Zero Trust Guiding Principles

Release Candidate

cloud security alliance®

This is a Release Candidate version and is subject to change.

Acknowledgements

The CSA Zero Trust Working Group

The scope of Zero Trust research and guidance necessarily includes cloud and on-premises environments along with mobile endpoints and is applicable to the Internet of Things (IoT) and operational technology (OT). The goals of the CSA Zero Trust (ZT) Working Group are to:

- Collaboratively develop and raise awareness of Zero Trust best practices as a modern, necessary, and cloud-appropriate approach to Information Security (InfoSec)
- Provide thought leadership and educate the industry about the strengths and weaknesses of different Zero Trust approaches so organizations can make informed decisions based on their specific needs and priorities
- Take a deliberately product- and vendor-neutral approach to architectures and mature Zero Trust implementations
- Enable the alignment between technology, security, business and operations.

Lead Authors

Alex Sharpe

Contributors

Madhav Chablani
Frank DePaola
Jonathan Flack
Sai Honig
Shamik Kacker
Andrea Knoblauch
Rajesh Murthy
Denis Nwanshi
Lars Ruddigkeit
Paul Simmonds
Nelson Spessard
Bernd Wegmann
Heverin Joy Williams
Lauren Wise

Reviewers

Sam Aiello
Jason Garbis
Brett James
Yves Le Gelard
Jennifer Minella
Chandrasekaran Rajagopalan
Aaron Robel
Michael Roza

CSA Staff

Erik Johnson
Stephen Lumpe

Table of Contents:

Abstract

Zero Trust (ZT) is a strategic mindset that is highly useful for organizations to adopt as part of digital transformation and other efforts to increase the security and resilience of their organization. Zero Trust is easily misunderstood and over-complicated because of the conflicting messaging within the Security industry, and from the lack of established Zero Trust standards. In fact, Zero Trust is based on long-standing principles that have become more critical because of changes in the way we work and live; remote workers, increased reliance on third parties, and the adoption of the Cloud to name a few. This document is designed to fill the gaps and provide clarity by mapping out the underlying principles, including established Information Security (InfoSec) principles like the Concept of Least Privileged, Separation of Duties, and Segmentation. These guiding principles will remain consistent across all Zero Trust Pillars, varying use cases, different environments, and products. This guidance will evolve as the industry evolves.

Executive Summary

Zero Trust is a simple approach to Information Security (InfoSec) that is often misunderstood and overcomplicated. When properly understood, ZT philosophy and strategy are valuable tools that organizations can use to enhance security, increase resilience, and guide digital transformation. This document seeks to provide a clear understanding of what Zero Trust is and the guiding principles to be remembered when planning, implementing, and operating ZT.

Historically, InfoSec relied heavily on technical controls, with security models based on the ability to collect assets and surround them within a controlled physical perimeter. This is no longer the case. Zero Trust recognizes the holistic relationship between people, processes, organizations, and technology, and that technical controls alone are no longer sufficient. Users were historically presumed to be "trusted" based on their location within the enterprise perimeter. Zero Trust upends this concept by requiring verification, irrespective of location, before granting access to an asset.

Zero Trust leverages long-standing principles like “never trust, always verify,” the concept of least privilege, and the practice of segmentation to increase cyber hygiene, reduce Total Cost of Ownership (TCO) and damage from incidents, and promote faster recovery times. By augmenting their existing security practices with ZT principles, organizations establish a strong foundation for safeguarding their assets in complex and distributed environments. This proactive approach enhances security posture and minimizes potential risks associated with the evolving threat landscape.

Zero Trust also recognizes that breaches happen. To foster resilience, ZT provides a means to contain the “blast radius” and reduce the impact of any breach while facilitating quick recovery. These same techniques increase the work and investment required by bad actors, further reducing the likelihood of incidents.

Recent interest in Zero Trust is driven by new business models, the adoption of the Cloud, and new government requirements. Zero Trust is mandated for all Federal Agencies in the United States by Executive Order[1] and is being adopted globally through initiatives such as the Digital Operational Resilience Act (DORA)[2] and the Network and Information Security (NIS2) Directive[3] in the European Union (EU). Zero Trust provides the required assurance through a combination of basic principles common to all Zero Trust initiatives. This document outlines those basic principles to guide any ZT initiative.

