Connection®
we solve IT®

MODERN INFRASTRUCTURE AND MULTICLOUD SOLUTIONS

A Practical Guide to Zero Trust Implementation in Multicloud Environments

Table of Contents

Introduction

Cyber resilience brings together business continuity planning, cybersecurity and operational resilience. The goal is to be able to maintain operations with little or no downtime even if the worst-case scenario—a devastating cyberattack or other disaster—occurs.

In today's world, cyber resilience should be among every organization's North Star objectives. On a global scale, cybercrime now costs its victims over $11 trillion per year, a number that's predicted to climb above $20 trillion by the end of 2026.[1] The expenses associated with data breaches, ransomware, and extortion attacks continue to increase, growing on average by more than five percent annually since 2020.[2] But these costs are not borne evenly by all victims. Some organizations—such as those in highly regulated industries like healthcare—see higher average breach-associated expenses, while others—such as organizations with mature security operations programs that leverage automation and AI—tend to experience lower costs.

The gaps between cybercrime victims who experience devastating losses and those that see only minor impacts from a breach event will grow wider as threat actors advance their capabilities. Emerging technologies like generative AI are making it possible for attackers to launch less sophisticated attacks (like phishing) at ever-greater scale. It's also becoming easier to create highly customized business email compromise (BEC) and social engineering campaigns.

To protect their revenues and reputations—and ensure they can retain their customers' trust—organizations of all sizes across industries must shift away from yesterday's ways of thinking about and implementing cyber defense.

This is exactly what Zero Trust addresses.

$11 trillion
annual cost of cybercrime worldwide [1]

58% increase
in phishing attacks from 2022 to 2023 [3]

108% increase
in business email compromise (BEC) attacks over the same period [4]

---

[1] Statista, Estimated cost of cybercrime worldwide 2018-2029, July 2024.

[2] IBM, 2023 Cost of a Data Breach Report.

[3] Zscaler, 2024 ThreatLabz Phishing Report

[4] Abnormal Security, H1 2024 Email Threat Report

Zero Trust: A New Vision for Protecting Modern Technology Ecosystems

With more and more organizations moving key portions of their IT infrastructures to the cloud, it's essential to adopt cybersecurity strategies that are a good fit for today's technology environments. They're typically complex, distributed, and borderless. In this sense, they're radically different from the on-premises networks—with servers and desktop computers protected by a perimeter firewall—that legacy security approaches were created to protect.

Zero Trust was invented to fill this gap. Designed to eliminate the vulnerabilities that arise when users are trusted automatically by default (like when they're inside the perimeter of a legacy network), Zero Trust is well suited for modern IT environments, where users in a wide variety of locations are constantly accessing data and services both inside and outside the corporate network.

But understanding what it takes to adopt Zero Trust isn't always simple. Nor is it easy to figure out how to advance your organization's Zero Trust maturity. Selecting the right technologies to implement requires wading through a sea of competing vendor claims, and even before you can do that, you've got to find the right strategy.

To make it easier, we've put together this practical guide. In it, you'll find a five-step plan to help your organization accelerate its progress on the journey to Zero Trust.

What Is Zero Trust?

Zero Trust is a cybersecurity strategy based on the core principle of "never trust, always verify." The term came into mainstream use as industry experts observed growing numbers of cyberattacks in which network perimeters were successfully breached. In the early 2000s, most corporate networks had an internal "trusted zone" that was protected by firewalls, a model known as the castle-and-moat approach to cybersecurity.

As IT environments and the threat landscape evolved, it became increasingly clear that nearly every aspect of this model was flawed.

- Network perimeters simply cannot be secured in ways that are 100% fail safe. It will always be possible for determined attackers to find holes or gaps.
- Whenever an attacker is able to gain access to the "trusted zone," it becomes very easy for them to steal data, deploy ransomware, or otherwise cause harm, because there's nothing stopping further movement.
- As organizations increasingly embrace cloud computing—and allow their employees to work remotely—the concept of being on-network is less and less relevant to their security posture.

