GETTING MAXIMUM PROTECTION THROUGH ZERO TRUST

An interview with John Summers,
CTO, Web Security & Performance, Akamai Technologies

Q&A

How do you describe zero trust?

John: Zero trust is all about the disappearing distinction between inside and outside. Organizations used to have their data centers and networks within a zone of control. They would trust what was on the inside, and be cautious about things coming in from the outside. Security was focused on keeping the bad guys out and letting the good guys in with the help of really good access control on crossing the perimeter.

But look at what's happening to our businesses today. The perimeter is dissolving. Infrastructure, applications, data, and users are more and more dispersed. Often there's no perimeter between mobile users and business apps in the cloud, and interactions happen over networks that the business doesn't control. So we must adjust our thinking for this new paradigm and build in security in new ways.

For starters, we can't trust a communication based upon where it's coming from. So whether it's inside the network or outside, before that communication gets set up, it should go through the same level of authentication and authorization checks. Simply approaching everything as untrusted goes a long way towards dealing with the transition state organizations are in, where an application that's in your data center this month will be in the cloud next month. And the user who is in your zone of control today is working from someplace else tomorrow.

Trust nothing, verify everything, maintain consistent controls — that's the essence of zero trust.

Say more about what drives the business need for zero trust.

John: The purpose of cybersecurity is to enable an enterprise to operate and innovate effectively and with confidence by protecting its digital assets and those who use them. Today those assets are distributed and in motion as never before.

The infrastructure we rely on now includes the Internet and the cloud, and as infrastructure is more software-defined, its physical location becomes more fluid. Network infrastructure connects enterprises with customers, mobile employees, and third parties — and those interactions necessarily cross the traditional perimeter.

Applications represent the business processes where value is created. Even mission-critical ones are moving out of the data center into the cloud, their data with them. Transactions have to be secured, data must be protected, and business activity must be audited for purposes of regulatory compliance — just like when those assets were inside the data center.

And users are everywhere. The enterprise must connect with customers on their devices and on their terms wherever they may be. Mobile and remote employees spend less time in the traditional zone of control. And business partners, suppliers, distributors, and contractors are highly distributed.

Add it up. Infrastructure, applications, data, and users can be anywhere. That has dramatically increased the level of exposure — the size of the attack surface that businesses must protect. It has also dramatically increased the complexity of network and security management.

We can't rein those assets back in and still thrive in the age of digital business. So we must secure them not with one perimeter, but more individually wherever they are. That requires high visibility and zero trust.

What does the transition to zero trust entail?

John: It takes a different security architecture. Security policy and controls have to be applied where they work best, which is with the digital assets being protected. Think about the right way to secure a communication from one endpoint in the cloud to another. You'd really like to be able to find the fastest communication path between those two points and then implement the appropriate security controls right in the middle of that path. No communication gets set up unless both parties have been strongly authenticated, and no data moves unless it's been strongly encrypted. That's what we need to do.

It also takes a different security mindset. Most security professionals have grown up in the network management world, where routers and firewalls and network packets are tools of the trade. It's natural to continue to try to encode security primarily at the network layer with techniques like microsegmentation. But that's the hard way, the complex way. We need to break that habit and move up to the application layer. The goal is to secure the interactions with applications regardless of what networks they're running over, because they're running over networks that the enterprise doesn't control. The application level is where business-defined security policy and control are best built in and enforced. At that level, security controls are portable to wherever the assets are.

What does zero trust mean for the enterprise?

John: Zero trust creates unprecedented visibility into what's happening with digital assets and users, not just what's happening in the network. That enables more comprehensive security in a highly dispersed business environment. Standard security controls can be built into applications and their interfaces, which makes for faster development and deployment of new business capabilities. So zero trust ultimately enables the business to be more agile, to proceed with greater speed and confidence in all of its digital initiatives.

Zero trust also reduces complexity and simplifies network management. When networking professionals aren't having to force business process layer security controls and policies down into the network, they can focus more on network performance and reliability and the digital experience being delivered to users.

Security controls can be addressed in business terms: Who is this user, how confident can I be of them, what application are they trying to talk to, what's the business risk of letting them talk to that application, and what policies and controls need to be on that communication path? Decisions about those policies and controls are clearly the responsibility of application owners, which is where they belong. That again simplifies the lives of the CISO and network professionals.

