The Basics of Zero Trust Architecture + 8 Best Practices

Devolutions

ZERO TRUST ARCHITECTURE ENTERS THE PICTURE AND STRIVES TO CLOSE THE VULNERABILITY GAP

The conventional approach to information security is to deploy enforcement mechanisms at the network perimeter, such as next-generation firewalls, proxy servers, network intrusion detection systems, and so on.

However, in recent years, organizations have become increasingly wary of automatically trusting users merely because they are behind the perimeter, or on a trusted network. That is where zero trust architecture enters the picture and strives to close the vulnerability gap.

What Is Zero Trust?

Introduced about a decade ago by Forrester Analyst John Kindervag, zero trust is based on the idea that nobody should be automatically trusted — even if they are behind the perimeter or using a trusted network. Instead, prior to accessing parts of the network, users, machines and apps should be authenticated through technologies such as MFA, IAM, encryption, analytics, and so on.

A key element of zero trust is the Principle of Least Privilege (PoLP). As we have previously discussed, PoLP is a policy in which end users are given only the amount of access they need to carry out their jobs — nothing more and nothing less.

It is important to clarify that the zero trust approach does not involve eliminating the perimeter. Rather, it leverages network micro-segmentation to move the perimeter in as close as possible to privileged apps and protected surface areas. In other words, instead of putting a security guard in the lobby of a building, zero trust puts a security guard in front of the elevators, stairwells, each office, etc.

The zero trust concept aligns with what many sysadmins and other information security professionals have been saying for years: assume that everyone — including those inside the organization — represents a potential cybersecurity threat until it is proven otherwise. The extension of this vision is that the "castle-and-moat" approach to perimeter security is out, and micro-segmenting and granular perimeter enforcement is in.

Benefits of Zero Trust

There are several benefits to implementing zero trust architecture, including:

- Prevents customer data from being exfiltrated to a command and control (C2) server outside the network.
- Reduces time-to-breach detection.
- Increases visibility into network traffic.
- Streamlines the security stack, as cloud-based, zero-trust solution vendors are responsible for managing, monitoring, troubleshooting, patching and upgrading.
- Enhances user experience through mechanisms like MFA and SSO, which eliminates the need for users to remember complex passwords and re-authenticate throughout the day.

Zero Trust Security Best Practices

1. Add prioritized cloud technologies to replace unauthenticated legacy services and systems. As advised by OpenSource.com: "Retrofitting security is hard. Ensuring it's applied moving forward is a lot easier. By drawing a line in the sand and ensuring all future deployments are compliant, the accumulation of technical debt can be avoided in an impactful way."

2. Design zero trust architecture based on how data moves across the network, and how users and apps access sensitive information. As advised by cybersecurity firm Finjan: "This will assist in determining how the network should be segmented, and where protection and access controls should be positioned using virtual mechanisms and/or physical devices between the borders of different network segments.

3. Verify trust upon access to any network resource using MFA in real-time. For more information on MFA, read our article here.

4. Extend identity controls to the endpoint to recognize and validate all devices. Just verifying users is not enough.

5. Organize users by group/role to support device policies. For more insight on implementing Privileged Identity Management (PIM), read our article here.

6. Leverage automatic de-provisioning, along with the capacity to wipe, lock and un-enroll stolen or lost devices.

7. Educate and coach end users to be part of the solution in the new zero trust environment. Otherwise, they will be part of the problem. Here are some end user training tips.

8. Regularly update end user rights based on changes to roles/jobs, as well as changes to prevailing security policies and compliance requirements.

From Our CSO Martin Lemay

A zero trust environment leverages PoLP and Defense in Depth. Defense in Depth adds multiple diverse controls in an environment that creates layers of security. Just like an onion, an attacker would have to peel its way to the heart. It is a means of slowing down attackers as much as possible using a variety of intricate defenses between networks and systems. Combined with monitoring, it will be a lot easier to detect attackers as they try to circumvent these controls in an effort to reach sensitive assets.

It is important to realize that moving to zero trust is a process that will take time — and there will be obstacles along the way that will put leadership, IT and end-user patience to the test. However, it is well worth the effort given that in network security terms, trust is something that must be earned rather than assumed. As advised by Forrester: "Zero Trust isn't a one-time project — it's a long-term, strategic goal that should be applied in all areas of the enterprise."

Zero Trust in Your Organization

Where is your organization on the zero trust spectrum? If you're thinking about implementing it, please share some issues and challenges that you are facing. If you have already implemented zero trust or are in the process of doing so, please share your experiences with the community — the good, the bad, and the ugly. We can all benefit from your knowledge.