Rethinking Cybersecurity

Zero Trust is reshaping network protection.

Beyond the Wall

A new security paradigm shakes perimeter security.

CISOs have fought the good fight. They've deployed a vast arsenal of defenses to keep invaders out of the castle and to shore up their networks against external threats. Yet it hasn't been enough. Data breaches compromise more than 6 million records every day. The global average cost of a single data breach is up 6.4 percent to $3.86 million.

Government and private sector institutions are vulnerable. The 2015 hack of the United States Office of Personnel Management, for example, involved 21.5 million records. Last year, a data breach of a major hotel chain exposed the personal information of a reported 500 million people.

Amid mounting attacks, Zero Trust seeks to reduce adversaries' opportunities for lateral movement. Perimeter defense is an all-or-nothing proposition. A CISO can build a moat around the IT castle, but an enemy who devises a way to lower the drawbridge gets access to everything. Similarly, the cyberattacker who breaches a perimeter network defense can in many cases attain almost unfettered access to the network and its treasures, including data troves and computing resources.

Cyberattackers bypass defenses by employing a predictable cycle that chips away at the perimeter wall through a series of stages detailed in various attack frameworks, among them phishing attacks, spear phishing, cline phishing, whaling, pharming attacks that use social engineering techniques, vishing or voice phishing and others. Often, it begins with the end user. No amount of training will prevent employees from clicking a bad link or opening an attachment, of course. Expecting otherwise is another systemic flaw in the current defensive architecture.

In a Zero Trust model, there is no particular distinction between outside and an inside at the network layer. Rather, the security lens shifts from the perimeter to the application layer. In the conventional IT architecture, a trusted user can often gain broad access to network resources after crossing the threshold. With Zero Trust, even users who has been rigorously authenticated will have access to a limited set of tools and services.

Unlike in the binary world of conventional security – out there and in here – a Zero Trust model proposes security should have granular identification, intense authentication, and rigorous internal controls.

It's not just the escalating cyber threat that should give IT pause and reason to consider a Zero Trust security model. As computing moves from corporate data centers to the cloud, and users are connecting remotely and via third-party tools, from public wi-fi networks around the world, the perimeter approach for defense creates inefficient traffic flows and faces limits in effectiveness.

The way users access networks has created a strong impetus for reimaging IT architecture and the apparatus of that access. With perimeter defenses no longer sufficient, Zero Trust security grants access only to valid users, at the application layer, enabling them to quickly, seamlessly and simply use only those applications to which they have authorized access instead of the entire network. It's a powerful new concept and a significant leap in the evolution of cybersecurity.

SPONSORED BY: Akamai Experience the Edge

How It Works

Decoupling access and connections shrinks the attack surface.

To understand the mechanics of a Zero Trust security model, consider the folly of giving users access to everything on a network when they require access to a single application. Traditional network security does just that. Once a user crosses the threshold and validates onto a network, that user often will have free access to poke and prod across a range of systems and applications.

Zero Trust decouples shared network access from the remote user connection, limiting a user's access only to those applications that are necessary and authorized. Limiting access can be done through hardware solutions that use multiple firewalls to achieve micro-segmentation. The level of complexity required, however, can quickly bog down IT resources.

Taking a more elegant approach, implementing Zero Trust using an identity-aware proxy to manage access, provides app-level security and a seamless end user experience. Users experience for authorized apps is unchanged. They log on through a web portal and only see the apps they have access to with a single-sign on experience. When opening an app, instead of accessing it on the network, requests flow through the proxy, which investigates and monitors every request. The proxy is aware of identity and can implement least privilege so that users get only the necessary level of access. This provides you the ability to endure your most sensitive apps and date, such as human resources and financial, are out of reach and invisible to everyone except authorized users.

And even before those application-layer safeguards kick in, Zero Trust ensures that only legitimate users get access to applications. Controlling access begins with strong authentication and a layer of geofencing. Those safeguards ensure that a device is authorized to a particular user and that the connection is coming from an expected location. Zero Trust then applies a dynamic range of systems checks to ensure that software patches are current; that the device is running the most recent operating system; and that the browser does or doesn't have known critical vulnerabilities.

In addition to validating the health and safety of the device, Zero Trust examines the user, validating name and password and confirming the presence of a layer of multifactor authentication or recognized client certificate.

Finally, Zero Trust validates end-users' activities, tracking requests over time to ensure that user behavior aligns with security expectations, such as did the user log-in from New York at 5:00pm and then attempt to log-in from Sydney at 5:05pm?. Zero Trust vets requests to ensure that they make sense, aren't syntactically malicious.

Validating device, users, and activity in an iterative way is more rigorous than the conventional name-and-password paradigm. The dynamic nature of today's IT systems demands a robust security strategy.

Moving beyond VPN

Securing access inside the perimeter is key.

The virtual private network (VPN), the longtime workhorse of enterprise networking, has been used to extend trust to remote users. As IT has evolved, however, security chiefs and IT leaders are questioning the premise of VPNs, often concluding that it is flawed.

VPN opens a conduit for remote users to access networks, a vital function at a time when many workers rely on mobile devices. By granting access at the network layer, it is feasible for a client on the trusted network to discover and probe all sorts of apps that typically exceed the least-privilege set of apps.

Zero Trust, a simple and effective means to user access, significantly reduces IT complexity.

