BEYOND ZERO TRUST

ConsoleWorks

Introduction

This document establishes what Zero Trust is and the design principles needed to both attain and to go beyond it. You will learn why it is an important foundation for securing your assets and devices and why it should be considered your baseline for cybersecurity defense. While the calls for implementing Zero Trust have never been louder, it is important that you are already thinking ahead and strategizing how to bolster your defense further, going beyond Zero Trust.

Featuring maturity models and design considerations, this will help you to understand where you currently are on the road to cybersecurity maturity and the components required of it. Each organization is unique, with its own complex network designs and considerations. While your needs may differ from other organizations, this will serve to inform your journey and elucidate considerations you need to defend against today's sophisticated attacks.

Zero Trust Overview

Zero Trust security is a model and set of system design principles that assumes a breach in your network is inevitable or that a breach has already occurred. It consists of a mixture of system monitoring, secure remote access and security automations to maintain the security of your environment and give a user the least-privileged access required to endpoints within your network.

The goal in a Zero Trust environment is to reduce your chances of compromised security and give yourself more opportunities to detect threat actors. It also builds more response options to quickly deploy and address a detected threat.

Zero Trust addresses the modern challenges businesses face and offers an approach resolving many of the vulnerabilities created by changes in how businesses operate today that the traditional "castle and moat" style of network defense is unable to effectively accommodate.

Why Implement Zero Trust

As technology has changed, business has benefitted and transformed. Work is accomplished through a myriad of applications, across a fleet of devices with multiple users accessing the network from anywhere, in part of an intricate supply chain. What was once centralized is now dispersed across the country or even the globe. Network environments have grown from simply being on-premises, up to hybrid, cloud or multi-cloud implementations.

This added complexity introduced profound gains in productivity for business. It also introduced new vulnerabilities. Users still need fast, simple ways to connect to the network and perform their role. But as users now connect to the environment, ensuring a secure, remote connection is tantamount to maintaining threat-free operations for your business.

Industrial control systems have continued to provide critical operations as their aging technology struggles to keep up the pace and now functions in a world wholly different from when they were built. Limited password capabilities, limited diversity of usernames and often direct access needed to the asset, leaves ICS uniquely vulnerable to those who wish to attack.

These changes happened alongside changes to the supply chain. With partners and contractors now added into the mix of accessing your devices, you have no way of knowing where they were prior to accessing your network or what they were exposed to.

Unfortunately for many businesses, one thing that has not changed is how networks defend an environment that has changed significantly. Threat actors, either hackers or nation-state, have equipped their selves with sophisticated ways to break through your defenses and exploit the gaps left open in your network as you try resolving new challenges with old solutions.

A Security Model to Meet Today's Threats

As attacks have grown in the past few years, their sophistication and aggression have as well. They targeted IT and OT alike, attacking critical pipelines and infiltrating networks through holes in supply chains. It has been nearly impossible to avoid news of these attacks, especially as they seemed to plague the news cycle month after month.

With COVID further disrupting the workforce, and quickening many organizations' moves to remote work and changes in network infrastructure, many were left with a patchwork, hasty solution to try to address these threats.

As your network is no longer a castle with a moat around it, you need a security model that is adapted to the newest threat environment and prepares you to protect your assets, devices and data.

Zero Trust is built with three foundational principles in mind:

1. **Never trust a connection.**
Older design philosophies rely on a verify once policy and giving trust to connections established within their security perimeter. In today's environment, this is not effective at preventing attacks. Your design decisions for network defense need to be more risk aware and always assuming worst intent from a connection.

Zero Trust verifies based on multiple data points about the user – their identity, their location, their device, their role, what they are attempting to access and if there are any abnormal traits associated with any of these points. This is not performed once; this is done every time.

While the user is connected, their session is also monitored. Should any behavior performed by the user's role be deemed out of the scope of their intended purpose, the connection can be flagged or immediately terminated. In tandem, verifying a connection every time to ensure it is congruent to your expectations and monitoring each session, you significantly increase your security.