[1] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
[2] https://www.digital-operational-resilience-act.com/
[3] https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333

Introduction

Organizations leverage Zero Trust to transform data and network cybersecurity management practices broadly. Many Zero Trust management concepts have emerged, including principles, tenets, pillars, architecture plans, and frameworks. While this evolution is a journey, transforming through ZT is not equated to a single project (business, operations, technology) or a specific product. Zero Trust is a mature methodology aimed at increasing the protection of critical assets in a highly distributed architecture. It requires upfront planning with all key stakeholders understanding that each ZT journey is unique. The greater the alignment with the business, the greater the likelihood of success in the Zero Trust journey.

Many organizations have changed their operating models to foster cloud adoption and remote work. Traditional security practices do not adequately address the new risk landscape this has created. Organizations seeking to improve their cyber resilience can no longer rely on a hard outer shell or solely on technical controls to mitigate their cyber risk. The cyber threat landscape continues to evolve and expand beyond the capabilities of a traditional fortress model to defend.

The scope of what needs to be protected has expanded as well. We are no longer dealing with just IT assets and data. The scope has expanded to include devices, workloads, applications, and business processes residing outside of IT. This is commonly referred to as Data, Applications, Assets, and Services, or DAAS for short.

By aligning the security architecture with the business operating model, organizations can transform their business while providing proper security without hindering business processes. When accepted as a foundational concept, Zero Trust supports many other enterprise efforts like privacy, compliance, and risk management.

This document provides guiding principles that any organization can leverage when scoping or initiating a move toward Zero Trust.

Target Audience

The primary audience for this document is Information Protection practitioners and their executive management. As guiding principles, the content of this document cuts across all Zero Trust initiatives. We recognize these Guiding Principles will be used by industry bodies and standards organizations as they build out the Zero Trust body of knowledge (BOK).

Guiding Principles

Zero Trust is not a standalone concept or technology. Rather, it is a comprehensive security strategy and approach that encompasses various principles, strategies, and technologies. It is designed to address the evolving threat landscape and the limitations of traditional perimeter-based security models.

The following Guiding Principles are designed to help practitioners stay on track and manage the Zero Trust journey.

Begin with the End in Mind (Business/Mission Objectives)

Zero Trust is a paradigm shift from the traditional fortress model where the good actors are on the inside, and the bad actors are on the outside. The traditional fortress model worked well when used for organizations built in a specific static location. Today, organizations live in an ecosystem that is distributed and, quite often, global. Zero Trust is designed to align the security architecture with the organization's distributed workforce and technology model that does not have an inside and an outside.

It is important to recognize that the guiding principles are stable. What they mean to each organization and the value they deliver is particular to countries, sectors, and individual organizations.

Beginning with the end in mind means a clear vision of your desired direction and destination, allowing you to realize results faster while avoiding burnout.

Desired outcomes often include:

- Enabling you to create value at reasonable risk, whether it be from a new offering, the penetration of a previously unreachable market, or a previously unknown competitive advantage
- Reducing the cost of compliance by establishing a foundation for all of your compliance, cyber resilience, and privacy needs
- Reducing the impact (e.g., cost) of incidents
- Reducing the complexity of your IT and reducing process debt
- Reducing the Total Cost of Ownership (TCO)
- Establishing a foundation for Third-Party Risk Management (TPRM)
- A more resilient Governance, Risk Management and Compliance (GRC) program that is more likely to defend against current and future threats

Do Not Overcomplicate

It is far too easy to forget that at its core, Zero Trust is a collection of long-standing principles applied in a way that aligns the security architecture with the way we work and live. Evolving toward a Zero Trust solution is not as complex as it may seem, especially when pursued as a set of deliberate steps over time coupled with your most critical assets as the priority. Once your most critical assets have been addressed you move through the rest of your assets based on criticality.

