Zero Trust Is Your Network Security Hero

Part 1:

Zero Trust: An introduction

Online, anyone can pretend to be someone else. Organizations have learned that to protect their network security, they need to shift from "Trust that this person is who they say they are, and verify later" to "Verify their identity first, and then trust them."

Vulnerabilities can come from a surprising number of places – including within an organization. An employee might click on a link in a phishing email. A bad actor might gain access to your network or to one of your third-party vendors.

Threats to cybersecurity are increasing, making it more important than ever to have proactive IT solutions. Zero Trust Network Access (ZTNA) provides a framework for top-level protection. Here we'll dive into exactly what Zero Trust is, its importance, core principles, benefits, best practices, and how we can help you set up Zero Trust for your organization.

Continue reading and you'll learn:

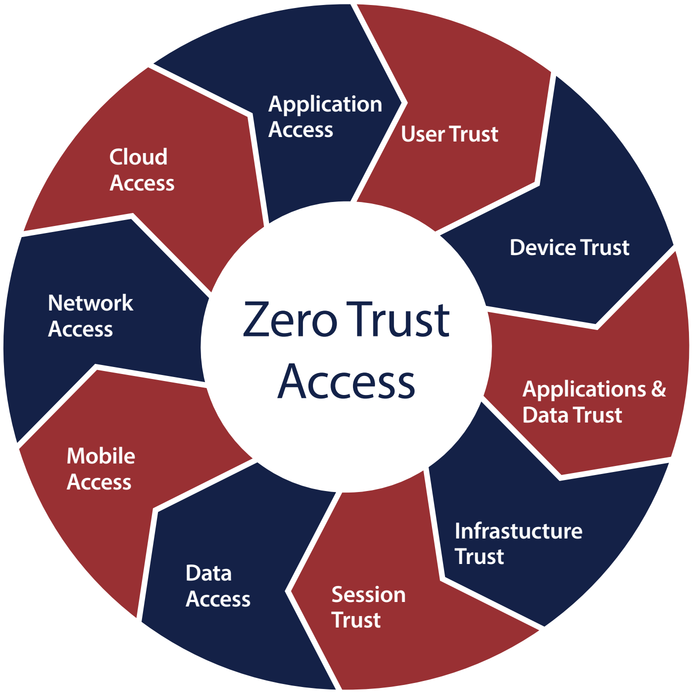
- Zero Trust, explained
- The impact of Zero Trust on network security
- The core principles of Zero Trust
- The key benefits of Zero Trust
- Setting up Zero Trust for your organization

Part 2:

What is Zero Trust?

In 2010, a former Forrest Research analyst, John Kindervag, coined the term "zero trust." Since then the concept has evolved into the complex framework of Zero Trust Network Access (ZTNA). So what is it, exactly?

ZTNA is a framework where users are denied access (to files, accounts, applications, and other resources) until they can prove they are who they say they are. A key component of Zero Trust is that users should have "least-privilege" access – meaning, they will only be able to access the resource they requested, and nothing more, until they can prove their identity again.



What is Zero Trust?

Networks no longer have a traditional edge. They can be located on-premise, but they can also exist in the cloud – or they can be a combination of both. Because resources and employees can be in any location, there need to be stronger safeguards against bad actors.

OLD VS. NEW

The old approach was that if you're in the organization/ network, you should be trusted. The Zero Trust approach is that you should be continuously checking to make sure users attempting to access resources are who they say they are.

Zero Trust is important because firewall rules and blocking by packet analysis are no longer strong enough security measures. Just because someone connects through your VPN or SWG does not mean that the connection is fully safe and should be trusted.

MORE CONNECTIONS CREATE MORE VULNERABILITIES

With more devices being added to organizations' networks, there are more opportunities for these devices to be exploited. This vulnerability is compounded by the fact that infrastructure is being expanded to include cloud-based apps and servers. The number of service accounts is also increasing, again, creating more opportunities for bad actors.

More accounts make it more difficult to maintain security. Zero Trust combats this issue by segmenting the network by identity, groups, and function. It controls user access, helping organizations contain breaches and minimize potential damage.

The Core Principles of Zero Trust

Zero Trust takes everything into account, from geographic location to behavior patterns, in determining legitimacy. There are 4 core principles of a Zero Trust framework: access, diversification, monitoring, and strategy.

ACCESS

No one gets access by default. There are zero trusted sources. Without applying this principle, a framework cannot be considered Zero Trust.

