Put Those Cloud Security Objections to Rest

Zscaler's Bil Harmer Makes the Case for Moving to the Cloud

FORMATION SECURI
EDIA GROU

zscaler™


Bil Harmer

Harmer is Americas CISO for Zscaler. He has been in the IT industry for 30 years. He has been at the forefront of the internet since 1995 and his work in security began in 1998. He has led security for startups, governments and well-established financial institutions. In 2007 he pioneered the use of the SAS70 coupled with ISO to create a trusted security audit methodology used by the SaaS industry until the introduction of the SOC2. He has presented on security and privacy in Canada, Europe and the U.S. at conferences such as RSA, ISSA, GrrCon and the Cloud Security Alliance. He formerly served as chief security officer for GoodData and vice president of security and global privacy officer for the cloud division of SAP.

In the wake of digital transformation, there remain some organizations that – for security reasons – resist the temptation to move to the cloud. What are their objections? Zscaler's Bil Harmer addresses these, as well as the critical questions security leaders should ask of cloud service providers.

In an interview with Tom Field of Information Security Media Group, Harmer discusses:

- Why some security leaders still hold out against the cloud;
- Critical steps to initiate the transition;
- Essential questions to ask of cloud service providers.

Overcoming Hurdles

TOM FIELD: Bil, you and I have toured North America talking about digital transformation. In today's digitally transformed enterprise, it's very hard to argue against moving applications and services to the cloud. What do you see as the biggest remaining security barriers for holdout organizations?

BIL HARMER: I think the security professionals have done a great job in the past protecting assets on premises, and it's that mindset that they sort of get locked into. And we have to start pushing through that. As new threats emerged in history, we deployed things to protect them. The cloud changed the number one constant that every security professional had, and that's the network control. So they were always using network control as a means to put the policies and procedures in place that they needed.

The new landscape requires a security transformation that has to go in lockstep with the overall digital transformation for a company. Security leaders really need to take a step back and say: How do I adapt to the new environment and avoid the idea of making vendors work within my confines? Because that's just a recipe for disaster.

Winning Security Leaders' Support

FIELD: So Bil, users are demanding and in some cases even paying for their own cloud services. Why, then, are some security leaders still holding out?

HARMER: I would suspect it's because security has historically followed the business. They appear to be holdouts in a migration, because it's never been security's place to set the direction for the company. The cloud and shadow IT provided such easy access into applications and services. Today, shadow IT is simply a user trying to do their job who's got a credit card and an expense management system and access to SSL. That's how they're getting these solutions. So at best, security is more like a "fast follower."

The real holdout is in paying the price on the security coverage of the user experience. So if they continue to dig their heels in and try to use that legacy network as a means to the end, they will impact their users on user experience and coverage. Threat actors have been

> “How do I implement those security tools to achieve the goals of my business at the risk level they would take?”

hitting users outside the corporate environment for years because it was simple. It was easy. We all hear about “the Starbucks attack” – jack them at a public Wi-Fi.

Or a CEO that just gets so angry, or upset, or frustrated with the user experience, that he says, “Punch a hole in something. Let me get to this directly. Take that out because it’s impacting me.”

And I think that’s the holdout: How do I implement in this fast-moving environment without my one legacy control that I was really comfortable with?

Strategic Steps

FIELD: Bil, in your role, you interact with many organizations in lots of different sectors. What strategic steps do you recommend to security leaders that are navigating this cloud transformation journey?

HARMER: Understand your business. Security professionals grew up in the technical side of things. A lot of us came out of the military or the police; we came out of the networking groups, the sysadmins, the guys and girls who were in there at the core, tweaking things, building iptables and ipchain firewalls in the early days. And so we approach it from a technical perspective. We come in and say, “What is your problem? Here’s the technical solution.”

We now need to understand the bottom line. We need to understand the cost of goods. We need to understand EBITDA. These are things that we don’t typically address, and unless we do, we cannot protect our businesses. So as you move forward, you have to be at the forefront with your business leaders, saying, “OK, we are able to accept this level of risk based on what we’ve decided from our risk register and our discussions with our board. Our departments want to go this direction because it reduces their cost of goods manufacturing or in distribution. How do I as a security professional provide the risk level with the tools I have? Because security is just a tool; it is not a state or an ideology. It is simply a tool. How do I implement those security tools to achieve the goals of my business at the risk level they would take?”

Ask the Right Questions

FIELD: So with all the cloud service providers out there, what are the questions security leaders need to be asking when they go shopping?

HARMER: Anything beyond “Do you have a SOC 2?” Seriously, though, security leaders need to think in terms of privacy, and I’m not talking very specifically about PII and the human privacy aspect that is in the forefront of everybody’s mind. Think of the concept of privacy as protecting data, whether it’s financial information, intellectual property, marketing strategy or the people. What is it that you are doing that may put the privacy of some piece of information, i.e., the dissemination of that information at the appropriate time – at risk? And then start asking those questions about who your partners are going to be, because cloud services are simply an extension of your IT organization. You have to make sure that they are in line and that you understand what they do.

So going back to my comment about SOC 2, a lot of customers will come and say, "Show me your SOC 2. Great, you have it. Wonderful. Well, is that my SOC 2 or is that my data center SOC 2? Do I have any sub-processors? What's their process? Where is my data going? Who is going to see it?"

Those are the questions they really need to ask, so that way they can understand: Is that vendor in line with the direction that they are going based on the risk levels?

> **"We enable security leaders to ensure that the policies follow the user, regardless of the network they're on."**

Zscaler's Role

FIELD: Bil, talk to me about Zscaler. What are you doing to help organizations make this journey successfully?

HARMER: Zscaler's architecture and implementation was specifically built to drive this change. We saw this migration to cloud services, i.e., managed services on somebody else's system, out there and that security was tied to the network. So we enable security leaders to ensure that the policies follow the user, regardless of the network they're on.

It simplifies the life of the CISO. It ensures the users have a much more productive user experience. And I can't stress that enough: Security today is the balance between user experience and risk mitigation. That is what we are trying to do. There is no perfect security and there is no point to perfect security because perfect security costs too much and doesn't result in a user experience that's usable. They will find a way around it. This has been that way for 20, 30 years. If it's too hard to use, they find a way around it.

So you need to find a balanced approach to ensure that the design that you're putting in place achieves the business goals and is productive to the user experience, and that's how Zscaler has approached it. ■

Listen to the full interview at https://www.bankinfosecurity.com/interviews/put-those-cloud-security-objections-to-rest-i-4374

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.

Contact

(800) 944-0401 • sales@ismg.io

About Zscaler

Zscaler enables the world's leading organizations to securely transform their networks and applications for a mobile and cloud-first world. Its flagship services, Zscaler Internet Access™ and Zscaler Private Access™, create fast, secure connections between users and applications, regardless of device, location, or network. Zscaler services are 100 percent cloud-delivered and offer the simplicity, enhanced security, and improved user experience that traditional appliances are unable to match. Used in more than 185 countries, Zscaler operates a multi-tenant distributed cloud security platform, protecting thousands of customers from cyberattacks and data loss. Learn more at zscaler.com

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

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

ISMG
INFORMATION SECURITY
MEDIA GROUP

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