Implemented and tested security controls that are preventative, detective, and corrective (or reactive) form the basis of Zero Trust. These fundamentals are critical to the success of your Zero Trust effort:

- Concept of least-privilege access controls (e.g., preventative)
- Separation of duties (e.g., preventative)
- Segmentation/micro-Segmentation (e.g., preventative)
- Logging and monitoring (e.g., detective)
- Configuration drift remediation (e.g., corrective/reactive)

Zero Trust builds on these core principles to move organizations away from the traditional fortress model to the distributed model common to the modern organization. It is also an opportunity to make the controls more granular and more sensitive with the addition of continuous authentication and authorization (e.g., preventative), user and entity behavior analytics (UEBA) (e.g., detective), and dynamic policy enforcement points (e.g., corrective/reactive).

Control types do not need to be reinvented or overly complicated for Zero Trust. Rather, the speed, performance, and agility of existing controls can be optimized.

Security basics form the foundation. The Principle of Least Privilege and Separation of Duties are strong examples. Ensuring all users (employees, contractors, and vendors) are uniquely identified and that their entitlements are reviewed on a regular basis, and updated as needed, is another. Identity life-cycle management is key.

Incorporation of Segmentation and micro-Segmentation helps to enforce the controls mentioned above and reduce the impact of an incident. Automation can simplify the amount of manual processes required in routine tasks.

Products Are Not the Priority

Historically, all things cyber-related have been the domain of technologists. It is only natural to solve technology problems with technology, which usually leads to product purchases and, quite often, consulting services. In many ways, Zero Trust is more about the people, process, and organizational dimensions than the technology itself.

A strategy that relies heavily on products without factoring in the people, process, and organizational dimensions will not be successful. The sole reliance on product purchases to realize your ZT journey is not a ZT journey. If you address the other dimensions first, you will better understand your requirements, supporting a stronger long-term ZT strategy and increasing the likelihood of choosing the right product(s), if any are required.

Access Is a Deliberate Act

One of the key differentiators of Zero Trust is the lack of reliance on a physical or network perimeter. In traditional models, like the fortress model, a user being granted access to the network was deemed sufficient to grant access to other assets. That philosophy arose because of the limitations of the technology that existed when created and because we operated in a world where we could collect assets within a perimeter.

Today, organizations exist in a global environment of remote workers, increased reliance on third parties like the Cloud, and increasingly complex supply chains. In many ways, organizations are more reliant on what exists outside of the walls.

Technology has progressed to the point where we can do better than relying on a physical or network perimeter. Zero Trust takes advantage of these advances in technology so we can better identify users, and make more granular access control decisions more often.

In today's world, identity must be explicitly verified and access only granted after authorization has gone through that verification process.

Historically, we have largely relied on IT organizations to determine who gets access to which assets. In recent years, the world has increased reliance on business owners (e.g., Data Owner) and process owners to determine who gets access to what and for how long. IT organizations are increasingly viewed as custodians (e.g.,Data Custodians.

Inside Out, not Outside In

Using the Inside Out strategy, how you write your corporate policies changes from "What are we trying to defend against?" to "What are we trying to protect?"

Legacy security models rely on a strong outer perimeter. These models presume anyone on the inside is good and anyone on the outside is bad. With de-perimeterization[4] progressing over the past twenty-plus years, more people and assets are outside than inside. This means that the outside in security philosophy no longer fits the way we work and live. Since no organization has unlimited resources (e.g., time, money, energy), we need to apply our energy where it will have the most bang for the buck.

The value of the asset is the guide to prioritizing our efforts. If you have a Business Impact Assessment (BIA), begin there. If you don't, perform an asset inventory and categorize your assets by value. Use a stack ranking of your assets by value (highest to lowest) to guide your work.

Once you know the assets to be protected and their relationships, you can identify both the protect and attack surfaces.

In the modern organization, what we are trying to protect is typically data, applications, assets, and services. Together, they are commonly referred to as DAAS.

- **Data:** This is sensitive data that can get an organization in trouble if it is exfiltrated or misused. Typically, data is considered sensitive because either a third party such as a regulator says it is, or because it is your Intellectual Property or operational data required to keep the organization running..

