HPE GreenLake

Understanding new security challenges in an edge-to-cloud environment

Zero trust strategies remain the key to navigating the new world of risk.

As computing shifts from the data center to the cloud and the edge, complex hybrid environments are making it more important than ever to ensure the security of users, devices, and data. Users working from home en masse, the proliferation of questionably secured Internet of Things (IoT) devices, and a larger and more sophisticated cybercriminal community have all been instrumental in making the attack surface broader, more complex, and harder to defend.

Of course, we should have seen all this coming years ago.

“The dissolving perimeter started in the early 2010s or even before that,” says Larry Lunetta, vice president of WLAN and security solutions marketing in Aruba. “These are not new phenomena. It’s only how they manifest themselves that’s new.”

Keatron Evans, principal security researcher at the Infosec Institute, a part of the Cengage Group, says these changes are upending how we think about security. “With people working remotely, traffic isn’t directed through the fortress of the SOC anymore,” he says. “Billions of dollars have been spent on building a security infrastructure, and now a lot of that is being bypassed.”

For Lunetta, the fundamental consideration of modern security is the increasing focus on the edge not just as a simple connectivity point but also as a potential point where compute and storage work are done. “It’s a different perspective, but the concerns are still the same,” he says. “Unless and until you connect to IT resources, you’re not a threat. And as soon as you do, you are. That’s where constructs like zero trust come in.”

Why zero trust matters more than ever

Zero trust is becoming critical in an edge-to-cloud environment because we’ve forced the issue. IoT devices are released with default (or no) user IDs and passwords, organizations and users are slow to install patches, and drive-by malware insertion attacks are commonplace due to poor cyber hygiene. “But it’s not the devices themselves that you’re trying to protect; it’s the IT infrastructure,” says Lunetta. “IoT devices like cameras and thermostats have been used as on-ramps, but that’s not where the damage is done. They just give attackers a way to insert themselves into the network.”

He adds, “The idea of corporate whack-a-mole is a tired cliché, but it’s accurate enough—and proof that organizations can’t win by simply chasing the latest threat. Organizations must have a strategy, they must have an architecture, and they must understand that they don’t have infinite resources to go into cybersecurity protection, so they must prioritize where they invest.”

According to Lunetta, we must develop security frameworks that consider not just the infrastructure but also user and workload behavior. “Zero trust is not just about network access,” he says. “It’s about identity- and policy-based access and enforcement of access to IT resources.”

The five key security challenges in the modern enterprise

For years IT’s approach to security has been to throw one software package after another at emerging problems in the hopes of staving off issues as they develop. But we’re now at the point where such an approach simply won’t work. With edge-to-cloud environments, “we can’t do all this by just ladling in third-party products all over the place,” says Lunetta. “Now, the infrastructure has to give you a hand—whether it’s securing storage resources, compute resources, or the cloud.”

Lunetta says a proper zero trust framework should address five key security challenges:

1. **Eliminate network blind spots:** Start by mapping the network inside and out, exposing IoT devices, remote users, and anything else that connects to IT resources from the edge so it can be profiled and managed.

2. **Verify identity before allowing access:** Simply inputting a user name and password is no longer sufficient to determine if a user is valid. New authentication techniques that consider user location and behavior ensure that only legitimate users and devices can connect to network resources.

3. **Compare endpoint configuration to compliance baselines and remediate as needed:** This key step allows security teams to define and enforce configuration guidelines, such as mandating patch installations.

4. **Establish least-privilege access to IT resources by segmenting traffic via identity-based policies:** Another critical component of zero trust, this step is designed to ensure network services are segmented based on the user's role. For example, marketing staff should not have access to app development cloud services or the on-premises accounting server. Even during a breach, usage policies can help ensure that damage is contained.

5. **Continuously monitor the security state of the user and device, and bidirectionally communicate with other elements in the security ecosystem:** The zero trust framework must be monitored in real-time. In case of any compromise, all rights stay suspended while the problem is investigated. Again, this limits the potential for damage.

According to Lunetta, users can implement this framework through a traditional on-premises model or a virtual cloud service.

Zero trust: Hand in hand with SASE

One of the more interesting questions around zero trust revolves around the emerging Secure Access Service Edge (SASE) framework approach, which promises converged network and security-as-a-service capabilities no matter where workers are located.

Some see SASE as the next step in modern security, so does zero trust still matter in an era where SASE works as advertised? Lunetta says it does, at least for now. Estimates vary, but reports hold that about 50% of workloads are still running on-premises.[1] "Most customers still need a zero trust strategy that integrates with and complements what happens from a SASE perspective," he adds.

However, regardless of the infrastructure specifics, it's critical that all enterprises, whether on-premises or off or somewhere in between, get started with zero trust measures soon. Work from home isn't going away, and the IoT is only becoming more prolific. Attackers are taking note of all this and using such trends to their advantage.

For the enterprise, Lunetta says, the message is clear: "The bottom line is that any time you make decisions about compute resources, storage resources, or the cloud, you need to ask one key question: Is this decision supporting my zero trust strategy?"

Learn more at

greenlake.hpe.com/security

[1] Estimates vary but reports suggest significant workloads are still running on-premises.

a50007981ENW