For users, zero trust reduces friction and improves their experience. We can strengthen authentication through means other than passwords. And the level of authentication can vary with what the user is doing — seamless access for simple tasks, more authentication when accessing sensitive data. A company directory look-up — go right ahead. Corporate financial information — a different thing altogether.

Finally, the greater visibility we're talking about is good for more than asset protection. It's visibility into your business. It provides more granular understanding of business processes and transactions operating online. You can analyze this information, gain new insights into how your processes and your customers are actually behaving, and find opportunities for improvements far beyond the realm of security.

How and where should organizations get started?

John: Some of the best use cases arise when there's a need to reconfigure networks in a big way. For example, a major retail chain needed to launch new business capabilities across over 10,000 locations. The business objectives were to provide better analytics for reducing costs and growing revenue at individual locations and in the aggregate. Trying to bridge all the store networks using VPNs and enforce security controls with microsegmentation was too complicated and had the wrong scaling characteristics.

The far better alternative was a zero trust approach leveraging the cloud and application-layer controls. Instead of stitching together a whole bunch of networks, they implemented attribute-based access with multi-factor authentication based upon people's roles in the organization. All the access control infrastructure is virtualized. Data transfers take place essentially between pairs of connections in the cloud, and there's no exposure to the Internet for the company's back-end systems.

That accelerated implementation while minimizing changes to the network. With that experience and success under their belt, the company is applying zero trust architecture to a range of business initiatives.

Another good use case is merger or acquisition, where synergies and financial success depend on the ability to merge technology and applications and business operations quickly. Some organizations have to do this repeatedly, as when a large financial services institution acquires a series of regional or local banks. The traditional approach — stitching networks together, dropping firewalls in front of firewalls, and trying to identify all the new assets to the old networks and their security controls — is complex, time-consuming, and error-prone.

In contrast, a zero trust architecture can overlay accessibility and controls. Keep the acquisition's systems running. Give their employees appropriate access to the parent company's applications and data, and vice versa. First, set up bridges between the perimeters and across the applications so the companies can coordinate operations quickly. Then, over time, merge the actual topology of the underlying networks to the extent needed.

Similarly, after a complete or partial divestiture, access to assets can be securely separated or selectively shared. Complex examples happen in the media and entertainment industry when specific assets are sold off. Say it's a content production operation spread over several facilities. Half the people there are going to start working for the new company, and the other half are going to stay with the old one. Among the apps they need to access, some will go to the new company, some will stay, and some may stay in the middle and need to be shared. Under that scenario, how are they going to rewire things? It would be very expensive and never work well.

The solution is to leave the physical infrastructure in place and overlay on it a virtual segmentation of user populations, with exclusive or shared access to applications, and full security controls. That can preserve people's productivity and deliver time to value for the business really quickly.

Those three examples carry an important underlying message — zero trust can be adopted gradually with sets of applications. It doesn't mean wholesale revamping of architecture and infrastructure. It can supplement and over time replace existing security mechanisms, delivering value as it goes. And do be sure to start with a use case that not only proves the concept, but also delivers significant value to the business.

What makes you so excited about zero trust?

John: At Akamai we're enthusiastic because we know it works, and we have unmatched experience doing it. Imagine for a moment that you have to deploy a business platform consisting thousands of servers around the world, all embedded directly into the fabric of the Internet. And they all had to securely communicate and interoperate with each other. And let's say you started to do that 20 years ago. That is, in fact, the Akamai story.

As the company was building out its highly distributed and Internet-based content delivery network — and guaranteeing high performance to our customers — we had to assume that no transmission was to be trusted.

So we have strong authentication for every endpoint. It's not just that we know the IP address — there's an exchange and validation of digital certificates before any communication gets set up. And no user gets to access the platform without going through an access control proxy. So there's a logically central point of policy enforcement based upon attributes — who you are, where you're coming from, what role you have in the organization, even what time of day it is, because when it gets to the off hours, maybe you shouldn't be coming in.

Today the Akamai platform has over 240,000 servers in over 130 countries. We operate at the edge of the Internet, where the notion of perimeter is obsolete. We handle a large portion of the Internet's traffic, giving us extraordinary visibility into security on the Internet and the security of our customers' infrastructure. That nonstop visibility continues to drive our perspective and our innovations in cybersecurity.

Nobody called it "zero trust" 20 years ago, but that's the approach we've been taking since day one. We didn't really have a choice if we wanted to do it right. So that's why we're passionate about zero trust and about helping our customers take security to the next level and make it an enabler of digital business.