- **Applications:** The collection of software, hardware, and often infrastructure that cooperate to fulfill a set of requirements.

- **Assets:** A resource that provides value that an organization owns or controls. Assets could include information technology (IT), operational technology (OT) or Internet of Things (IoT) devices including point-of-sale (POS) terminals, SCADA controls, manufacturing systems, and medical devices.

- **Services:** The application of business and technical expertise to deliver value to customers by facilitating organizations' desired outcomes without the ownership of specific costs and risks. In the modern enterprise, this can be cloud-based, like Software-as-a-Service (SaaS), between applications like an Application Program Interface (API), or for common use, like the Domain Name System (DNS).

[4] https://en.wikipedia.org/wiki/Jericho_Forum

The Kipling Method is a standard tool for authoring policies. It is essential to ensure alignment of the security strategy within the business model.

These questions can only be answered through cooperation between the owners of the assets (the business) and the asset custodians (usually IT).

- **WHO** can access the asset? What are they allowed to do? Can I be sure they are who they claim to be?
- **WHAT** asset(s) are they trying to access? **What** actions are they allowed to take?
- **WHEN** does the permitted access begin? **When** does it end? Are there only certain hours access is permitted?
- **WHERE** is the asset located? Can it only be accessed from certain locations? Are certain locations not permitted to access the asset?
- **WHY** does this user need access to this asset? The reason for protecting an asset is its sensitivity. Is the sensitivity defined by a compliance mandate?
- **HOW**. Are there limited ways the asset can be accessed?

Breaches Happen

It is unrealistic to presume you are 100% protected against cyber risks. It is not practical for defenders to plug all of the holes, while attackers only need to find one. At the core of Zero Trust implementation is the verification of the claimed identity and of permitted access directly before granting access to assets.

Traditional models relied heavily on physical and technical controls. Organizations also relied on their abilities to keep bad actors out. As the world has become more digital and the walls have become more porous, the world has recognized that breaches do happen. They are often facilitated by an outsider masquerading as a valid insider and sometimes by an actual insider. The role of Zero Trust is to reduce the likelihood of breaches, to reduce their impact, and to foster quicker recovery. We do this by implementing more robust access controls, paying more attention to detecting potential incidents, and planning for incident response and recovery.

Once it is understood that most incidents are, at the root, a human problem, it is understood that breaches will happen. Instead of focusing on being secure, the practitioner's mindset switches to resilience. The key to reducing the blast radius of an incident is segmentation and micro-segmentation.

Each reduces likelihood and impact by constraining the ability to move laterally across the enterprise and by constraining the propagation of bad acts. For example, if a bad actor takes over the account of a valid user, segmentation means they cannot gain access outside of the valid user's sphere. In the case of malware (e.g., ransomware), the infection of a single machine will not spread throughout the enterprise without impunity.

In more traditional security models, once you are inside the perimeter, you are trusted and can move freely anywhere you want within that perimeter. Older security architectures were like a Cadbury Egg - a tough outer shell with a gooey inside. Imagine a spy traveling freely with impunity once they enter a community.

In a Zero Trust model, users and devices are untrusted everywhere they travel. They must be interrogated before gaining access to any assets. Imagine an old European city with many winding streets, built house to house. Neighbors know each other. If you go to these streets, everyone is suspicious and gets interrogated. Why are you here? What is your business? Are you a thief? A tourist? Here on business? It does not happen once; it happens every place you go. The same is true for Zero Trust. Any time access to an asset is requested, the identity is verified, authorized access is verified, and the interaction is logged. The level of interrogation is commensurate with the value of the assets and the risk environment.

The shift in mindset results in key outcomes from your ZT journey. First, it limits the blast radius when breaches occur (and they will). Second, it reduces a hacker's ability to move laterally across your enterprise. Thirdly, it reduces the impact by limiting which assets can be damaged by a single event.

From the perspective of the Board of Directors and Senior Leadership, predictability may very well be the key outcome. When a user is breached, you know the potential impact is limited - it is no longer the entire enterprise. You know exactly what is at risk. Your likelihood is no longer 100%, and your impact is no longer incalculable.

