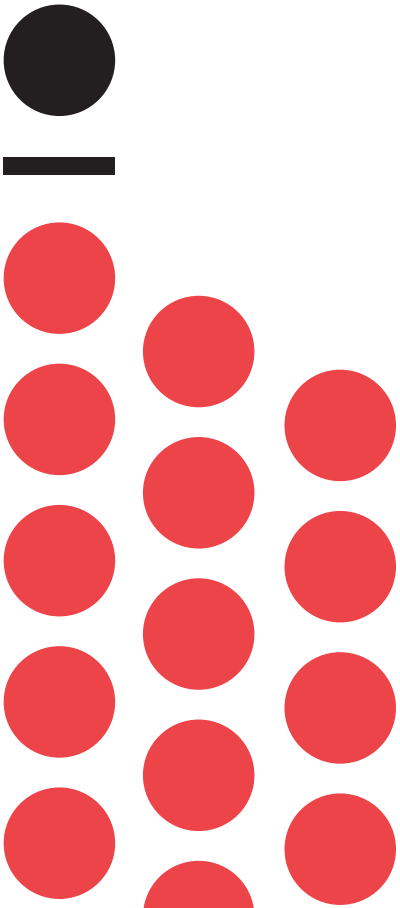
Adapting Zero-Trust Principles: Case Studies and Lessons from the Field



Written by:

ADVANCED CYBER SECURITY CENTER

C3 INTEGRATED SOLUTIONS

Table of Contents

Introduction

As cloud architectures, software-as-a-service, and distributed workforces have increasingly become the dominant reality of today's modern organization, the zero-trust security model has risen to prominence as the preferred security paradigm, even for the U.S. federal government.

As a result, there's an almost paralyzing number of publications and resources that describe zero-trust security principles and the components that make up a zero-trust architecture (ZTA). (A recent Google search on "zero-trust best practices" returned more than 77 million results.)

Perhaps not surprisingly, the majority of the resources available fall into two camps:

Vendor-neutral publications that tend to do a very good job of outlining the ideal zero-trust architecture in conceptual or academic terms, but struggle to demonstrate how practitioners can take such lofty generalities and ideals and apply them directly in a real-world implementation; and

Vendor-published white papers that typically hold a bias toward demonstrating how their particular security offering or category of offerings fits into a zero-trust architecture.

What the industry lacks is a diverse library of examples that showcases the adjustments and decisions practitioners make when applying zero trust to existing environments and use cases.

This report synthesizes the experiences of more than a dozen real-world practitioners representing a diverse cross section of organizations.

Organization Types

- Large multinationals
- Federal government agencies
- Small businesses

Industries

- Consulting
- Energy
- Finance
- Government
- Insurance
- Not-for-profit
- Technology

In this report, we highlight **three specific recommendations culled from discussions with nearly a dozen organizations implementing their versions of zero trust** and focus on how different those recommendations can look based on the idiosyncratic nature of any given organization's corporate philosophy, complexity, infrastructural ideology and mindset, and technologic or resource constraints.

We explore these recommendations through the experiences of a panel of technology leaders all implementing zero trust in their organizations. Most were members of the Advanced Cyber Security Center (ACSC), an organization of security leaders committed to strengthening cybersecurity defenses through collaboration. Given the sensitive nature of cybersecurity defense, the majority of our panelists elected to remain anonymous.

We hope that readers will be able to learn from the diverse experiences of IT and security leaders working to operationalize zero-trust principles within their organizations. By using concrete examples to demonstrate the practical considerations and common challenges associated with a transition to zero trust, we aim to demonstrate how seemingly rigid zero-trust recommendations can be adapted to support your own organization's journey to a zero-trust future.

What Is Zero-Trust?

"Zero-trust security models assume that an attacker is present in the environment and that an enterprise-owned environment is no different—or no more trustworthy—than any nonenterprise-owned environment.

