ManageEngine
PAM360

Does Zero Trust replace "traditional" current IAM practices?

- Ian Aitchison

www.manageengine.com/pam360

Trust no one. Why Zero Trust makes PAM even more important

These days you can't open an internet industry news feed without hearing about Zero Trust. It's the latest hot topic in IT and information security. There's a lot of good in the Zero Trust model, but the current noise and hype is adding uncertainty around the more traditional security models in identity and access management (IAM).

Does Zero Trust replace "traditional" current IAM practices?

The biggest question seems to be around privileged access management (PAM). I've heard a few people recently commenting: "We don't need PAM anymore; we're going to Zero Trust".

I would have zero trust in anyone that gave you that message. As is typical with security, a multi-layered approach requires application and management of multiple IAM techniques, from single sign-on (SSO) to PAM to identity governance and administration (IGA), and more.

Let's look at how Zero Trust adds another layer, but doesn't remove the need for strong PAM. And we'll finish with a good cake analogy.

First, some background.

Why Is Zero Trust a thing?

There are many articles on this. I'm not going to repeat the same long descriptions, you can easily find this elsewhere. The main points are:

1. The old business model for an IT security business was as a citadel securely surrounded by a strong wall and a deep moat, and all citizens within the wall were trusted when inside.

2. Everyone's big switch to the cloud, Software as a Service (SaaS), and home working has meant that the citizens are working outside the walls at home, at a remote office, when traveling, or during a COVID-19 lockdown. They're also used to working in a modern SaaS/cloud/consumer-app way, without tripping over things like permissions, file shares, and VPNs. It's nice working outside, until you need to get to something inside.

3. Zero Trust takes the consumer and SaaS experience of personal identity authentication whenever required, and uses that throughout the corporate resources and applications. There is no wall and no "trusted" open access zone. Everyone and everything needs authentication, equally, at relevant points, whether inside or out.

The walls come tumbling down.

What about PAM?

Privileged access management, at its most basic starting point, exists to solve a uniquely "citadel" problem.

- The old business model has organizations running their own racks of servers in a basement, inside the citadel. There are lots of servers—in the dark, with flashing lights.

- IT admins access those multiple servers and services using "privileged" super user administrator accounts. They log in as local admin a lot.

- When you have hundreds (or thousands) of servers, and several super-user administrator staff, those local admin accounts are common, shared, and used by many IT administrators. "What's the local admin password?" is a common IT internal question. Sometimes the answer would be "It's on the whiteboard". Yikes!

- If a local admin logged into your web server at midnight, and deleted 1,000 website resources, you don't know which person actually did that. You only know that the Local Admin account was used by someone.

Of course, it didn't just stop at the web server. In the old business model, it came down to one misguided principle: privileged accounts were "anonymous" and could be shared. With that, all it took was one bad employee and bad things happened.

Along comes PAM tools—such as ManageEngine PAM360—which secure your privileged accounts; ensure that they can only be accessed by a known person, for a known reason, at a known time; audit their use; flag warnings; and manage across large infrastructure.

It's true that a Zero Trust model should reduce the overall dependency and sharing of anonymous privileged accounts. But it also increases the importance of managing a wide range of accounts that have privileges. The local admin accounts don't go away; you need to still secure and manage them, and ensure they're not being abused or misused.

Knowing when and why they're used is more important. For that, you really need credentials vaults, session monitoring, behavior analytics, and event correlation to achieve all the audit, compliance, and governance constraints required to ensure your organization is strong and safe.

It's all about good cakes

Hopefully this explanation makes things clearer. Zero Trust—like a layer of frosted icing—is vital for ensuring your organization has a strong security "cake". But that cake must be made of multiple layers. Those layers include all parts of IAM, and particularly PAM.

Zero Trust doesn't replace all the layers that make up the cake, but it helps ensure it's the most secure cake.

Don't trust the icing salesperson who says you don't need a cake anymore.

www.manageengine.com/pam360

4141 Hacienda Drive Pleasanton,
CA 94588, USA
US +1 888 204 3539
UK : +44 (20) 35647890
Australia : +61 2 80662898
www.manageengine.com/pam360

ManageEngine
PAM360