The ability to more effectively correlate identity, actions, and assets greatly enhances your Data Loss Prevention (DLP) efforts as well. Without a defined perimeter, DLP is no longer as simple as watching what comes in and what goes out. By leveraging ZT principles, with innovative data discovery mechanisms, we can detect potential breaches before they occur, catch them faster when they do and reduce the complexity of administrative and operational data loss tasks.

The key is to verify frequently and in a manner commensurate with the value of the assets. Looking for anomalies in user behavior and presuming that malicious actors want your assets is an integral part of this.

Understand your Risk Appetite

Risk Appetite is a well-accepted risk management concept. Risk Appetite is the level of risk an organization is willing to accept while pursuing its objectives. Inherent Risk is the level of risk that exists before actions (i.e., treatments) are taken. The objective is to treat the risk to reduce it to a level below the Risk Appetite. This is called Acceptable Risk.

Organizations are not monolithic. It is common for different parts of an organization to have different levels of acceptable risk. These are commonly referred to as Risk Tolerance. For example, the Venture Capital part of a Financial Services firm will tolerate a higher level of risk than the Fixed Income part of the same institution. While the distinction is important, the guiding principles of Zero Trust apply equally to Risk Appetite and Risk Tolerance. For the sake of readability, the discussion does not make a distinction.

Zero Trust reduces the Inherent Risk to acceptable levels by implementing controls that reduce the Likelihood,[5] the Impact,[6,7] or both.

The CIA Triad is a widely accepted Information Security (InfoSec) model designed to help organizations look at the potential harm (e.g., impact) to an asset. For the sake of completeness, the NIST and ISO definitions are both included.

1. **Confidentiality:** Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.[8]

   The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.[9]

   Data exfiltration is an example of the loss of confidentiality of an asset.

2. **Integrity[10]:** Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.[11]

   The property that data has not been altered or destroyed in an unauthorized manner.[12]

[5] https://csrc.nist.gov/glossary/term/likelihood
[6] https://csrc.nist.gov/glossary/term/impact
[7] ISO 31000, Risk Management, uses the term "consequences"
[8] https://csrc.nist.gov/glossary/term/confidentiality
[9] https://www.iso.org/standard/14256.html
[10] ISO only has a definition for Data Integrity not Integrity
[11] https://csrc.nist.gov/glossary/term/integrity
[12] https://www.iso.org/standard/14256.html

Loss of integrity is the hardest of the three to grasp. As a general rule, if it causes you a loss in confidence, it is an attack on integrity. For example, a file being infected with a computer virus. Deep Fakes, hallucinations, artificial intelligence (AI), and all forms of fraud involve a loss of integrity.

3. **Availability:** Ensuring timely and reliable access to and use of information.[13]

   The property of being accessible and usable upon demand by an authorized entity.[14]

   Ransomware is probably the most recognizable result of the loss of availability of an asset. By encrypting the data, the business is denied access. When access to a utility like water is denied, that is also an attack on availability.

All organizations need to determine their risk appetite. That determination goes far beyond just their ZT journey. As part of that journey, it is well advised to understand what has been agreed upon, the role of Zero Trust, and the tools regularly used by the organization. The most common tool is probably the Risk Register.

Cyber risk is one of the few risks a business must manage that can affect many others, making it hard to fully quantify. Many organizations have chosen qualitative measures instead (e.g., Very High, High, Medium, Low).

Others are required to, or have chosen to, conform to a standard like the EU's Digital Operational Resilience ACT (DORA[15]), Network and Information Security (NIS) Directive (NIS2),[16] NIST SP 800-53,[17] or the Federal Financial Institutions Examination Council (FFIEC) developed the Cybersecurity Assessment Tool (FFIEC's CAT).[18]

Some organizations have chosen to adopt different quantification techniques to calculate the Value at Risk (VaR).[19] One of the most well-known is the Factor Analysis of Information Risk (FAIR).[20]

Whichever strategy you pursue, the principle remains the same; at its core, Zero Trust reduces risk to acceptable levels.

