and handle vulnerabilities. It's more at the workload level. Then, there's a procedural domain, which is about process. Oftentimes, we overlook the importance of repeatable processes for doing certain tasks. For each of those, you're assessed from a level zero to a level five. It's a good tool to follow.

There are some other good, very specific benchmarks. The Center for Internet Security has some for cloud providers that are tactical and very control-oriented. AWS has a well-architected framework that is a road map for architecting real secure workloads. And at Qualys, we provide benchmarks and architectures that will give you a high level of risk reduction.

Qualys®

The leading provider of information security and compliance cloud solutions.

CLICK HERE TO LEARN MORE: www.qualys.com

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 28 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

(800) 944-0401 • sales@ismg.io

BANK INFO SECURITY® CU INFO SECURITY® (Just for Credit Unions) GOV INFO SECURITY® HEALTHCARE INFO SECURITY®

infoRisk TODAY® CAREERS INFO SECURITY® Data Breach TODAY (Prevention. Response. Notification.) CyberEd.io

ISMG
INFORMATION SECURITY
MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io