Zero Trust was created to address these challenges, providing a new model for securing data and resources that's based on continuously validating that a user/device should be granted access before they're allowed to connect to any service or resource.

Zero Trust Is Becoming a Cross-Industry Standard

Zero Trust has been widely adopted by organizations across many different verticals. According to one recent survey, nearly 70% of technology leaders are in the process of implementing Zero Trust policies within their enterprises.[5]

There have also been far-reaching efforts to adopt Zero Trust within the public sector. The 2021 Executive Order on Improving the Nation's Cybersecurity, for instance, called for the federal government and organizations in critical infrastructure sectors to advance their Zero Trust maturity.[6]

Both the National Institute of Standards and Technologies (NIST) and the Cybersecurity and Infrastructure Security Agency (CISA) have published detailed definitions of Zero Trust, along with extensive guidance on how to achieve it.

[5] Enterprise Strategy Group, Trends in Zero Trust, April 2024.

[6] The White House, Executive Order on Improving the Nation's Cybersecurity, May 2021

Zero Trust: Official Definitions

National Institute of Standards and Technologies (NIST):

Zero Trust (ZT) is the term for an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources. A Zero Trust architecture (ZTA) uses Zero Trust principles to plan industrial and enterprise infrastructure and workflows. Zero Trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet) or based on asset ownership (enterprise or personally owned). Authentication and authorization (both subject and device) are discrete functions performed before a session to an enterprise resource is established. Zero Trust is a response to enterprise network trends that include remote users, bring your own device (BYOD), and cloud-based assets that are not located within an enterprise-owned network boundary. Zero Trust focuses on protecting resources (assets, services, workflows, network accounts, etc.), not network segments, as the network location is no longer seen as the prime component to the security posture of the resource.[7]

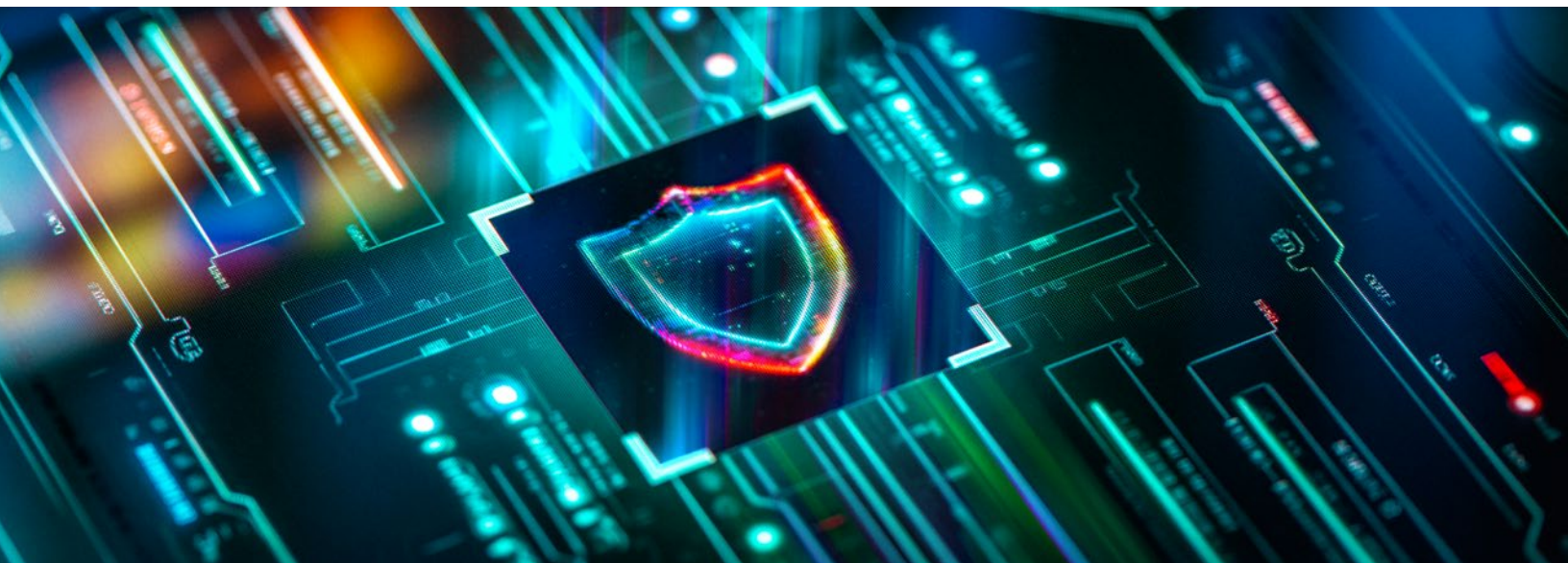
Cybersecurity and Infrastructure Security Agency (CISA):