Organizations, by necessity, must continually evolve or they will cease to exist. The threat landscape is also continually evolving, forcing organizations to continually re-assess their risk appetite. Either can

[13] https://csrc.nist.gov/glossary/term/availability
[14] https://www.iso.org/standard/14256.html
[15] https://www.digital-operational-resilience-act.com/
[16] https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333
[17] https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
[18] https://www.ffiec.gov/pdf/cybersecurity/ffiec_cat_may_2017.pdf
[19] https://www.investopedia.com/terms/v/var.asp
[20] https://www.fairinstitute.org/

uncover new vulnerabilities or new exploits. To further complicate matters, there are always the unknowns that no organization can adequately predict or prepare for. Ransomware is a prime example. The concept was well-known in the community but not mainstream because it was not practical until cryptocurrency became widespread. Collectively, these types of risks are referred to as unknown-unknowns.

The basic blocking and tackling aspects of Zero Trust go a long way towards future-proofing the organization against these evolutions and unknown-unknowns. As new threats present themselves, new vulnerabilities are created, or previously unknown-unknowns appear, the core Zero Trust principles will reduce the Likelihood or Impact, potentially both.

The COVID-19 pandemic, geopolitical developments, supply chain shocks, high-impact climate change events, and the growing cyber threats to critical infrastructure have led to a paradigm shift in how governments and organizations look at operational resilience, so understanding and quantifying your risk tolerance levels will continue to take on greater importance. We are already seeing other jurisdictions worldwide define new legislation like the EU's DORA. This will have a long-term impact on enterprise risk management practices which must continuously innovate and adapt to new cyber threats.

This is where Zero Trust has a crucial role to play. At the very least, it will make your organization more resilient and increase agility.

Ensure the Tone from the Top

Zero Trust is an enterprise effort, and more than just technology, so it requires cooperation throughout all levels of the organization to be successful. This can only be achieved with the proper executive sponsor and clear messaging from the top. The right person must be appointed and kept informed. In a perfect world, Senior Leadership will actively communicate the seriousness of Zero Trust, including alignment with business strategy, proper capital allocation, and corporate policies.

The best of all situations is to have Zero Trust sponsored by the Board of Directors. At the very least, it needs to be sponsored by Senior Leadership. If your Zero Trust effort is confined to a business unit or geography, your Zero Trust effort is best served when sponsored by the Business Unit Leadership or at the top of the Organizational chart within the geography (e.g., Country Leadership).

Communication is key for a successful Zero Trust effort. A Communications Plan structured to ensure alignment between participants and stakeholders through a consistent and traceable flow of information will aid in directing your ZT journey.

A diagram mapping out stakeholders provides clarity regarding roles and responsibilities. Commonly referred to as a Responsible, Accountable, Consulted, Informed (RACI) diagram, it describes the participation by various roles in completing tasks or deliverables for a project or business process.

Leaders should set the tone by fully supporting the Zero Trust model and emphasizing its importance to the organization. They should communicate regularly about the importance. It is also critical to instill a corporate culture that recognizes cyber risk is everyone's responsibility. It is not the responsibility of just a few.

Instill a Zero Trust Culture

Zero Trust is everyone's responsibility, not just the purview of IT or the Chief Information Security Officer (CISO). The core ZT principles should be woven into training and awareness programs. Empowering the workforce to spot and elevate issues as they arise prevents headaches and promotes increased cyber resilience.

What is a Zero Trust culture? It is a culture where employees are keenly aware of what has to be protected and to what degree. Most importantly, all staff understand authorization to access is never implied. It is a deliberate act. All employees and individuals an organization does business with should know how to identify suspicious activities and report any cyber-related concerns to the appropriate channel, as well as understand why certain security controls are in place. A Zero Trust culture is adaptable and not married to any particular technology or architecture. People are empowered to protect assets in the way that makes the most sense for the present and into the future.

Security was once the purview of a discrete department (i.e., IT) but is now pervasive. Developers can embrace it. Business leaders can embrace it. End-users can experience its benefits through friction-free interactions with their devices. Most of all, the organization should understand that Zero Trust enables them to apply technology more intelligently. A risk in adopting this type of culture might lie in reducing the role of a centralized security department before the dispersed cultural awareness has taken root.