2. **Assume a breach has happened or will happen.**
Zero Trust is a mindset as much as it is an architecture. Part of this mindset relies on the assumption that an attack has happened or will happen, so you must treat every connection as if its origin is unknown and you are always working to verify the connection is

valid and is performing its role as expected. You do not want a connection accessing your network for three hours before you realize said connection should not be there.

Putting this into action means implementing network segmentation to reduce the impact of an attack. By implementing both security zones and segmenting access to devices and users within those zones, you reduce your surface area should an attack occur.

You are constantly verifying connections and using analytics to gain visibility into what is happening on your network so you can have heightened situational awareness and detect a threat or attack before or while it happens, rather than after it has taken place and the damage is done.

3 Least-privileged access.

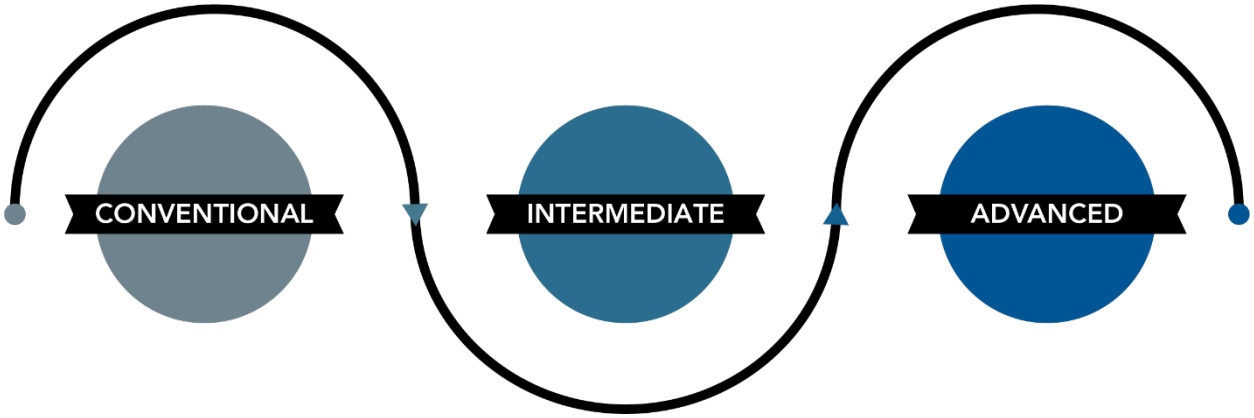
Least-privileged access reduces role privileges and only shows the parts of your network to the user that you want or need them to see to accomplish their role, and only when they need to access it. It is part of ensuring that a user receives only the level of access they need, and only when they need it, to perform their role and nothing more.

A contractor can be granted access for the date and time of his arrival on the site to the exact devices and assets he will touch, for the duration of time that he will need to access them. Once he has completed his job, his access is revoked. The contractor never saw more than he needed to on your network.

If an employee is servicing a ticket, certain accesses can be granted in relation to the needs of the ticket and once the ticket is serviced, access of those devices is revoked.

The theme in least privileged access is that users receive no additional information about your network than is necessary, nor do they gain access to the network beyond durations needed to achieve their role, while also limiting the actions they can perform on endpoints. By enforcing least-privileged access across roles in your network, you reduce any role's ability to gain insights into the network or even access broader elements of the network that could make an attack become debilitating to your organization.

Zero Trust Maturity Model



Conventional

This is the typical approach to cybersecurity and where most organizations who haven't started shifting to Zero Trust are situated.

- Typical "castle and moat" style architecture with a verify once and trust identity model.
- Little to no rules around role-based access.
- Network structure is not segmented, leaving the organization available to large-scale attacks.
- Logging and monitoring are limited. Organizations don't know who did what or when.
- High uncertainty around device baselines or compliance. Probable drift and unpatched, exposed devices.

Intermediate

An intermediate-level organization has implemented more rules around access and started to reduce their vulnerability levels, achieving higher levels of security.