Zero Trust provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised. Zero Trust Architecture (ZTA) is an enterprise's cybersecurity plan that uses Zero Trust concepts and encompasses component relationships, workflow planning, and access policies. Therefore, a Zero Trust enterprise is the network infrastructure (physical and virtual) and operational policies that are in place for an enterprise as a product of a ZTA plan.[8]

---

[7] NIST, NIST Special Publication 800-207: Zero Trust Architecture, August 2020..

[8] Cybersecurity and Infrastructure Security Agency (CISA), Zero Trust Maturity Model Version 2.0, April 2023.



Making Progress on Your Zero Trust Journey

Zero Trust is broadly accepted as a security standard that organizations should strive toward. It's also, as the above definitions make clear, a complex concept.

Most organizations with established security programs will already have implemented at least some controls designed to protect their internal corporate network (e.g., physical firewalls). For these organizations, the challenge is to move away from the legacy model (and the ways of thinking that accompany it) towards Zero Trust adoption—gradually, while staying within budget, and while continuing to advance visibility, control, and the ability to respond to threats.

This might not be easy, but it's very possible with the right strategy.

Step 1: Start by understanding the Zero Trust frameworks.

NIST's definition of Zero Trust describes it as an architecture—that is, a way to plan and implement an enterprise security infrastructure and set of workflows on the basis of Zero Trust principles. The focus is on protecting individual resources, not networks or portions (segments) of networks.

NIST SP 800-207 also includes a roadmap for adopting Zero Trust. The publication describes the building blocks that are needed to create a Zero Trust Architecture (ZTA). Different tools, solutions, and/or processes can be used here, as long as they play the right role within the architecture's design.

From NIST's perspective, the goal of Zero Trust is to prevent unauthorized access to resources while making access control enforcement as granular as possible.

There are two key areas of emphasis:

1. Mechanisms for making decisions about which users or traffic flows are granted access to resources

2. Mechanisms for enforcing those access decisions

There are multiple ways to implement a Zero Trust Architecture. These include:

1. Identity governance-based approach

2. Micro-segmentation-based approach in which individual resources or small groups of resources are isolated on a network segment protected by a gateway security solution

3. Software-defined perimeter-based approach in which a networking solution like software-defined wide-area networking (SD-WAN), secure access service edge (SASE), or security service edge (SSE) configures the entire network so as to restrict access to resources in accordance with ZT principles