Instilling a Zero Trust culture within an organization means promoting an understanding and acceptance of the Zero Trust security model across all levels of the organization.

Start Small and Focus on Quick Wins

Since Zero Trust is a strategy and not a specific set of products, working with its foundational concepts (such as designing from the inside out) can enable teams to achieve success incrementally without large upfront expenditures. Protect surfaces consisting of DAAS elements should be identified and prioritized based on size and impact.

Obtaining and maintaining buy-in from leadership is easier when a small, low-cost protect surface is selected as a pilot so its metrics can be leveraged to highlight the change to the security paradigm and demonstrate business value[21]. Moving towards full Zero Trust brings many positive business outcomes. It is important to continue to highlight the benefits to the larger organization and the risks which were reduced from all cyber-related changes.

Taking on too much and aiming for a bigger win that takes longer can mire a project and correlate an organization's Zero Trust efforts with failure rather than success.

Continuously Monitor

Zero Trust presumes that no participant (e.g., user, device, service, or application) is trusted implicitly. Instead, a decision to accept a claimed identity or to grant requested access is a deliberate act. All requests for access to enterprise resources must be authenticated and authorizations verified, as if they are coming from an unknown source, before access is granted. Even then, it is for a limited duration (not perpetual).

Knowing that bad actors often compromise the accounts of valid users, and malevolent insiders often attempt to exceed privileges to suit their needs, it is important to monitor and log events. Monitoring is essential to detect potential bad acts early. Logging is essential for identifying indicators of compromise (IOC), determining impact, and collecting evidence. Both monitoring and logging foster continuous improvement. It is important to have monitoring in place that will eventually oversee the entire organization's activities.

Monitoring and maintaining a Zero Trust infrastructure involves regular auditing of access privileges, continuous monitoring of network behavior, maintaining up-to-date security patches, conducting risk assessments, and reinforcing user security awareness.

[21] A detailed description of attack surface and protect surface can be found in the Zero Trust Advancement Center Resource Hub hosted by the Cloud Security Alliance, https://cloudsecurityalliance.org/zt/resources/

It is a common misconception that Zero Trust is perimeter free. In today's interconnected world, the perimeter is not as distinct or as solid as it once was. However, we are not relieved of our obligation to be diligent just because we cannot rely on a strategy that guarantees to keep the bad actors out and only allows the good actors in. Quite the opposite, as it is incumbent on organizations to define, monitor, and control internal and external boundaries to protect their assets.

Useful References

- Zero Trust Advancement Center Resource Hub hosted by the Cloud Security Alliance, https://cloudsecurityalliance.org/zt/resources/
- US Federal Zero Trust Resource Hub. https://zerotrust.cyber.gov/

Suggested Reading

- National Security Telecommunications Advisory Committee (NSTAC), Report to the President on Zero Trust and Trusted Identity Management, 2022 https://www.cisa.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20Zero%20Trust%20and%20Trusted%20Identity%20Management%20%2810-17-22%29.pdf
- Zero Trust Maturity Model Version 2, Cybersecurity and Infrastructure Security Agency (CISA), April 2023 https://www.cisa.gov/zero-trust-maturity-model
- Executive Order on Improving the Nation's Cybersecurity, The White House, May 12, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
- Press Release for NSA Guidance on Advancing Zero Trust Maturity Throughout the User Pillar, US National Security Agency (NSA), 2023 https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3328152/nsa-releases-recommendations-for-maturing-identity-credential-and-access-manage/
- Advancing Zero Trust Maturity Throughout the User Pillar, National Security Agency (NSA), March 2023 https://media.defense.gov/2023/Mar/14/2003178390/-1/-1/0/CSI_Zero_Trust_User_Pillar_v1.1.PDF
- Zero Trust Architecture, National Institute of Standards and Technology (NIST), Special Publication 800-207, 2020 https://csrc.nist.gov/publications/detail/sp/800-207/final