- Access-based policies gate endpoints, networks and data. The user may still be considered "trusted" after verification has occurred. Permissions are managed manually.
- The network is more segmented, reducing risks of an attack affecting the whole environment or having access to everything.
- Monitoring is implemented to understand what has happened and by whom. You now have more insight into what is happening across the network.
- You track your devices and check baselines, though it is infrequent, and it is a long, manual task.

Advanced

Your Zero Trust baseline is established here. While the intermediate level helped you pave the way, at this level you have automated operations, your network is micro-segmented and true Zero Trust policies are enforced company wide.

- Secure, least-privileged remote access, with associated roles and controls are enforced for everyone. Every identity is continually verified, no inherent trust is permitted.
- Your network has been structured into many security zones, each with its own access rules and redundant layers of security.

- You are aware of all your devices and have authenticated them. Your device baselines are checked against your standards to prevent drift or tampering.
- Network monitoring informs you automatically of threats and your threat response is also planned and implemented.

Going Beyond Zero Trust

The Zero Trust architecture was built with today's threats in mind. However, Zero Trust should merely be the architectural foundation in which you build more sophisticated defenses atop. Zero Trust is a great design principle, but technology available today can take you further than the traits that a Zero Trust architecture stresses as key in your environment. By leveraging additional considerations and technologies, you address the areas of cyber security that Zero Trust does not stress or make critical in its approach to network security.

Guiding Principles Beyond Zero Trust

Zero Trust primarily focuses on access and monitoring said access, while fracturing and segmenting how users move within your network. This is all with the assumption of a breach or incoming breach kept in mind. This significantly reduces the perniciousness of threats to your environment but leaves your defense strategy myopic.

Zero Trust does not speak as well to reducing your overall environment of incoming threats and threat reduction because it primarily focuses within. Why build a fortress in a bad neighborhood when you can build in one that is already relatively safe? By making your house secure and also selecting a more secure environment for it, you've further reduced the chances of an incoming threat.

Zero Trust also leaves other important elements of defense within your network out of the equation that are equally important. Below we review key design features and business considerations to further bolster your cybersecurity.

Assess more than just connections.

Your security goes beyond people. In Zero Trust you focus on their access to your devices and assets. It's also critical to assess your devices. Do you know how many devices exist in your network; do you know their status? Do you know their baselines? Have you established a "golden image" of the configuration you want for your devices? Device drift happens over time and leaves you open to new exploits. You need to be prepared to tackle these risks as much as you tackle the risks of users connecting to them.

Authenticating your devices is critical. As users bring their own devices into your network or certain devices remain on the network that no longer have a specific use for your organization, it is important to always be evaluating their utility to your company and their risk they pose to your security.

Important as well, is focusing on your software footprint. As you work to establish high cybersecurity maturity, reducing your footprint on your endpoints should be a goal. Reducing

the footprint of software to fewer devices makes it easier for you to maintain and update them and will keep you more secure.

Every link in your chain must be strong.

Your security needs to start at the business level, with you assessing your supply chain. Look at not only what your vendor's technology is doing for you, but how they are protecting their self and your supply chain. Do you know if your vendors can sustain a massive attack? What is their impact to your business and how have you secured that?

Today's environment has too many supply chain threats for you to not make this a critical point in your vendor evaluations. Make sure your vendor has validated and performed the necessary processes to protect customer and product information and to protect their business.