In this new paradigm, an enterprise must assume no implicit trust and continually analyze and evaluate the risks to its assets and business functions and then enact protections to mitigate these risks.

In zero trust, these protections usually involve minimizing access to resources (such as data and compute resources and applications/services) to only those subjects and assets identified as needing access as well as continually authenticating and authorizing the identity and security posture of each access request."

—NIST Special Publication 800-207, "Zero-Trust Architecture

For more information:

- NIST Special Publication 800-207, "Zero-Trust Architecture" https://csrc.nist.gov/publications/detail/sp/800-207/final
- CISA Zero-Trust Maturity Model https://www.cisa.gov/zero-trust-maturity-model

Where to Start with Zero Trust

Regardless of your situation, the initial discovery process cannot be skipped and should lead most organizations to focus initial efforts on solidifying capabilities around identity, device, and asset management.

Equally important is ensuring that robust contextual signals and telemetry across the technology stack are aggregated for use by the system's policy engine(s).

Specifically, NIST SP 800-207 identifies six introductory steps for organizations transitioning to zero trust:

1. Identify Actors on the Enterprise
2. Identify Assets Owned by the Enterprise
3. Identify Key Processes and Evaluate Risks Associated with Executing Process
4. Formulate Policies for the ZTA Candidate
5. Identify Candidate Solutions
6. Initial Deployment and Monitoring

Our IT and security leaders focused in on the first three exploratory steps as critical to understanding gaps in capabilities around the Identity and Device pillars and found that the six steps should be completed roughly in that sequence to formulate a corporate zero-trust strategy.

A Journey Rather than a Destination

Zero-trust transformation is best understood as a journey—one that is likely to require years of concentrated effort, and in many cases, may never achieve full adoption. Some who may already realize that full adoption is not possible for their environment may reasonably ask then, why undertake the effort?

The reality is that there are immense security and operational benefits to transitional implementations of zero trust, including shrinking trust boundaries, gaining granular control over access requests, and increasing visibility into an organization's sprawling perimeter of users, devices, applications, and platforms. By moving your organization away from the traditional location-based security model (however incrementally) and toward a continuous and adaptive system of explicitly and automatically validating access controls, you will naturally, and in most cases, dramatically, improve your security posture.

With the exception of greenfield environments that can be built from the ground-up according to zero-trust principles, our panel of participants all recognized that, "Zero trust is a long-term goal deployed in multiple steps. Which steps and in what order varies based on corporate appetite for change, resource availability, technical and organizational structure, and authority."

Three Lessons for Implementing Zero Trust

The challenge in implementing zero trust is not in understanding what steps to take, but rather how to apply those steps to your organization.

In our panel, we not only had a wide variety of represented industries and company sizes, we also had differing levels of zero-trust maturity. Despite that, three foundational themes emerged from the reams of best-practice recommendations as the most critical to success regardless of size or industry.

1. Define your zero-trust perimeter

There are few (if any!) cases in the real world where organizations have the level of control needed to strictly apply zero-trust best practices across their entire environment. Clearly defining the edges of what can be tightly controlled and what cannot is critical to ensuring that those areas don't "bleed" into each other and compromise the integrity of your zero-trust architecture.

2. Use an incremental implementation strategy designed for organizational impact

What stood out in our panel was how differently organizations defined the journey. Some chose to implement individual zero-trust elements sequentially across their organization, while others implemented all zero-trust best practices at once, but to small groups at a time. In either case, an incremental approach can produce faster, more frequent "wins" that build organizational momentum.

3. Identify and sustain an internal evangelism strategy to assure long-term success

Finding the right evangelists and continuing to strengthen their commitment accomplishes two goals: First, this gains the support needed for the initial, often very disruptive zero-trust project, and second, this approach maintains zero trust long-term through continued best practices, reinforcement, and accountability.

While these themes may seem straightforward, we were struck both by how vehemently our panel emphasized them and how differently they were interpreted and deployed across separate (and in some cases, the same!) organizations. In the next few sections, we'll outline these themes and provide examples of how our panelists implemented them.

