Zero Trust Security Explained

Traditional cybersecurity protocols can't keep up with the rapidly evolving modern workplace environment. The complexity of hybrid work, the rising number of fully remote employees and the dramatic increase in the use of cloud-based systems make traditional perimeter security ineffectual. A new security model is needed to keep the corporate network safe. This model is "zero trust."

Zero trust is adapted to the modern workplace. It embraces mobility and protects people, networks, applications and devices, regardless of their location. Review the following guidance to learn why zero trust is important, how it works and how it can benefit your organization.

What Is Zero Trust?

Traditional network security trusts the identity and intentions of users within an organization's structure. This puts the organization at risk from malicious internal actors and rogue credentials by allowing unauthorized and uncompromised access to the organization. The phrase "trust, but verify" is often used to describe traditional network security approaches.

The zero-trust approach removes the concept of trust from within an organization's structure. With zero trust, a data breach is assumed with every access request. Every access request must be authenticated and authorized as if it originated from an open network. The concept "never trust, always verify" is emblematic of the zero-trust approach.

What Are the Benefits of Zero Trust?

The zero-trust approach is one of the most effective ways for organizations to control their network, applications, and data. This is especially important today, as companies expand their infrastructure to include cloud-based applications and servers. The growing usage of locally hosted machines, VM and Software-as-a-Service products, and a dramatically increasing number of remote employees have made it difficult for organizations to secure their systems and data. Implementing a zero-trust approach benefits companies in a wide range of ways, including:

- **Minimizing your organization's attack surface**—By granting the lowest level of access possible for users and devices to perform their essential functions, organizations can minimize the affected area within their organization should a breach occur.
- **Improving audit and compliance visibility**— The first step to implementing zero trust is for an organization to know what devices exist and which credentials are on each device. In this way, devices are constantly kept in an audit-ready state.
- **Reducing risk, complexity and costs**—All access requests are vetted prior to allowing access to any company assets or accounts. This dramatically increases real-time visibility within the organization and helps prevent costly data breaches.
- **Providing Layer 7 threat prevention**— Layer 7 refers to the application level of the Open Systems Interconnect model. This layer identifies communicating parties, supports end-user processes and applications, and consults privacy and user authentication. By establishing who can access the different levels of your organization at any given time the zero-trust approach stops unauthorized users or applications from accessing your organization's crucial data and prevents the unwanted exfiltration of sensitive information.
- **Simplifying granular user-access control**— Zero trust requires an organization to define which users may access certain aspects of an organization. As a rule, each user is granted the least privilege possible to perform their necessary functions.
- **Preventing lateral movement**—Segmenting the network by identity, groups and function allows organizations to contain breaches and minimize the damage from a hacker who was allowed to move freely within the organization's perimeter.

How Does Zero Trust Work?

By combining a wide range of preventative techniques, including identity verification, behavioral analysis, microsegmentation, endpoint security, and least privilege controls, implementing a zero-trust approach can significantly reduce an organization's risk of becoming a data breach victim. Zero trust relies on three essential principles:

- **Verify explicitly.** Every user request must be authenticated and authorized using all available data points. This step is designed to ensure the person or application requesting access is who they say they are.
- **Use least privileged access.** Users should be given the least amount of access necessary to perform their authorized functions. Just-in-time (JIT) and just-enough access (JEA), risk-based adaptive policies and data protection can all help secure data and user productivity.
- **Assume breach.** Use end-to-end encryption to prevent data from flowing to undesired endpoints. Use analytics to drive threat detection, improve visibility and enhance defenses.

How Can I Implement Zero Trust?

Zero trust is relatively simple to deploy. Adopting the principles of zero trust doesn't require any costly products. Use the following principles to employ zero trust at your organization:

- **Define the attack surface.** To adopt a zero-trust framework, your organization's critical data, assets, applications and services must be identified. This critical information forms a "protect surface," which is unique to every organization.
- **Create a directory of assets.** Determine where the sensitive information lives and who needs access to it. Know how many accounts there are and where they connect. Consider removing old accounts and enforcing mandatory password rotation.
- **Adopt preventative measures.** Give users the least amount of access necessary to do their work. Use multifactor authentication to verify accounts. Establish micro-perimeters to act as border control within the system and prevent unauthorized lateral movement.
- **Monitor continuously.** Inspect, analyze and log all data. Escalate and store logs with anomalous activity or suspicious traffic. Have a clear plan of action for how to handle anomalous activity.

For additional risk management guidance and insurance solutions, contact us today.