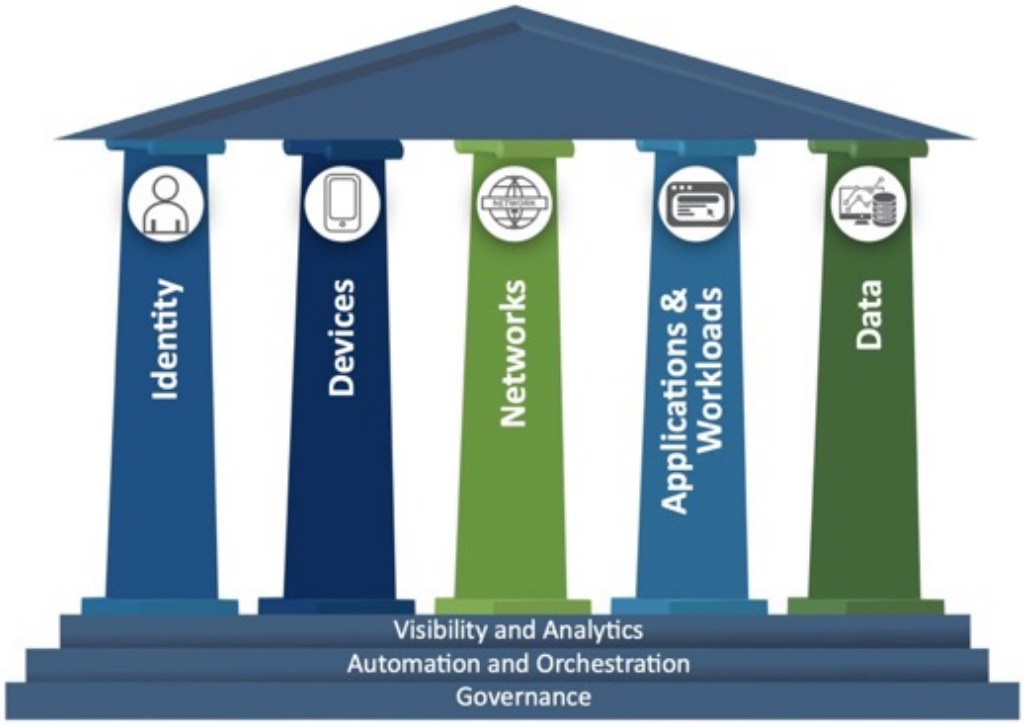
CISA's Zero Trust Maturity Model is based on similar concepts. It emphasizes enforcing fine-grained security controls that govern users' access to systems, applications, data, and assets, and building out these controls while keeping users' identities, context, and data access needs in mind.

This approach is complicated. According to CISA, the path to Zero Trust is an incremental process that may take years to implement.

CISA's model includes five pillars. Advances can be made within each of these areas to support the organization's progress towards Zero Trust.

> Zero trust presents a shift from a location-centric model to an identity, context, and data-centric approach with fine-grained security controls between users, systems, applications, data, and assets that change over time.
>
> **—CISA, Zero Trust Maturity Model, Version 2.0**

The Five Pillars of the Zero Trust Maturity Model [9]



[9] Cybersecurity & Infrastructure Security Agency, https://www.cisa.gov/

Step 2: Understand what it means to progress towards maturity.

CISA's Zero Trust Maturity Model describes four stages of progress towards maturity: traditional, initial, advanced, and optimal.

It's possible to progress toward maturity within each of the five pillars (identity, devices, networks, applications and workloads, and data). This typically involves adding automation, enhancing visibility by collecting data for use in analytics, and improving governance.