Define Your Zero-Trust Perimeter

In "Planning for a Zero-Trust Architecture: A Planning Guide for Federal Administrators," NIST admits that, while "[i]n an ideal zero-trust architecture, every unique operation would undergo authentication and authorization before the operation is performed...this level of granularity may not always [be] possible and other mitigating solutions…may be needed to detect and recover from unauthorized operations."

While security concerns and best practices might drive us to daydream of an ideal zero-trust architecture, the pragmatic reality is hindered by two core considerations: 1) the cost-benefit analysis as it relates to both hard dollars and business efficiency/velocity, and 2) the challenge of retroactively applying zero-trust principles to an existing estate.

In this section, we'll cover the first consideration. The second will be covered within the context of the next section on incremental implementation.

One important note: While we recognize that the use of "perimeter" in this context could be confusing, we use the term deliberately. In too many cases, organizations attempt to implement zero trust in half measures. In our panel's experience, however, zero trust works best when the zero-trust environment is treated as its own entity rather than a specially treated part of the existing infrastructure. As such, it requires as much planning and consideration about what falls within its boundaries (and how to treat what falls outside of it) as any other perimeter requires.

All Trust Isn't Equal

While an optimal scenario would result in an entire organization's infrastructure operating under zero-trust principles, the reality is that for many, such an endeavor is either prohibitively expensive (particularly for an existing operational environment), or would introduce unacceptable impediments to business velocity—or both. In addition, it's often simply not possible to fully adopt zero trust due to technological limitations.

Regardless of the reason, our panel urged their peers to think deliberately about which systems, data, processes, and business units/departments are determined or required to be in scope for your zero-trust initiative. Such deliberation need not be permanent—as you'll see in this first example, for most of our panelists, the zero-trust perimeter expanded over time—but in many cases, there were immutable reasons why certain parts of their organizations could not be part of the zero-trust architecture.

In the case of one Fortune 100 insurance company, regulatory pressures around payment card information (PCI) drove the adoption of zero-trust principles and the resulting scope of the zero-trust environment. The regulation dictated the minimum perimeter required for zero-trust transformation, and the team used that PCI perimeter as a contained pilot for zero trust before expanding to other parts of the business.

Regulatory-Dictated Perimeter

The "right" boundaries for zero trust will vary from organization to organization.

Similar to the PCI example in the call-out box, organizations that do business with the U.S. federal government, and particularly with the Department of Defense, are subject to certain

minimum standards of security to protect the government's sensitive information. Defense contractors are required to implement the security controls in NIST SP 800-171 to protect the confidentiality of Controlled Unclassified Information, which can be efficiently achieved by adopting a zero-trust architecture.

For paper co-author C3 Integrated Solutions, a security services firm specializing in implementing and managing NIST 800-171-compliant architectures for the Defense Industrial Base, the zero-trust perimeter is based on the level of responsibility the company accepts on behalf of its clients.

In the area of their business that is responsible for providing environments that meet regulatory-driven specifications, the only areas not included in their zero-trust design are those areas with technologic constraints such as lack of support for single sign-on or other integrations with the system's policy-enforcing components. In such cases, those system components are strictly cordoned off from the rest of the environment with compensating controls and restrictions on the types of data that can be processed or stored on such components.

One Global 500 energy company represented the approach of many of our panel members, with the head of cybersecurity innovation, technology, and architecture stating, "Base your zero-trust strategy, priorities, and initial perimeter on the current state of your highest risk environments."

Explains C3 CTO Ryan Heidorn, "If you have the ability to do so, 'rebuilding' on modern cloud architecture can enable rapid adoption of zero-trust principles and comes with a host of other security and IT management benefits."

However, some of C3's clients are large and serve multiple industries, of which the U.S. Government is just one. For many of these companies, limiting adoption of C3's zero-trust system to accommodate just the part of their business that services Department of Defense contracts makes both financial and business efficiency sense, while the rest of their business remains under existing architecture.