In a Zero Trust environment, external users launch sessions by way of a branded portal or a client connector. Authorization requests move through a cloud-based proxy which in turn talks to the active directory environment and applications themselves. When external users request a connection to an internal application, creation of a unique pathway facilitates the connection.

This arrangement eliminates the need for an inbound port, a doorway that could swing open too wide and create a security risk. In addition, the Zero Trust model applies a range of checks to validate the system integrity and identity of end users, while implementing multi-factor authentication along the way.

Zero Trust, then, provides another layer of protection against one of the perils of the VPN paradigm: the "lost laptop" nightmare. In such a scenario, a found device grants a nefarious hacker complete freedom of movement within a network. Zero Trust also helps limits opportunities for authorized users to explore parts of a network that are off-limits. As an application-based constraint, Zero Trust helps to keep everyone in his or her lane.

Zero Trust also checks the access of contractors and other third-party users whose presence on the network has concerned many IT chiefs. It simplifies overall architecture, a desirable goal for IT departments that deploy multiple VPN concentrators, sometimes well-removed from their Infrastructure as a Service cloud server. By combining all access-related activity at the proxy, Zero Trust enables a slimmer simpler system profile.

SPONSORED BY: Akamai
Experience the Edge

Trust in Zero Trust

Getting user buy-in is critical.

The buy-in of a network's users is critical to the success of any new security deployment. Without rank-and-file support, employees are capable of tuning out or disregarding new security initiatives. It's incumbent upon IT leaders who pursue a Zero Trust approach to bring end users along with them

Employees are burned out by changing cybersecurity requirements. Among CISOs, 78 percent say the biggest risk to their organizations is "people trying to do their jobs the way they want with a disregard for policy," according to a report by the Society for Human Resource Management.

Unlike other security approaches that emphasize compliance by users, Zero Trust is virtually transparent. Users access applications the way they always have. This seamless experience is among the attributes of Zero Trust that support the change management aspect of implementation. There's very little here for the IT team to explain, indoctrinate, justify or motivate. When employees see it in action, the premise of a new security offering becomes easier to swallow.

It's not just the simplicity that sells users on Zero Trust. For years, end users were told that they had compromised security by falling for a phishing attack and unwittingly downloading something that should have been left alone. From the perspective of those employees, Zero Trust shifts the burden of security away from end users to where they think it rightly belongs, in the lap of IT. Everyone needs to be trained in good cyber hygiene, but when it comes to change management, Zero Trust scores high with end users who prefer to spend more time on mission attainment, less in the security loop.

To deliver on the promise of seamlessness, IT departments will need to do some work to enable Zero Trust, which limits user access based on predefined roles and permissions. Ideally, IT departments will collaborate with application owners to create definitions and ensure identity is adequately and accurately mapped.

The process of engagement and collaboration will help to ensure a smooth transition. By working closely with application owners, IT can help ensure that end users across the system feel a sense of buy-in, that they recognize and appreciate the benefits of the security paradigm. For starters, it is simpler and more secure.

Rather than reinforce its longstanding role as the roadblock to getting things done, the IT department can use Zero Trust to reposition itself as a partner to other business units. By working together to implement Zero Trust, it's possible to form powerful new alliances in support of better security across the enterprise.

SPONSORED BY: Akamai Experience the Edge

The Upside of Zero Trust

Among many benefits, ease of use is near the top.

Zero Trust rethinks security. It suggests a shift away from the longstanding practice of perimeter defense, toward the adoption of a cloud-based, application-centric approach to security.

The perimeter approach isn't working. Zero Trust offers a simpler, smarter way to implement security while simultaneously lowering the overall burden on IT staff.

Consider third-party contractors. It's been a heavy lift to onboard these users. You give them a laptop, deploy a certification, implement local device management, load and configure VPN software. Zero Trust collapses the process, streamlining third-party connections via the Enterprise Application Access.

Zero Trust likewise simplifies routine maintenance, in part by shifting from VPNs, which obligates IT to keep up with vulnerabilities, to a SaaS model where the provider owns vulnerability management.

IT change management also gets streamlined and simplified. If you're engaged in a merger, for example, or switching from one contractor to another, it requires effort to introduce new end points in a conventional architecture. As a cloud service, Zero Trust allows IT to onboard a new contractor once and then flow through the needed identity information to all end users in a single initiative. The architecture of Zero Trust makes it inherently simpler to manage such tasks, without having to reconfigure applications or reset multiple VPNs.

Zero Trust also is optimized to handle security in an increasingly HTTPS-driven world. Whereas the conventional security apparatus cannot see inside encrypted packets, Zero Trust is designed to automatically decrypt and inspect encrypted traffic at the proxy level. This lightens the operational burden on IT while simultaneously eliminating blind sports, allowing operators to peer inside the payload, rather than making inferences based on ports and protocols. The new approach is simpler and safer.

In much the same way, built-in Recursive DNS queries make it possible to catch attacks earlier. Inherent to Zero Trust is the notion of considering data from as many data sources as possible. By looking to see how an end point is behaving in terms of DNS services, the system gains deeper insight and, again, enables IT to catch potential problems earlier and with less effort.

Finally, Akamai's Zero Trust solutions are built from the ground up to plug into dev ops workflows, with APIs and an open architecture that readily integrate with existing IT solutions. When implementing Zero Trust, these elements help to ensure a smooth and seamless transition.