PING IDENTITY | UBERETHER IAM ADVANTAGE PARTNER

Why authorization is at the heart of zero trust

A modern identity, credential and access management infrastructure continuously verifies known users' permissions

Bryan Rosensteel | Ping Identity

Identity is incredibly valuable, but all its value is derived from what it protects. Breaches are not about the breach of the identity credential, they're about the breach of the data that credential protects. And government data is particularly valuable.

In the past, applications were responsible for authenticating a user's identity. However, FIPS 201-3 Section 7 instructs agencies to redirect such requests to a federation engine. Now agencies can start pulling in telemetry information to understand a user's or a device's overall riskiness. For example, if there is a zero-day vulnerability in a particular chipset, an agency can decide to block any devices with that chipset from accessing the network.

From authentication to authorization

We have tended to focus on the person behind the keyboard, but a digital identity is much more comprehensive.

It's not just who or what they are (in the case of a non-person entity), but also what they're coming through. Telemetry information can build that context and take the user from an unknown to a known state during authentication, and then authorization takes over.

With authorization, agencies can determine whether known users have the right permissions to perform a specific action. It's no longer a question of whether they can get into an application but whether they can execute that API, go into that folder or access that URL.

Every time a user performs an action, an authorization event is run to determine whether they should be doing what they're trying to do. That notion of continuous authorization is at the heart of zero trust, and it can be achieved through a modern identity, credential and access management infrastructure.

A powerful security model for government

All of Ping Identity's technologies are available through UberEther's IAM Advantage platform. For identity governance, the platform uses SailPoint's technology, which creates a lot of entitlements or attributes in a very sophisticated way. Everything that is happening in the identity governance engine is stored in a directory where it can be read by Ping Identity. So, for example, when a user logs in, we can feed that authentication information to a privileged access management module so agencies can apply fine-grained access controls.

Agencies can set up all these technologies very quickly, which makes IAM Advantage a powerful model for government. The platform excels in resource-constrained and security-centric environments, and it gives agencies unparalleled functionality and scalability.

With IAM Advantage and Ping Identity, agencies can strengthen their ability to protect valuable data by modernizing the way they manage identities and access. ■

Bryan Rosensteel is principal solutions architect at Ping Identity.