Risk-Based Perimeter

For the Global 500 energy company on the left, given the significant restrictions and costs associated with implementing zero trust across their global IT infrastructure, they sought to objectively assess where the costs of zero trust are justified by its benefits.

Security leaders took a two-pronged approach to defining the perimeter. The first step was to explicitly identify areas that needed to be "in scope" for zero trust. By reviewing their risk register, the team was able to identify areas of highest risk and evaluate how zero trust might dramatically reduce that risk. Presuming there wasn't a compelling reason not to (e.g. technological fit), those high-risk areas were prioritized for zero trust.

The next step was to explicitly identify areas that were "out of scope" for zero trust. In this case, they conducted a limited cost-benefit assessment to quickly identify areas where zero-trust benefits did not outweigh the costs and/or the restrictions that zero trust imposes. For this organization, customer service and field service fell into that category.

Opportunistic Perimeter

In a different example, a multinational technology company with a highly federated enterprise architecture had neither the interest nor corporate structure to enforce zero trust across all or even most aspects of the organization. Their governance structure is loose, and while there exists a centrally managed and tightly controlled core corporate network, the global complexity of the organization and its infrastructure, as well as a fast pace of acquisition activity, makes zero trust very difficult as an enforced corporate strategy.

That said, zero trust is a desired state, so this company has taken an opportunistic approach. As the senior manager of enterprise security architecture put it, "Zero trust can thrive in greenfield projects. [But for most situations, you need to] be opportunistic and focus on 'next-gen' projects to adhere to zero-trust principles."

Example: A business unit is standing up new lab space to test customer issues. Due to the purpose of that lab space, it cannot be locked down in the same way as the corporate network. That lab space is deemed "untrusted." For the core corporate network then, that lab space is treated in the same way that any outside system would be treated and is air-gapped from the core network.

The lab is not considered a part of the corporate network, despite being owned and operated by corporate employees.

At the corporate level, and for central systems, this "opportunistic" company has defined and adopted a set of zero-trust principles. For all other aspects of the business, their approach includes:

- **Globally publishing the zero-trust principles adopted for the core corporate network;**
- **Requiring new projects and modernization initiatives to adopt those zero-trust principles; and**
- **Defining three levels of trust (fully trusted, partially trusted, and untrusted) and assessing each system against those levels. That assessment dictates how and in what manner that system can interact with the core corporate network.**

Technologically Defined Perimeter

Of the inhibitors to zero-trust adoption, technology limitations are the most straightforward. One example highlighted by C3 was an external system such as a software-as-a-service (SaaS) application that doesn't support single sign-on (SSO) through its chosen identity provider (or worse, SaaS vendors that "upsell" SSO as a feature that is gated behind a more expensive license tier).

In C3's case, whenever faced with such a scenario, they make a risk determination based on the classification of the data that will be stored or processed within the system. For certain classifications of sensitive data (e.g., data in client environments), the company has a hard line—it will not use a system that doesn't support integrations with their identity provider. Example: If the system is just for general business data, they implement a variety of risk mitigation strategies, such as using long passwords, multi-factor authentication, IP restrictions, and ensuring that system permissions are incorporated into their role-based access model.

Key Takeaway

Be explicit about which areas of your business should strictly follow zero trust — and which will not.

In reality, defining the perimeter for each of our participants was not quite as clear cut as laid out above. Most of our participants deployed a combination of two or more of the above strategies.

Thematically, however, the advice was clear, regardless of which strategies make most sense for your organization: Think deliberately about how you define the scope of your initial zero-trust initiative(s). By clearly identifying your constraints and understanding your greatest areas of business risk and technology requirements, you'll be more likely to achieve success.

Use an Incremental Strategy Designed for Organizational Impact

By implementing incrementally, you get a chance to learn, adjust, and strengthen your zero-trust approach. You also gain visible milestones that help build momentum as you expand.