DIVERSIFICATION

Diversify your preventative techniques. Utilize MFA, least-privilege access, and microsegmentation (dividing access by identity, groups, and users, which limits the spread of a breach).

MONITORING

Track threats in real time. If there's suspicious activity, it needs to be investigated immediately to see if there's a breach or if a user's access needs to be revoked.

STRATEGY

Utilize Zero Trust as one part of a comprehensive security strategy. It's essential to still automatically perform updates, monitor and upgrade devices, and establish an incident response plan.

The Benefits of Zero Trust for Network Security

Zero Trust improves network security by identifying risks and adding layers of protection.

IDENTIFY AND REDUCE RISKS

Zero Trust gathers insights about cloud activity, users, and devices. Automated technology can gather data to track normal behavior patterns, which helps establish a baseline. When activity occurs that strays from the baseline, it's easier to see that this activity could be a threat to the network. Once the risk is identified, it can be addressed.

EXPAND PROTECTION

Zero Trust improves governance and compliance while maintaining control across a network. It helps identify threats, which are constantly evolving, and stop events before they occur, such as:

- phishing emails
- compromised machines
- stolen passwords
- stolen database credentials
- keyloggers

Zero Trust Best Practices

For your organization to see the benefits of Zero Trust, it's essential that you implement these two best practices: never stop monitoring and always follow least-privilege protocol.

NEVER STOP MONITORING

You don't know what threats are there if you're not looking for them. That's why Zero Trust frameworks require that all activities should be logged using data security analytics. Again, if you establish baselines based off of normal behaviors, you can identify suspicious activity when it breaks the pattern. Automation can make this logging and identifying efficient and even affordable.

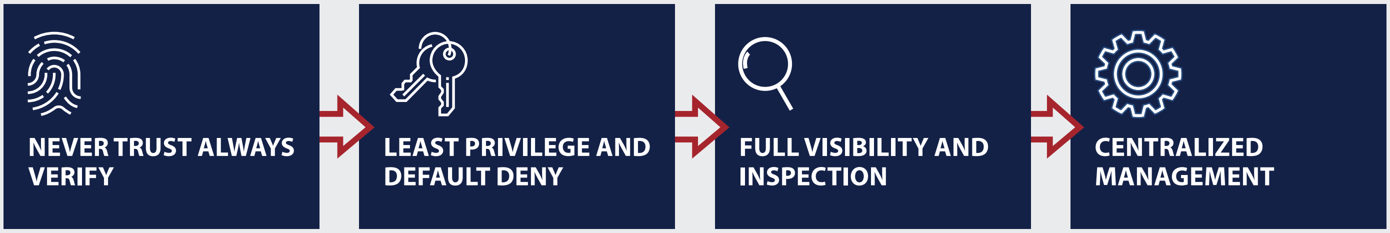
ALWAYS FOLLOW LEAST-PRIVILEGE PROTOCOL

Uses cannot access files, apps, accounts, or any other resources until they've proven their legitimacy. Users don't have the right to access data. They have the privilege – but only after they've proven that they are who they say they are by following MFA protocol. Access should be granted on a case-by-case basis.

Setting Up Zero Trust for Your Organization

Zero Trust frameworks won't be the same for every organization, however, all should use a type of controller. These controllers gather real-time data, which they use to build a risk profile. The data includes:

- the location of the device
- the network it's being connected to
- the application being used
- and more



NEVER TRUST ALWAYS VERIFY

LEAST PRIVILEGE AND DEFAULT DENY

FULL VISIBILITY AND INSPECTION

CENTRALIZED MANAGEMENT

How Net-Tech Provides the Zero Trust Framework IT Support Seattle Organizations Need

Net-Tech offers Zero Trust as part of our PTO IT subscription program. You don't have to make any decisions about which processes to follow. As your managed IT services provider, we take care of it all – from the installation to the monitoring to the updates.

We will assess your organization's unique situation during your complimentary consultation. Then, we can help you migrate to the best tools and services to match your needs. Net-Tech will manage and monitor your entire cyber strategy to keep your data both safe and accessible using cutting-edge frameworks like Zero Trust.

Want to discover more ways to keep your systems safe? Contact us for a complimentary IT analysis with one of our top cybersecurity experts today.

net-tech

2100 124th Ave NE, Ste 112
Bellevue, WA 98005
425-452-8324 | **net-tech.com**