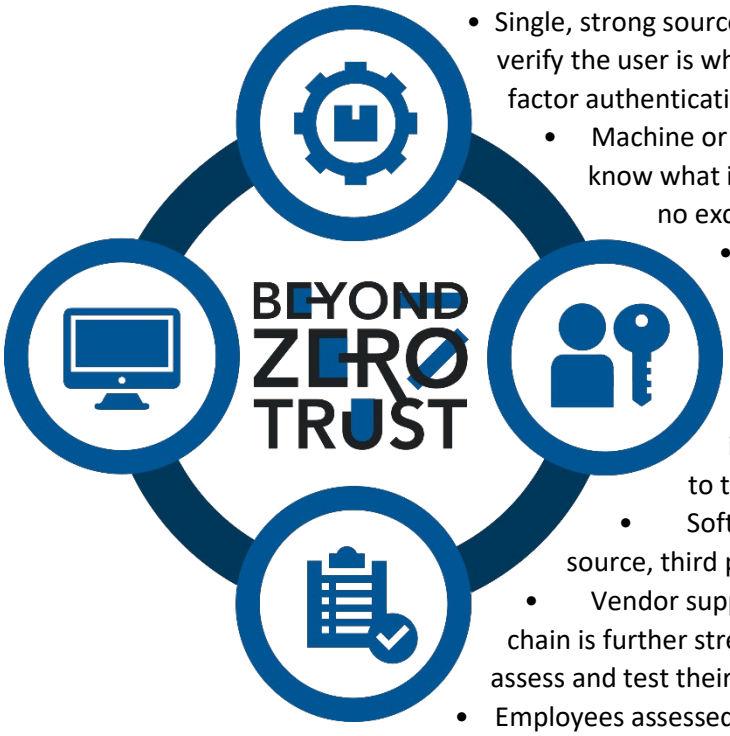
If they can attest to their security practices, through penetration testing of their business and their products, as well as prove their security resilience through other processes, like the SOC for Supply Chain examination or others, you can be more assured that your whole environment, external and internal, is protected.

Sever direct connections.

You want to further visit your connections and their relations to endpoints on your network. While Zero Trust addresses controlling those connections with least-privileged access, severing the direct connection between human and endpoint takes you a step further in protecting your fleet.

The implementation of a protocol break will hamper any direct access to endpoints. All access is negotiated and brokered through the protocol break. As this prevents direct connections to endpoints, users will be unable to pass through viruses, ransomware or malware to the endpoint. This also means no user will know passwords to the endpoints, as they are never directly accessing endpoints.

The Final Maturity Level – Beyond Zero Trust



- Single, strong source of user identity and user authentication to verify the user is who they claim to be and is validated by multi-factor authentication
    - Machine or device authentications ensuring that you know what is in your fleet of devices and that there are no excess, unused devices.
    - Additional context, such as policy compliance and device health are fully automated and ready on demand.
    - Strong extensive automated monitoring, auditing and logging of all activity, available in multiple formats (screen capture, logging to the keystroke).
    - Software supply chain audited for safety (open source, third party, patches)
    - Vendor supply chain audited for safety. Your supply chain is further strengthened by your choice in vendors who assess and test their own security.
- Employees assessed before access is even permitted, with background checks, security awareness training to make sure every level of the organization is security-minded and enforcing Zero Trust.
- Security policies and procedures are reviewed and updated regularly.
- Critical configuration monitoring and change controls. At this level even endpoints are treated as untrusted, always verifying valid accounts and usernames, patches installed, checking against baselines, and monitoring that endpoint's configuration to ensure security and awareness beyond just users.
- New efficiencies enabled through automatic monitoring of problem resolution. Replicating what works and is effective or alerting you to man-made mistakes (innocuous or otherwise) that inhibit the full faculties of your network and create business problems or vulnerabilities.
- Password management is handled automatically. Passwords can be changed across devices, enforcing the unique password requirements for IT and OT environments.
- No software on your endpoints, reducing your burden of needing one more thing to patch and track.
- A protocol break brokers the connection between users and devices, meaning they never directly connect to your endpoints and prevents viruses, malware or ransomware passing through to your devices.

Conclusion

Each company's needs are different and implementations of Zero Trust and beyond will likely happen in steps and phases across specific areas before being adopted entirely. What is most important is that the organization continually strives to implement and adopt the Zero Trust mindset and always evaluates its technologies to ensure that they align with their current and future cybersecurity needs.

Beyond technology, it is also critical that employees at all levels of the organization are onboard. Understanding and reinforcing the Zero Trust mentality at all levels of the company will heighten security beyond what technological defenses accomplish.

Once Zero Trust is attained, it is critical to remember that you have achieved your cybersecurity baseline in today's environment, and that much work still remains to further enhance security and reduce vulnerabilities from an attack.

ConsoleWorks is a cybersecurity platform that innately enforces Zero Trust. You can learn more about it here.