SECURING YOUR DIGITAL BUSINESS

An interview with Josh Shaul, VP, Web Security Products

Q&A

What's the most important thing that CIOs and other senior business executives need to know about information security today?

Josh: We're in a new age in information security. The traditional "moats and castles" model that businesses have relied on for decades — surrounding the "castle" of enterprise data, applications, and networks with the "moat" of a secure perimeter and firewalls — is becoming outdated and increasingly irrelevant. Applications, data, and users have moved outside the firewall and into the cloud, and they are traversing the public Internet. They've "jumped the moat" and traditional security systems are largely left guarding an empty castle.

What's driving all this movement to the cloud?

Josh: Today, every business is a digital business, and the Internet is a critical part of the information infrastructure. It's the primary connector between cloud-based workloads and on-premise data and applications. It's the connector for millions or even billions of connected devices that compose the Internet of Things.

Enterprises have to be in the cloud for a variety of reasons:

- One, to deliver fast and engaging digital experiences to customers. Their expectations for speed, reliability, and customization of web and mobile experiences continue to escalate. That's why we say "slow is the new down." In this digital economy, there's always an alternative, and impatient customers will quickly go elsewhere.

- Two, to enable employee productivity. Today's employees need to work from home, from the road, and from customers' locations, and they may need access to their systems and applications from around the world and while in transit.

- Three, to coordinate with business partners. It's a global digital community of suppliers, partners, and contractors — all of whom need secure, fast, and reliable access to portions of an enterprise's applications and data.

- And four, to drive digital business transformation. To digitize and accelerate business processes, enhance products and services with technology, launch new digital applications for customers, open new markets, and globalize their brands, enterprises have to leverage resources in the cloud.

What are the implications for business risk?

Josh: Digital businesses now expect and rely on the Internet to provide mission-critical levels of speed, reliability, and security — things it was never designed to do under even the best of conditions. Meanwhile, the consequences of cyber attacks on revenue, business operations, and brand reputation can be extremely high.

The backbone of a digital business — websites and cloud-based applications — is under constant threat of attack from malicious actors. The APIs that serve as the connective tissue for applications and digital experiences create porousness in security perimeters and open up hundreds or even thousands of new endpoints that attackers can exploit. VPNs, user access controls, credential vaults, authentication systems — all these traditional security mechanisms actually provide potential points of attack and exploitation.

And it's not just the distribution of infrastructure and data into the cloud that creates new risks. It's the very process of creating these applications and digital experiences themselves, because of the ever-expanding network of people who need to access software, networks, and systems to develop and manage the applications that power

the digital strategy of a business.

Yet as enterprises embrace the cloud, they still have the same requirements for security, protection of sensitive data, and compliance as they always have. Those don't change. But the attack surface and risk profile are now exponentially larger, and those requirements must be met in new ways. The digital-age CIO is challenged with finding a way to ensure security and compliance on the increasingly distributed and cloud-based network the business is relying on more every day. Businesses have to be in the cloud, and they have to be secure in the cloud.

Please say more about how the threat landscape is changing.

Josh: Today's attackers are no longer just cyber criminals operating with the most advanced resources and tools. Everyday users have the power to stage complex, highly distributed attacks. By taking advantage of freely available and highly sophisticated toolsets and "attack-for-hire" services, novice as well as experienced cyber criminals have the capability to bring down and exploit global websites with DDoS attacks for a fraction of the traditional cost, effort, and complexity.

These attacks are not merely becoming easier to mount, but also far more sophisticated and dangerous. In the past, the greatest risk may have been having sensitive product files stolen, or network passwords compromised. But now digital businesses must confront hundreds of new exploits that just a few years ago might have seemed like science fiction — malware that "steals" files and holds them hostage for ransom, scraper-bots that can capture credit-card data in the microseconds that it's unencrypted and vulnerable in memory, coordinated attacks using armies of connected IoT devices (thermostats, light bulbs, Wi-Fi routers) that can shut down a site. And in every case, traditional security approaches simply can't cope effectively in this cloud-based world.

What new approaches are needed?

Josh: Enterprises need new approaches not only to providing security, but to designing their security needs in the first place.

On the provisioning side, we need security built for the way cloud works, built to take advantage of the shape of the Internet — not try to defy it. Protection must

be distributed wherever the business assets are. Traditional centralized approaches to security simply can't do that, and it's impractical if not impossible to try to move entire security architectures into the cloud.

At Akamai, we start with two assumptions. One, the enterprise is no longer the perimeter; rather, the entire cloud is the new perimeter. Or perhaps better said, the perimeter has evaporated entirely. And two, we're working with what Forrester calls the "zero trust network" — all network traffic is potentially suspicious. Under those conditions, security must be pervasive and it must map to users, data, and applications wherever they are.