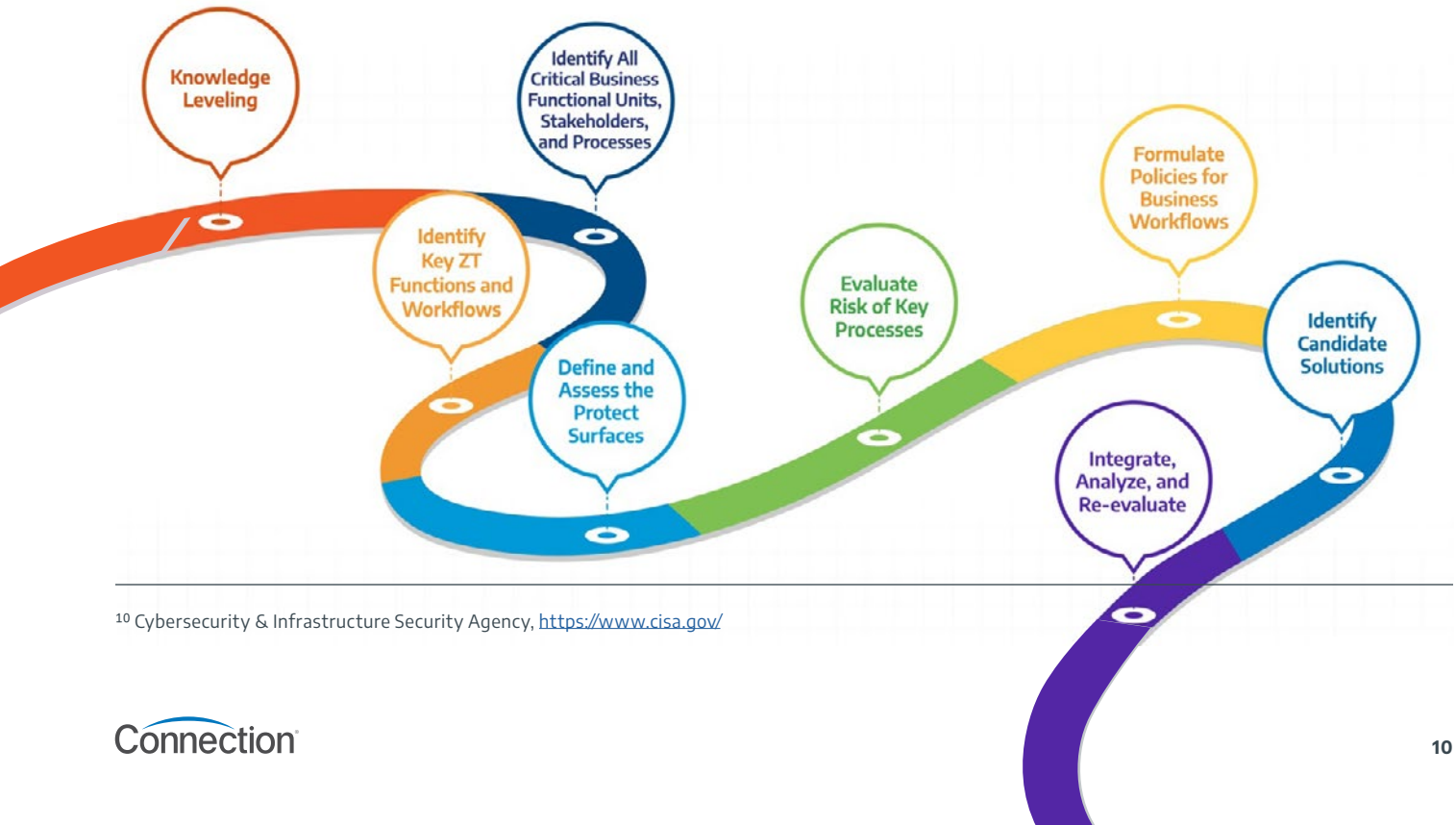
Advancing Zero Trust Maturity

Let's say, for example, that your organization is running a cloud-native application on AWS.

