Traditional security models operate under the assumption that everything inside the organizations’ 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 Access (ZTA) 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 Network Access strategy shifts the fundamental paradigm of open networks built around inherent trust, to a zero-trust framework through the adoption of rigorous network access controls.

A ZTA strategy focuses on network connectivity, and has three essential functions.

1. WHAT: Know every device that’s on the network

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 ZTA 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
A Zero-trust Access Strategy Has 3 Needs

2. WHO: Know every user that accesses your network

User identity is critical in developing an effective ZTA policy. 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.

3. ON and OFF: Know how to protect assets on and off the network

According to a recent report, 63% of companies are unable to monitor off-network endpoints, and over half can’t determine the compliance status of endpoint devices.¹ One of the primary culprits for this challenge is enhanced workplace mobility, coupled with an increased emphasis on remote work.

With a ZTA strategy, 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 virtual private network (VPN) connectivity. This allows security teams to see, control, and protect every asset whether it is on or off the network.

Next-stage Considerations

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