FLYER

A Zero-trust Strategy Has 3 Needs

Identify, Authenticate, and Monitor Users and Devices On and Off The Network

Traditional security models operate under the assumption that everything inside the organization's network should be trusted. However, automatically extending trust to any device or user puts the organization at risk when either becomes compromised, whether intentionally or unintentionally. That is why many security leaders are turning to a zero-trust approach to identify, authenticate, and monitor users and devices, both on and off the network.

Digital innovation is creating new leaps in productivity, but at the same time creates new cybersecurity risks. Attackers, malware, and infected devices that bypass edge security checkpoints often have free access to the network inside.

For these reasons, organizations can no longer trust users or devices on or off the network. Security leaders should assume that every device on the network is potentially infected, and that any user is capable of compromising critical resources, intentionally or inadvertently. A zero-trust strategy shifts the fundamental paradigm of open networks built around inherent trust to one that delivers on the zero-trust principles of:

- Ongoing verification of users and devices
- Creating small zones of control
- Granting minimal access to users and devices

Discover and Identify Devices

The proliferation of applications and devices is expanding the perimeter, creating billions of edges that must be managed and protected. Overwhelmed IT staff struggle to manage the flood of devices, whether those are coming from Internet-of-Things (IoT) initiatives, bring-your-own-device (BYOD) policies, or any other area of the corporate environment.

The first step of adopting a zero-trust strategy is to discover and identify all devices on the network—whether that's an end-user's phone or laptop, a network server, a printer, or a headless IoT device such as an HVAC controller or security badge reader. With this visibility, security teams then can know every device type, function, and purpose it has within the network. From there, teams can set up proper controls of the access those devices have. Then, once proper control is in place, a zero-trust access approach also includes continuous monitoring and response of devices, which helps to identify and remediate problematic devices so they cannot infect other devices or systems on the network.

Know Every User That Accesses Your Network

User identity is critical in developing an effective zero-trust policy. Zero-trust access (ZTA) is about knowing and controlling who and what is on your network. Role-based access control is a critical component of access management. Organizations need to know every user that is attempting to access the network. Are they an employee? A contractor? A guest? A vendor? Establishing user identity requires log-in and multi-factor authentication; passwords are weak and frequently stolen. Certificates should then be used to enforce identity, and can be tied to role-based access control (RBAC) to match an authenticated user to specific access rights and services.

Once identity is established, access policies are determined by a user's role in the organization. A "least access policy" can be used to grant access to those resources necessary for a role or job, with access to additional resources provided only on an as-needed basis.

As the zero-trust model is more widely adopted, security leaders can begin to implement the right controls that grant users the right access to the network from anywhere. The ability to onboard all users with role-based access to the network provides a robust network security that benefits the entire organization and the entities (partners, suppliers, contractors) it works with. Zero-trust network access (ZTNA) is the natural evolution of virtual private network (VPN) technology because it offers better security, more granular control, and a better user experience. Unlike a VPN, the ZTNA application access policy and verification process are the same whether a user is on or off the network. By default, users on the network are assumed to be no more trustworthy than users that are off the network.

Protect Assets On and Off the Network

Enhanced workplace mobility, coupled with an increased emphasis on remote work, and the ability to work from anywhere has led to increased interest in endpoint security and ZTNA as a way to improve or replace a VPN network.

With a zero-trust strategy in place, organizations can address the challenge of protecting off-network devices by improving endpoint visibility. Vulnerability scanning, robust patching policies, and web filtering are all critical elements of a zero-trust strategy. In addition, a zero-trust approach can enable secure remote access to networked resources via VPN connectivity. This allows security teams to see, control, and protect every asset whether it is on or off the network. Going beyond VPN, ZTNA extends traditional ZTA network access to per-application usage, so systems administrators not only know who is on the network but even which applications they are currently using, with transactions and usage constantly being monitored and inspected.

Next-stage Considerations

A true zero-trust framework identifies, segments, and continuously monitors all devices, which makes it possible for organizations to ensure that their internal resources remain secured, that data, applications, and intellectual property remain protected, and that network and security operations are simplified overall.

July 15, 2021 9:00 AM
696154-B-0-EN