ManageEngine

The Pillars of Zero Trust

The modern Zero Trust security model isn't limited to network micro-segmentation, identity governance, or software-defined perimeters. These are key parts of your Zero Trust model—depending on which approach you take.

However, Zero Trust isn't just network segmentation or identity and access management. It's built upon five key pillars and, without them, your security strategy will remain incomplete:

1

Data security

Data is the new gold, it's what attackers are usually after. That's why identifying, classifying, managing, and securing your data both at rest and in motion is a key part of any Zero Trust security approach.

2

Networks

A potential starting point for a Zero Trust implementation, this pillar or control focuses on network segmentation, isolation, and control. By being able to monitor and control your network, you can limit the risks posed by cyberattacks.

3

Identities
(people and devices)

The core of identity-centric Zero Trust approaches, this control focuses on managing, monitoring, and securing user and device access. This can reduce the risks posed by stolen credentials, malicious insiders, and other threats.

4

Workloads*

Securing all applications, computational resources, and other components associated with your workloads can go a long way towards mitigating security risks to your organization.

5

Endpoints

Organizational endpoints, including IOT devices,are often ripe targets for threat actors. To reduce the risks posted by them, you need to be able to monitor, manage, and secure every device on your network, and isolate them if needed.

These pillars aren't the end of the Zero Trust ecosystem. To ensure holistic coverage and security you also need to have:

Visibility and analytics tools

Security monitoring and analytics tools enable your security team to know what's happening in your network. They can help spot ongoing cyberattacks, signs of compromised accounts, malicious insider activity, and more.

Automation and orchestration

Automation is the name of the game, and security is no different. Having security orchestration automation and response capabilities at your disposal can shorten incident response times, and act as a force multiplier for your security teams.

Reference

The Zero Trust eXtended (ZTX) Ecosystem, Forrester Research (August 23, 2021)

The path to Zero Trust starts with identity, Identity Defined Security Alliance

Learn more about Zero Trust at
manageengine.com/zerotrust