← All Articles

What is a Zero Trust Solution?

Zero Trust solutions are frameworks for securing an organization's data and infrastructure in modern IT networks with a "never trust, always verify" approach by constantly authenticating users, devices and connections on a network.

Zero Trust Solutions Explained

In the past, organizations tended to trust any request originating inside the network. However, this practice enables attackers who have successfully breached defenses to move freely throughout the network. In contrast, a Zero Trust approach authenticates everyone and everything inside or outside the network on every request.

Zero Trust solutions ensure that legitimate users and applications can access the resources they need, but nothing more. As a result, the Zero Trust framework can block inappropriate access and lateral movement throughout an IT environment.

Why Zero Trust Solutions Matter

Zero Trust solutions address several key trends in IT environments and cybersecurity.

- **Changing IT infrastructure.** Traditionally, security has focused on protecting the perimeter of an IT network. Security teams have relied on firewalls and other tools to inspect and monitor traffic entering and leaving the network. But the rise of hybrid cloud infrastructure has obliterated the network perimeter. Data and IT resources may live anywhere in the world, making traditional network security technology ineffective.
- **Highly distributed workforces.** Workers in today's hybrid workplaces may connect to the network anywhere on unsecured home or remote networks. As a result, it's harder for IT teams to provide a secure connection.
- **Sophisticated security threats.** Threat actors are constantly finding new ways to breach defenses. Once inside a network, they can often move undetected as they target high-value assets.

The Zero Trust framework improves security by blocking and neutralizing many common security threats that can otherwise take advantage of these new IT developments.

How Zero Trust Works

Zero Trust solutions implement several principles to improve network security.

Risk awareness
In a Zero Trust framework, security teams assume threat actors have already breached the network. Security activities focus on identifying and remediating threats as soon as possible.

Least-privilege access
Zero Trust systems make data and resources inaccessible by default. The principle of least privilege gives users only as much access as they need for business purposes at any moment. Broad permission to access data and IT resources is never granted.

Real-time monitoring
Security teams must constantly monitor the network for threats and suspicious traffic. Tracking data as it moves through the network helps IT teams validate users and prevent misuse of resources.

Microsegmentation
Microsegmentation techniques create security perimeters around individual assets or small sections of the network. As a result, a successful breach in one area won't impact security throughout the network.

Multi-factor authentication
Multi-factor authentication (MFA) requires users to present two or more pieces of evidence to verify their identity. This practice dramatically reduces the possibility that unauthorized users can access IT resources.

The Components of Zero Trust Solutions

Technologies for implementing Zero Trust focus on securing six areas of an IT environment.

- **Identities.** A Zero Trust solution for authenticating users and managing role-based access control policies ensures that only valid users have access to the network.
- **Endpoints.** Endpoint security solutions validate user-controlled devices like laptops and smartphones and autonomous devices like IoT sensors.
- **Applications.** Securing the application layer is critical to the Zero Trust framework. Microsegmentation solutions help protect Zero Trust application access for both on-premise and cloud-based workloads.
- **Data.** Zero Trust data security solutions identify sensitive data, protect it with encryption and restrict access only to users with legitimate business needs.
- **Infrastructure.** All infrastructure – including routers, switches, cloud and IoT – must be protected with a Zero Trust approach.
- **Networks.** Zero Trust solutions for networks include encrypting traffic end-to-end and implementing network segmentation to prevent unauthorized access.

Additionally, Zero Trust platforms include automated technologies that minimize human error, increase efficiency and consistently apply Zero Trust policies throughout the IT environment. Monitoring and analytics deliver comprehensive visibility and insight into the health of systems and the behavior of users.

Zero Trust Solutions from Forcepoint

As a premier Zero Trust vendor, Forcepoint has offerings for organizations seeking superior Zero Trust security services.

Zero Trust Network Access (ZTNA)
Forcepoint ZTNA makes it easy to implement Zero Trust policies to verify remote workers. This Forcepoint solution provides access to only the private apps each user needs rather than all the apps in internal data centers and private clouds. Forcepoint ZTNA offers real-time protection with agentless access on any browser or device, allowing remote workers to connect to apps using their own devices.

Data Loss Prevention
Forcepoint Data Loss Prevention (DLP) supports Zero Trust data security by enabling businesses to discover, classify, monitor and protect data – with zero friction in the user experience. Using security policies to detect sensitive information going in and out of the organization, Forcepoint DLP blocks sensitive data from leaving the domain. With Forcepoint, IT teams can prevent data from being lost, accidentally or maliciously leaked or accessed by unauthorized users.