The second recommendation follows a similar vein—even if your ambitions for zero trust are expansive, our panel found that incremental implementation gave them the chance to learn, adjust, and strengthen their zero-trust implementation strategy. In particular implementing a strategy that had visible milestones helped build momentum as the team moved to successive phases of the project.

Beginning with Identity

For many of our panelists, identity was a logical place to start. Traditional location-based security focuses on defending the corporate network perimeter and relies heavily on the assumption that both sensitive corporate assets and the people that need to access them are centrally located and contained. Of course, this assumption bears little resemblance to today's modern, messy, and highly distributed businesses.

For one global insurance company, zero trust was a corporate strategy and would be deployed across its multiple global platforms. As a result, harmonizing identity needed to be the first step to controlling access. Once established, the team was able to create identity-based separation between its privileged access accounts and the remainder of the organization's users.

Explains the company's senior director of cybersecurity architecture, "We needed the ability to authenticate every person that has access to any of our systems. We adopted Azure Active Directory as our identity-management platform and migrated access to all our global platforms to that system."

C3's Heidorn also highlighted identity as a first step, commenting,

"Modern implementations of identity and access management are cloud-native, so some legacy systems could be a stumbling block. For example, some systems simply won't support integration with a cloud-native identity provider or will require intermediary steps like syncing identity, which adds additional complexity. By starting with identity, you may identify dependencies and complexities that require large-scale projects to work through or around."

Heidorn also advocated for Azure Active Directory, noting that it also provided an easier integration of user and device telemetry into the same cloud-native services and tools that can be used to create and enforce central policy.

The lead architect for zero trust at a global technology company also looked to the CISA model as a guide and underscored the importance not just of a centralized identity store, but also a complete understanding of devices and assets in the environment and robust telemetry across the technology stack.

He reinforced, "Telemetry is key—you need complete and deep visibility into all network

traffic. Without these…components, you will quickly discover that it is difficult or impossible to build a meaningful policy engine to authorize transactions within the system."

Incremental Progress through Successive Implementations

For some of our panelists, their approach to incremental implementation was a variation of defining the perimeter. In such cases, the organization will typically start with a small, very clearly defined pilot project and use the learnings and model from that to either extend the boundaries of the initial scope in successive projects or to create multiple zero-trust silos.

An example of the first is the insurance company referenced in the first section. After the implementation of zero trust to meet PCI-DSS compliance, the company took their learnings from that first project, iterated, and then extended the zero-trust model to other areas of the business unrelated to PCI data.

For an example of the second, we turn to a large federal agency with dozens of groups, all under a federal mandate to adopt zero-trust principles. For this agency, they elected to implement the CISA model in its entirety, group by group. So rather than attempting to harmonize identity across all agencies simultaneously, the agency picked the most technologically sophisticated and mature group as the prototype and sought to implement telemetry and all five pillars within that one group before moving on to the next.

By starting with the most technologically advanced organization rather than the weakest, they were able to focus in on unanticipated hiccups in the project without distraction. That experience helped them be better prepared for the less technically savvy agencies later.

Key Takeaway

When designing your implementation strategy, balance architectural ideals with technologic constraints, organizational realities, and the need for visible milestones.

Again, zero-trust leads will have to determine the best path forward for success in their organization, recognizing some of the inherent challenges with one approach over another. For example, the challenge around centralizing identity ranges based on the size and distribution of an organization. Where large organizations may struggle to manage and harmonize multiple identity stores across different geographies or business units, small organizations may struggle with siloed identities across various platforms.

Organizations coming from a network-centric security model will first need to confront real-world challenges around identity silos and lack of visibility or control into devices and endpoints to enable the development of a centralized policy engine at the heart of a zero-trust architecture. Needless to say, such a dramatic shift in primary focus has broad implications for how networks, systems, and applications are designed, and the organizational changes required to implement zero-trust principles are intense.

Incremental implementation is something of an obvious recommendation, but the success of such initiatives relies heavily on judiciously choosing which incremental approach has the highest likelihood of success for your organization.

