5 STEPS
TO ZERO TRUST ACCESS

Modern enterprise security is a complex task of managing risks that constantly change from multiple varied locations. Firewalls and network-based access have always been a critical part of enterprise network security, but they're less relevant with today's mobile users consuming resources that are hosted in private datacenters and multiple public clouds, all from a range of corporate and personal devices. Zero Trust access uses continuous and adaptive authentication and authorization to keep unauthorized users out and protect against data and application attacks.

If you're a security practitioner beginning your journey toward Zero Trust, here are the steps you should take:

#1

STOP ONLY VALIDATING THE NETWORK. Customers access your applications from public WiFi in coffee shops on a regular basis, so validating the network isn't enough. Your employees and partners must also be able to do the same. This means that critical high-risk applications have to be safely exposed to the open Internet.

#2

AUTHENTICATE THE USER. Intelligent authentication is the backbone of a Zero Trust security architecture. This means the user needs multiple "factors" to prove their identity, with the three factors being something the user knows (like a password), has (like a phone) and is (like a fingerprint). Different user activities might require different levels of authentication. For example, reading email might only require a password, but issuing a paycheck might require a password and proof of ownership of a private key stored on a hardware device.

#3

AUTHENTICATE AND VALIDATE THE DEVICE. Sometimes, even valid users can be tricked into doing work on compromised devices. If that computer or phone is compromised, critical enterprise data and passwords will also be compromised, even if the user has been strongly authenticated. Device identification and certificate issuance can be leveraged to check whether the user is working on validated hardware that hasn't been tampered with.

#4

AUTHENTICATE THE APPLICATION. Even if a valid user is on a validated device, they still might be missing a critical security patch. They may even have been conned into installing a malicious browser plugin or be using an imposter application. Any of these cases could allow an attacker into a critical system. Methods of application validation vary widely. Some things—like OS version control—can be accomplished through device management. Others—like OAuth client validation—require newer and tougher security standards like Proof Key for Code Exchange and Token Binding.

#5

AUTHORIZE THE TRANSACTION. Finally, the transaction itself must be authorized. A central authorization engine must judge whether or not a user is allowed to perform a transaction. Without enough information to make a decision, "No" should always be the default answer. This may involve static rules like "only employees can send corporate email" and dynamic rules like "only users with a risk score below 65 can view the corporate directory." To determine whether or not a current transaction is malicious, a risk scoring system employs a number of weighted variables like behavioral biometrics, continuous authentication, location, time and comparison against patterns of past attackers.

To learn more about getting started on your journey to Zero Trust, visit www.pingidentity.com/en/platform/initiatives/zero-trust.html

Ping Identity

#3408 | 02.22.2019 | v01