Security, policy, and controls must move away from the enterprise "castle" to the "edge" of the cloud. That makes security more complete and more portable. For example, if security is not tied to a specific infrastructure configuration, then when an Internet service provider goes down, the business can move simply and seamlessly between providers, confident that users, applications, and data remain secure in any new environment.

And on the security design side?

Josh: Organizations typically try to establish levels of protection based on the value and sensitivity of assets. For example, customer data gets extra safeguards. But the approach tends to be rudimentary and not very granular — it's extra protection, yes-or-no. And that's only half the story. The other half is how assets may be exposed by applications and transmission. What specific hazards is the business exposed to and how can they be mitigated? Play out the attack and asset loss scenarios. The combination of asset value and potential exposure should determine protection tactics.

At a more macro level, an organization can follow the procedures and best practices prescribed by internal standards, industry standards, and regulatory compliance — and still not be adequately protected against cyber attacks. That's because, as we discussed, the threat and security landscape is in constant motion. The objective is to be agile enough to deal quickly with new threats. That calls for a flexible security technology platform, not just a collection of current point solutions. So design your approach to security for future flexibility as well as immediate protection.

How does more distributed security work?

Josh: In the cloud, bigger is definitely better. The performance and security requirements of a cloud delivery platform simply cannot be achieved with anything less than massive scale and distribution. So Akamai deploys more than 200,000 servers in 130 countries across the Internet, carrying as much as 30% of global web traffic at any given moment.

Massive scale and distribution create massive visibility — huge amounts of real-time information about users, endpoint performance, network performance, and Internet performance as a whole. That information is the backbone of cloud-perimeter-based security capabilities. It includes an unparalleled real-time view of Internet security exploits, including all the attacks against all the enterprises we support.

That real-time security intelligence means that as threats evolve, the ability to stop them evolves right alongside, thwarting web application and DDoS attacks right at the Internet edge. In the majority of cases, Akamai can block an attack within one network hop of the attackers themselves, ensuring that malicious traffic stays as far away from enterprise data centers as possible.

You can't route traffic faster than the Internet can unless you're everywhere, measuring and comparing every possible path. You can't see security threats as they emerge unless you're on the networks where they originate, anywhere in the world. And you can't reliably defend against DDoS attacks unless you have more capacity than you're being attacked with. So again, bigger is better.

What are some specific ways that enterprises can leverage cloud-based security to reconfigure and improve their protection?

Josh: The basic challenge is around access. Providing access to applications and data, whether they live in the cloud or in a traditional data center, requires opening up access methods that represent a huge potential attack surface for malicious actors.

So how can an enterprise provide fast, simple, and secure remote access that "keeps the bad guys out" without getting in the way or slowing your business down? Take two examples.

In a traditional, firewall-based security model, you would typically provide outside users with VPN access into the corporate network, sometimes even going so far as to ship them a corporate-owned laptop preconfigured for access. Unfortunately, that VPN access is a huge potential attack vector, and many notable security breaches came about in exactly that way. The better alternative is to connect applications behind the firewall only to a small web app exposed to the public Internet. Since the connector at the firewall can communicate only to the desired application, and nothing else on your network, you can't open up your entire network to a VPN user.

Another common scenario is supporting branch office access to enterprise applications. The traditional configuration would be to connect the branch-office network to a private WAN and then to your corporate data center, so that traffic is inside the "enterprise perimeter" and protected via the traditional firewall. But what happens when an employee in a branch office accesses the public Internet through a direct connection? Suddenly, all bets are off. That connection can easily be exploited by malware, phishing attempts, and other threats, all outside the protection of corporate security.

The Akamai approach here is to monitor domain name service requests across the Internet in real time and intelligently score domains for threat risk. Users are automatically and immediately blocked from accidentally or intentionally accessing malicious domains and services. This validation happens in milliseconds, even before an IP connection is made, thus stopping threats very early in the "security kill chain" and far away from the enterprise perimeter.

What are your summary points for CIOs and other business and technology executives?

Josh: If your business isn't already digital, it's going to be — and if you're not already in the cloud, you will be. You'll need to provide the best and most secure digital experiences for your customers, employees, and business partners, no matter where they may be or what devices they may be using.

Because today's digital business lives and works in the cloud, its information security has to live and work there as well. The keys to cloud-based performance and security are massive scale, distribution, and visibility. You need to notice what's happening wherever it's happening and respond to threats in real time.

Digital assets have already "jumped the moat" and jumped beyond the control of traditional security methods. Cloud-based security has become essential. It can dramatically improve the security posture of the enterprise and lower its business risk. It can enable the enterprise to conduct and expand digital business with both confidence and ambition.

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.