THE IMPORTANCE OF GOVERNANCE

Regardless of how incremental implementation is broken up, our panel emphasized the importance of defining a governance model to oversee incremental implementations, especially over time, as initiatives could stretch for years. Such governance need not remain a wholly separate initiative but instead can leverage existing governance structures such as regularly scheduled architectural reviews and sign-off processes.

Internal Evangelism Will Drive Adoption & Accountability

Your goal should not just be to implement a zero-trust architecture, but also to sustain zero-trust principles over time through active management and accountability.

To be successful in zero trust, organizational buy-in needs to be obtained both for initial adoption and for long-term accountability. No matter how you approach zero trust at the outset, your goal should not just be to implement a zero-trust architecture, but also to sustain zero-trust principles over time through active management and accountability.

Associate Zero Trust with Business Objectives

First and foremost, messaging around zero trust has to resonate so that at least your stakeholders and participants understand and appreciate the need, even if they grumble about the details. Ideally, they embrace the path forward and evangelize it further. You'll want to actively identify influencers and potential naysayers and come up with a strategy to amplify positive feedback while proactively depositioning negative commentary.

Our panel highlighted two approaches, which can be used in tandem: the first ties zero trust into clear business goals, and the second emphasizes security concerns as a driver. In some cases, these can be one and the same.

For one of our not-for-profit members with government connections, the zero-trust initiative was tied to an immediate need: the ability to securely support remote work. This was particularly important as the organization had a variety of partners that needed to access the organization's resources without giving them access to the corporate network. The need to support working from home and provide a better environment for users helped fund and accelerate the initiative, enabling the organization to move their security perimeter to the cloud. However, they did a soft deployment; rather than force an install on any user, they focused on gaining buy-in from both executives and employees through a series of roadshows to educate on both the personal and organizational benefits of the move.

For one national corporation, there was a widely accepted business imperative around cloud transformation. As an organization-wide initiative, the cloud transformation initiative provided a golden opportunity to strengthen security during the architectural redesign. In addition, regulatory pressures around security were driving a greater need for more visibility and control for parts of the organization.

In this case, this two-pronged messaging provided the ammunition needed to shoot down any objections because they were tied not just to immutable regulatory requirements, but also to an initiative that represented the future of the organization.

At C3, security is core to the company's value proposition, with a core company value of "Practice Security First." In this case, company leadership has driven adoption, and has explicitly indicated to employees that all other business goals—including profitability—are subservient to maintaining a security-centric culture and environment. The cost of adopting zero-trust technologies was a concern, but leadership determined that the improved security posture from adopting modern security best practices, coupled with the value of enhancing the user experience and enabling and securing modern work scenarios such as working from home, made the effort worthwhile. With leadership on board and communicating the messaging, the rest of the organization followed.

Operationalize Accountability for Long-Term Success

In that last example, it's easy to see how zero trust will be maintained over time. But for companies that don't have full organizational buy-in, the long-term success of a zero-trust environment is entirely dependent on the accountability structure. Our panel warns zero-trust leaders to

> *consider what kind of support system will be needed after deployment for accountability and incremental improvements—and to build that structure in during implementation rather than after.*

This is particularly true for organizations that need to recruit and build their zero-trust champions. Consider the case of this international reinsurance company: Rather than focusing first on the deployment of any zero-trust principles or technologies, this company developed a series of 12 workshops for different areas of the business, for example, application development, infrastructure, operational technology, etc. By bringing in different groups for the workshops, they can customize the discussion and address specific needs, concerns, and pain points to gain buy-in. That workshop process will be used to build requirements, simultaneously recruiting advocates in influential areas of the business while ensuring that leaders fully understand the impact.

Key Takeaway

Develop the long-term support structure (e.g., organization, company-wide governance model, accountability, and talent) as part of the implementation process.

