TAKING ENTERPRISE SECURITY TO THE NEXT LEVEL

An interview with John Summers, Enterprise VP and GM, Akamai

Q&A

What are the top things that business leaders need to understand about today's cybersecurity threats?

John: Recognize that the days of the generic threat are over. Threats are highly targeted at your organization by people on a mission to seek something, often intellectual property or personal or financial information. Or the mission is simply to get in and eavesdrop on the activities of your organization.

The people who do this are highly skilled and well resourced. Some of the best at breaching cyber defenses are the nation-state actors. They're persistent and patient, and they do their very best to fly completely under the radar by making their interactions with your infrastructure and business and people look as innocuous and business-as-usual as possible. That's a whole new class of threat. It's evolved over the last several years and is really making security much more challenging.

Meanwhile, business leaders have the imperative to drive their organizations to greater agility and add new value to customers and business partners, supply chains, and distribution chains. Businesses have to digitize so they can operate and change faster and faster. Out of necessity, they connect more, communicate more, and make more use of cloud infrastructure.

So, at the same time that the threat actors are getting much more devious in the ways they penetrate technology infrastructure, enterprises are having to make their infrastructures more permeable, to open up connections that can make the business be competitive. That's the central tension of cyber security today. How to open up the business to move faster but remain cognizant of and defend against the ways it's threatened?

What should business leaders know about today's common approaches to security?

John: Historically, everyone in the security industry has come out of the network security layer. That's the world of moats and high walls where there was an inside and an outside. But that world is disappearing. A highly interconnected business has bits of infrastructure and its users in other places — not behind walls but out with customers, out with business partners, and then connecting back to business-critical applications from sometimes far-flung locations.

This pervasive connectivity makes the legacy network security mindset largely irrelevant. When you're coming in to access an application from over the Internet, it's not traversing a network that you control, and so network layer controls are much less effective at spotting and deflecting cyberthreats.

What, then, is the necessary alternative?

John: The security perspective needs to evolve away from the network and up to the user, data, and application layers. Those are the new control points, the places to control business interactions in the world of cloud infrastructure. You need to know who the users are. You need to know what applications they should have access to and only give them that access. And you need to make sure the data traversing between users and applications is the right data and secure in transit. I call this the security evolution from "packet, port, and protocol" to "user, data, and application."

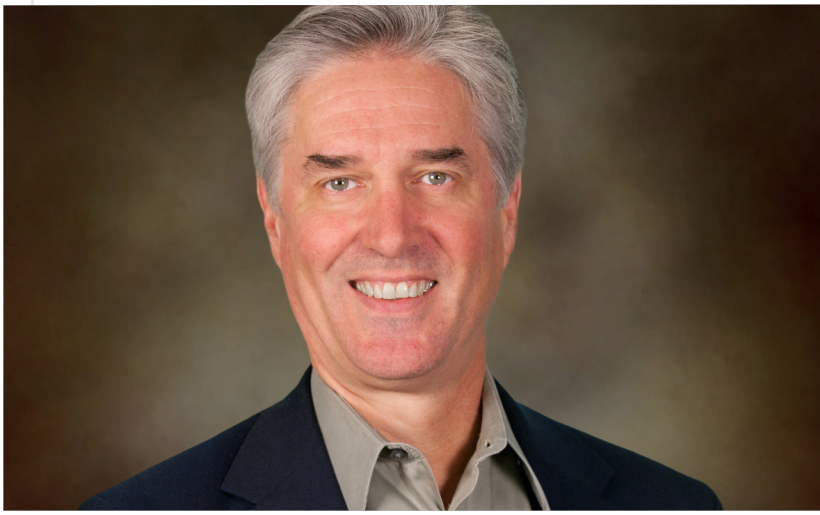
The challenge is that we need a lot more security professionals trained on new approaches and controls. And vendors must shift their thinking about enterprise security in the highly distributed and connected world. Akamai has real advantages here because we grew up delivering content securely over the Internet, and we built our platform directly on the fabric of the web. We've had to operate at the asset

level — user, data, application, the device that's communicating with us — for 19 years. That entails strong authentication, strong encryption, and complete visibility regardless of what networks are in use.

The Internet is composed of something on the order of 15,000 different networks. When you operate in the middle of that, asset-layer security is your only choice. We're eager to share with customers what we've learned over those 19 years about how to take security to the next necessary level.

Please say more about what must happen behind the scenes to protect those assets.

John: You need visibility into the assets and their behaviors in order to determine how much they can be trusted and how much business risk there may be in trusting them.



***John Summers**, Enterprise VP and GM, Akamai Technologies*

We've always had user identities in a traditional corporate security model, but now those identities have to be used for accessing applications, including major SaaS applications, that live in the cloud rather than in our data centers.

As an extension of the user, we need to know things about the device being used. Is it managed by the company, or is it a largely unmanaged device of the user's choosing? Security policies and practices have to account for BYOD in order to make things easy for the user.

With any application in the cloud, we need to know that the user is accessing the right application, as well as whether the application is fully trusted, or only semi-trusted, or not known at all. This is extremely important, for example, when users fall prey to spear phishing attacks by clicking on email links that appear to come from familiar sources or be part of normal business. To detect possible attacks, we need to know both what's being communicated and the trustworthiness of the destination.