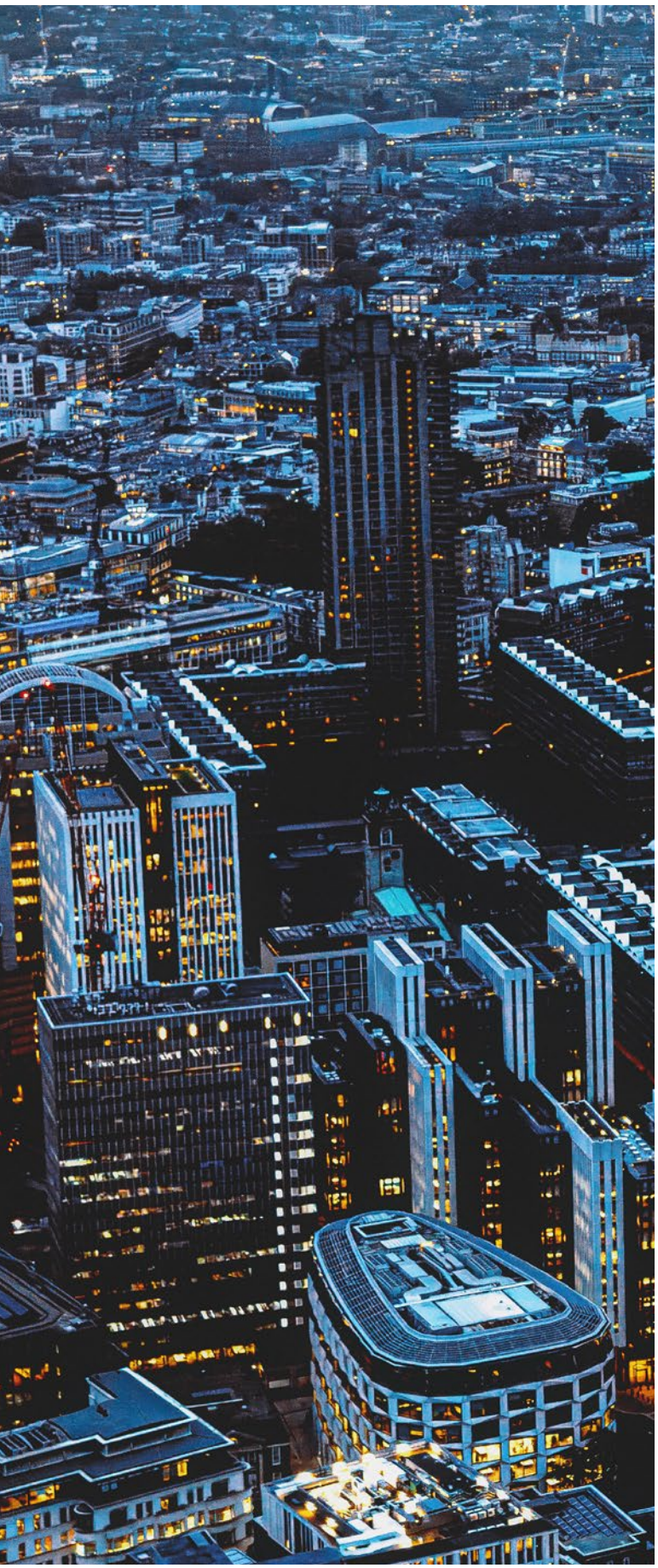
Making progress within the "identity" pillar might include moving from manual access provisioning and deprovisioning for this app (traditional) to beginning to automate identity-related policy enforcement (initial). To further your Zero Trust maturity, you could apply automated lifecycle management controls that are consistent across this application and a number of others that you're running (advanced). Optimizing Zero Trust maturity could include fully automating just-in-time identity lifecycle management, adding dynamic policy enforcement with automated reporting, and collecting telemetry data that allows for comprehensive visibility across this application and all others in your environment.

The more mature your organization is, the more you'll be able to correlate events across the five pillars. This way, security teams can understand how they're related across the attack lifecycle—which might begin with a compromised identity on a single device and then move across the network to target sensitive data in your cloud-native app running on AWS.

Zero Trust Roadmap[10]



[10] Cybersecurity & Infrastructure Security Agency, https://www.cisa.gov/



Step 3: Identify the Zero Trust adoption or migration strategy that will work best for your individual organization.

Unless you are building a new architecture from the ground up, it will usually make the most sense to work incrementally. This means implementing Zero Trust architecture components one by one, while continuing to operate in a hybrid perimeter-based/Zero Trust environment. With this approach, you will make gradual progress on your ongoing modernization initiatives.

Steps to take in an incremental approach:

1. Start by identifying the areas of greatest cyber and business risk. Make changes here first, to protect your highest-value data assets, and move on sequentially from there.

2. Carefully examine all of the assets, users, workflows, and data exchanges within your organization. This will enable you to map the resources that you need to protect. Once you understand how people use these resources, you can build out the policies you'll need to protect them.

3. Prioritize projects on the basis of business risk and opportunity. Which will make the biggest impact on your overall security posture? Which will be the easiest to complete quickly? Which will be the least disruptive for end users? Asking questions like these will empower your team to make strategic decisions.

Step 4: Evaluate technology solutions to see which ones best match your business processes and current IT ecosystem.

This will require introspection as well as an analysis of what's on the market.

Questions to ask include the following:

- Does our company permit the use of employee-owned devices? If so, will this solution work with your existing bring your own device (BYOD) policy?
- Does this solution work within the public cloud or clouds where we have built out our infrastructure? Can it also govern access to SaaS apps (if we are using them)? Can it work for on-premises assets as well (if we have them)?
- Does this solution support the collection of logs? Does it integrate with the platform or solution we use for access decision-making?
- Does the solution support all the applications, services, and protocols in use within our environment?
- Is the solution a good fit for our employees' ways of working? Would additional training be required prior to implementation?