Consider questions such as:

- If you're engaging with experts as part of implementation, who maintains the internal ownership, and how do you build internal expertise?
- Who is on the steering committee; how engaged are they, and how influential are they across one or more audiences?
- How do you sustain and encourage engagement after implementation? (One tip offered by the panel: Continue to tie zero trust back to other desired business objectives to increase the weight of the zero-trust initiative.)

Strong evangelism is all the more critical for organizations whose zero-trust implementation journey is likely to span years. For some organizations, the first zero-trust initiatives might be treated as a special project with a dedicated task force, while successive projects might become more standardized as early learnings are translated into a sort of blueprint. In such cases, zero trust becomes part of the fabric of the existing governance structure, capitalizing on preexisting processes and forums to drive progress.

Remember to keep firmly in mind that zero trust is a journey, so you'll want to build in ways to reenergize the initiative over time.

Conclusion

Regardless of how each of our panel members tackled zero trust, there was still a lot of discussion around how to define and implement zero trust in their organizations. Across all of our discussions was a feeling of still needing to "figure things out," coupled with a general recognition that idiosyncratic differences from company to company necessitates modifications even to the most universal of recommendations.

We hope this paper has helped clarify how differently other organizations are executing against three universal recommendations and provided actionable next steps to consider. To recap our three recommendations:

Define your zero-trust perimeter. Whether you limit that perimeter based on technologic constraints, organizational structure, corporate priorities, or something else entirely, remember that thinking of zero trust as a true perimeter is critical to long-term success.

Implement incrementally, ideally prioritized for impact. Not only is zero trust a long journey for most organizations, it can also be a windy one. To maintain momentum and buy-in, carefully consider how to break up zero trust so that early wins will gain or maintain the support of key stakeholders.

Evangelize early and often. By recruiting respected personnel to be your evangelists from the early planning stages, you can anticipate and address potential roadblocks while creating a long-lasting structure that will help you maintain accountability long-term. Waiting until your first implementation nears completion is way too late.

Appendix

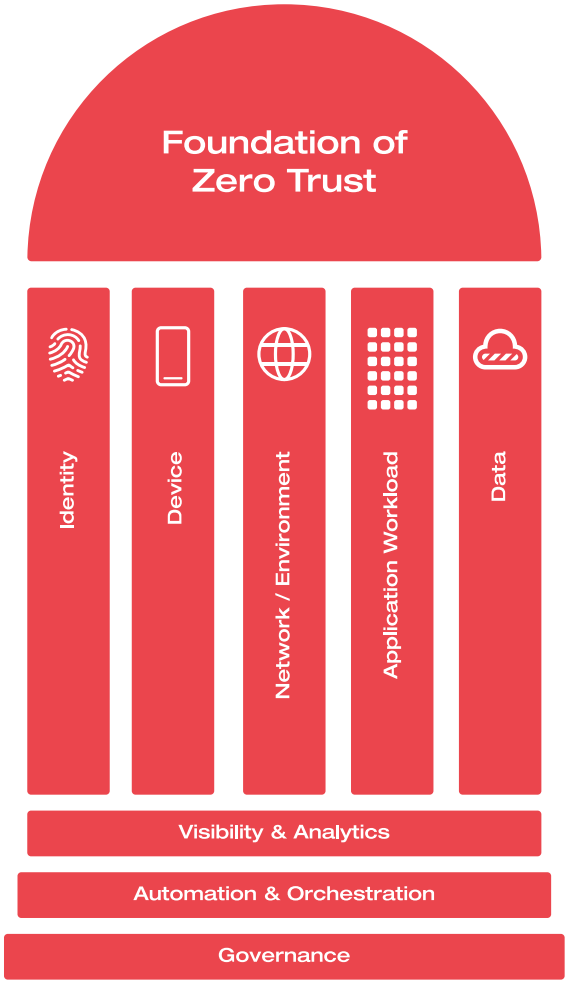
Zero Trust: A Quick Overview

In practice, adopting a zero-trust strategy can take various forms, from redesigning and retrofitting existing architecture to migrating to a new system architecture or components. The NIST white paper, "Planning for a Zero-Trust Architecture: A Planning Guide for Federal Administrators," asserts that "[m]oving to a zero-trust architecture will likely never start from scratch."