And then there's data. Trying to secure it starts with understanding its importance. Is the data being transmitted between the user and the application critical to the business, or not so critical, or we don't care if it's stolen? The classification of data is truly nascent in most enterprises. People talk about it as necessary, yet few organizations do it well. One financial services executive confided that there are basically just two classes of data: "Stuff I can get in trouble for and everything else."

In securing all these assets, we have to recognize that security decisions and actions are much less cut and dried than they used to be. It's not about approving or blocking access to IP addresses. It's not that black and white. We need to be much more nuanced in our security decisions, we need much more granular visibility into what's going on, and we need to be much more business-risk-based in the application of security policy.

What are the business benefits of a more risk-based cybersecurity model?

John: The objective is lowering the risk to the business, risk to the brand, while at the same time not getting in the way of innovation and acceleration and change. Ideally, security practices enable business agility — enable the business to roll out new applications continuously in a way where each new release doesn't expose the business to additional risk.

That represents a profound shift. Security has historically been thought of as a barrier one has to get through in order to accomplish a business objective. Security people often thought of themselves as gatekeepers — you can do this, you can't do that.

Instead, security should be about providing counsel to the business on how it can accomplish its objectives in ways that carry the lowest risk and highest opportunity. Security has to be seen as a source of risk assessment and guidance on how to lower risk to a level that makes it sensible for the business to pursue the opportunity. CSOs need to give their business colleagues optionality around varying the amount of risk the business can take on. No security organization can take risk to zero.

What's an example of security practices enabling business agility?

John: We worked with the digital team of a large financial services firm. They are all about new applications, rapid innovation, rapid experimentation, and new business value. They wanted to be able to deploy new applications quickly yet with confidence in their security. Together we developed an application deployment framework with a security layer built in, so all the applications are architected to be scalable and secure from the ground up.

Security tools they were using, for checks and monitoring, authentication, and access control, were all included in the framework. So the developers could just do their job of building new apps. Security wasn't an extra step to be added on — it was built in. The security methods went from barrier to enabler.

Here's an extension of that approach. Applications increasingly incorporate APIs and machine-to-machine communications. Most organizations don't pay a lot of attention to the security of those machine-to-machine, API-to-API, bits-of-software-to-other-bits-of-software communication. They link together a whole set of APIs and then add a security wrapper only where the application talks to the web or the user.

Yet if you can build in secure communications at the API layer, it's a huge advantage for any application using those APIs. Security is built into the software for what's valid for the API to send and receive. Applications can be deployed faster while being more thoroughly secure.

The fundamental principle here is that security has to be designed in as you think about the business infrastructure, and has to be integrated into the infrastructure, not overlaid at a later date. When you create new data, that's when you should think about its importance to the business, rather than trying to add a security classification later on. When you deploy applications, security should already be embedded. That's the next threshold of security practice that organizations have to cross.

How should organizations get started on the path to more asset-based and risk-driven security?

John: You want to integrate security more directly into the fabric of the business. Start the exploration around business processes not infrastructure. Look at the data that's being exchanged between various steps in a process, and assess the potential risk to the business of losing some of that data at each of those steps. Then put in place the right security controls around who can participate in the process, what authentication is required at each end of the communications, and what should be the limitations and controls on those communications. If you can think about security at the business process layer, that makes things much clearer as you move down into the infrastructure layer.

You also want to bring the domains of security and application development more closely together. It's often said that security is everybody's job, but you're not going to be able to train all your developers on how to be security people. However, as just discussed, you can create an application framework that makes it easier for people to develop new applications with security built in. In the process, you'll see what additional competencies are needed in the security group around application layer security and user and data access control mechanisms.

What's your closing advice to CIOs and CSOs about how to accelerate their progress taking cyber security to the next level?

John: First, the adoption of cloud shouldn't be feared — it should be embraced. It can actually help you to become more secure at the same time it's helping your business to become more agile, more profitable, and able to grow faster.

Second, follow the principle of zero trust. You should assume that everything is potentially compromised and put in place business and security policies based on that assumption. It's only in the easy cases that you know when something's definitely good or definitely bad. Most of the security world is that gray zone in the middle. So you need to assess how risky you think things might be and gather evidence over time to update your security posture.

Third, embrace the responsibility of guiding the business regarding risk, not just

making gatekeeper decisions. It's a bigger and a more value-adding role. Security professionals are really risk professionals, who need to think specifically about how business risk is driven by security risk, not just about the security risk. That way, the business can be nuanced about security strategy and policy just as it is about business strategy and tactics.

As the world's largest and most trusted cloud delivery platform, Akamai makes it easier for its customers to provide the best and most secure digital experiences on any device, anytime, anywhere. Akamai's massively distributed platform is unparalleled in scale with over 200,000 servers across 130 countries, giving customers superior performance and threat protection. Akamai's portfolio of web and mobile performance, cloud security, enterprise access, and video delivery solutions are supported by exceptional customer service and 24/7 monitoring. To learn why the top financial institutions, e-commerce leaders, media & entertainment providers, and government organizations trust Akamai please visit www.akamai.com, blogs.akamai.com, or @Akamai on Twitter.

Akamai is headquartered in Cambridge, Massachusetts in the United States with operations in more than 57 offices around the world. Our services and renowned customer care are designed to enable businesses to provide an unparalleled Internet experience for their customers worldwide. Addresses, phone numbers and contact information for all locations are listed on www.akamai.com/locations.