Step 5: Implement the initial deployment and monitor its performance.

Once you are satisfied with the success of your project, you can build upon this by taking the next steps toward Zero Trust maturity.

Zero Trust in Multi-cloud Environments

By design, Zero Trust is intended for use in modern IT ecosystems, which almost always include components from one or more cloud providers. Zero Trust is a natural fit for multi-cloud environments. That said, building and enforcing consistent policies across diverse types of devices, users, and locations can be challenging, and relying on multiple cloud providers increases the complexity and diversity of your environment.

Depending on your vertical, business objectives, and compliance requirements, your individual organization's strategy will be different from everyone else's. It's important to take these differences into account when selecting solutions and developing an implementation strategy.

Building a strong multicloud identity architecture is very important. Individual users' devices need to be able to connect to your internal network, to cloud resources, and (in many cases) to other remote assets. A solution like SASE, SSE, or SD-WAN can enable this connectivity while supporting granular policy enforcement. A multicloud network access control (NAC) solution that was purpose-built to enforce Zero Trust can make intelligent authentication decision-making possible even across very diverse environments.

Don't forget about cloud vendor-provided solutions.

Public cloud providers like AWS, Microsoft, and Google offer native tools that can be leveraged to analyze, improve, and maintain your cloud security posture. In many cases, leveraging these solutions makes good business sense. They can be both cost-efficient and highly capable.

The Value of Working with a Trusted Partner

Many of the architectural design decisions that must be made when implementing Zero Trust are complex. The right technology partner will be well versed in all of the technology products, services, and solutions available on the market today, so they'll have a keen sense of which ones are best for your business.

Expert tip:

Look for a partner who is well versed in integrating across multiple public clouds and platforms.

Cost control can be an issue in multicloud environments: using vendor-provided solutions can be less expensive but may make it more difficult to maintain consistent controls across different platforms or infrastructures. Figuring out the best strategy may require cost-benefit analysis as well as a deep understanding of your IT environment.

The right partner can help you with this decision-making. They should have extensive partnerships with multiple security solution vendors, so they'll be able to help you see past individual vendor claims to discover which solutions are truly the best fit for your needs. They may also be able to secure advantaged pricing on your behalf, since they work with multiple vendors at the same time.

Look for a vendor that can fill in in a one-time consulting engagement if needed, but who also has the expertise to deliver managed services over the long haul. This way, you can be confident that you won't encounter excessive administrative burden, and that you'll be able to gain full value from the tools and solutions you select.

Meet Connection

To safeguard organizations against mounting cyber risks, implementing a Zero Trust architecture is vitally important. But it's also complex. From understanding Zero Trust frameworks, to choosing technologies, to building out an implementation strategy, advancing your Zero Trust maturity can be a long-term project with many moving parts.

Teaming up with the right service and solution can make progress toward Zero Trust both easier and more affordable. Over the longer term, your team can have confidence that you're mitigating some of the biggest (and potentially most expensive) risks that your business faces.

Connection, a Fortune 1000 company, calms the confusion of IT by delivering customers industry-leading technology solutions to enhance growth, elevate productivity, and empower innovation. Dedicated specialists focused on exceptional service customize offerings tailored to the unique needs of the customer. Connection offers expertise across multiple technology areas, delivering solutions to customers in over 174 countries.

Our strategic partnerships with companies like Microsoft, AWS, HP, Intel, Cisco, Dell, and VMware make it easy for our customers to find the solutions they need to advance their Zero Trust maturity.

How Connection Can Help

Connection is your partner for Zero Trust implementation. From hardware and software to consulting and customized solutions, we're leading the way in areas critical to success with Zero Trust and multicloud environments.

Explore our Resources
Modern Infrastructure
Cybersecurity Services

Reach out to one of our Connection experts today:

Contact Us
1.800.998.0067