Tenets of Zero Trust

NIST SP 800-207, "Zero-Trust Architecture," lays out seven tenets of zero trust, clarifying that "these tenets are the ideal goal, though it must be acknowledged that not all tenets may be fully implemented in their purest form for a given strategy."

1. All data sources and computing services are considered resources.
2. All communication is secured regardless of network location.
3. Access to individual enterprise resources is granted on a per-session basis.
4. Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes.
5. The enterprise monitors and measures the integrity and security posture of all owned and associated assets.
6. All resource authentication and authorization are dynamic and strictly enforced before access is allowed.
7. The enterprise collects as much information as possible about the current state of assets, network infrastructure, and communications and uses it to improve its security posture.



The Role of Identity and Telemetry in Zero Trust

Unlike in a network-centric model, which broadly grants access within the protected boundary of a corporate network, zero trust seeks to verify (authenticate, authorize, encrypt) every request, using telemetry and contextual signals to make policy- and risk-based access control decisions. Effectively, because it focuses on individual resources such as user identities and devices, identity becomes the new security perimeter.

While the CISA Zero-Trust Maturity Model benchmarks zero-trust implementations across five "pillars" (Identity, Device, Network/ Environment, Application Workload, and Data), others, such as Microsoft CISO Bret Arsenault, advocate for a distilled version that focuses on the first two pillars of the CISA model and the foundation that underpins them (telemetry across the technology stack, or "visibility and analytics").

Arsenault's approach was succinctly captured in this fireside chat at RSA 2021, where he explained, "We simplified [zero trust] down to… healthy device, strong identity, and persistent telemetry."

About the Authors

John McKenna

John McKenna is the President and CISO Chair of the Advanced Cyber Security Center (ACSC), where he leads practice-sharing programs with members, including Zero Trust initiatives. John was previously the Global CISO for Liberty Mutual, overseeing their cloud migration journey and zero-trust deployment until his retirement in 2018.

Ryan Heidorn

Ryan Heidorn is the Chief Technology Officer at C3 Integrated Solutions, where he leads the technical direction and delivery of the company's compliance offerings for the U.S. Defense Industrial Base. Ryan teaches cybersecurity at Endicott College in Beverly, MA and serves as a Board Director for the National Defense Industrial Association (NDIA) New England chapter.

About the Organizations

Advanced Cyber Security Center

The Boston-based Advanced Cyber Security Center (ACSC) advances member cyber defense strategies through regional, national and global practice-sharing networks of industry leaders and provides professional opportunities for rising talent.

The ACSC was established in 2011 as a 501(c)3 organization and was the model for Information Sharing and Analysis Organizations (ISAOs) when Presidential Executive Order 13691 was implemented in 2015. ACSC members represent the financial services, healthcare, technology and other sectors, along with leading universities, the Federal Reserve Bank of Boston, and the Commonwealth of Massachusetts. To learn more about ACSC, visit https://www.acscenter.org/

C3 Integrated Solutions

C3 Integrated Solutions accelerates CMMC cybersecurity compliance by designing, implementing, and managing IT & cybersecurity solutions purpose-built for the U.S. Defense Industrial Base. C3 offers a wide-range of compliance-centric managed IT services—from targeted services customized to fit within a client's existing environment to the Steel Root Platform, a packaged and fully managed CMMC Platform purpose-built to meet compliance requirements.

A leading provider of Microsoft 365 GCC High and Azure Government, C3 is a leading AOS-G Partner, a CMMC Registered Provider Organization (RPO) and one of the few companies to successfully support the DIBCAC assessment of a CMMC Third-Party Assessment Organization (C3PAO). To learn more about C3, visit https://c3isit.com