

Planning a Zero Trust Initiative

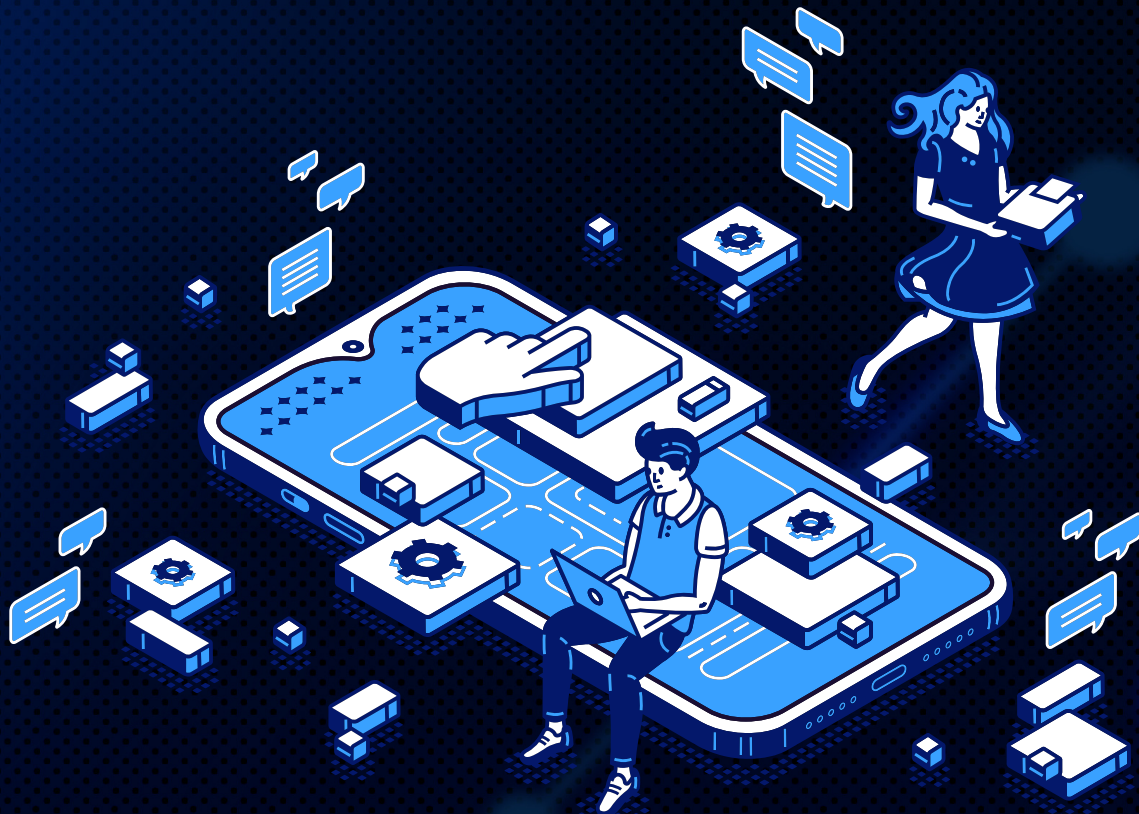
An unbiased guide for IT architects who are starting or supporting a Zero Trust initiative.

Andy Ruth, Managing Director
Jaylene Ruth, Director of Operations
Andrew Wilt, Chief Creative Officer



Start Here

i **This eBook is written for IT architects** who are starting or supporting a Zero Trust initiative. The guidance is framed on architectural best practice and process used for any major IT initiative. The six primary topics to get you started and heading in the right direction are business alignment and justification, creating a common vision and guiding principles, defining target and transitional states, creating a roadmap, mapping organizational skills for program execution, and finally, convincing leadership to buy in to a Zero Trust model .



Visit us at sustainableevolution.com

TABLE OF CONTENTS

01 **What is Zero Trust?**
An IT security strategy built on an asset and data-centric explicit trust model 4

02 **Why Should Leadership Care?**
Why Zero Trust is a critical business imperative, and how to get buy-in 5

03 **Defining Objectives**
Align your initiative with a business objective. 9

04 **Principles and Commandments**
A critical part of the envisioning process for an initiative 12

05 **Target State**
Describe what you want to do and why 15

06 **Create a Roadmap**
Lay out workstreams and define associated projects 18

07 **Create a Skills Matrix**
Innovation without action is just a good idea. You must know what skills you need and in what quantity. 24



What is Zero Trust?

Zero Trust is an IT security strategy to transform from a network-centric, implicit trust model to an assets and data-centric explicit trust model. That's the short answer.

Zero Trust is transformational. A Zero Trust initiative impacts people, process, and technology across the company and throughout the company's ecosystem of vendors, partners, and users.

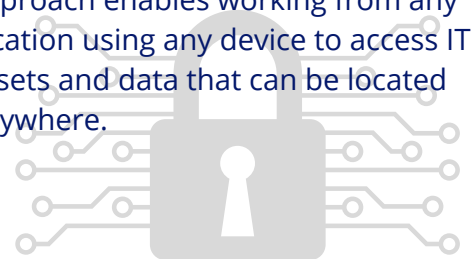
Like most transformational events, zero trust requires executive sponsorship, thought leadership, and a heavy dose of change management. You must create a common and clear vision for the future state zero-trust establishes.

Zero Trust updates traditional IT security architecture and operations to better support contemporary business models. Contemporary business can be described as:

- Every product having some or all digital components, whether the product is a smart refrigerator, car, or web application.
- People and applications (customers, users, IT assets, etc.) requiring access to IT assets across the Internet using personal and organization-owned devices. Access is required from anywhere on any end point rather than only granting access in a secure building with a secure network.

Traditional IT environments can be described as having a limited set of digital products with customers accessing the digital assets operated primarily inside of a strong network and infrastructure boundary. Users and IT assets in traditional IT environments are operated and managed inside of that secure network and infrastructure. The network and infrastructure are operated in known environments and are the primary source of security for the environment.

Zero Trust retrofits traditional IT security to shift the security model from controlling the state of the identity, device, and network to grant access to data, to a model that uses automated rules to determine the level of access granted based on the state of the identity, device, and network. This approach enables working from any location using any device to access IT assets and data that can be located anywhere.



Why Should Leadership care?

Gaining a Zero Trust posture is a critical business imperative, but using logic or scare tactics won't be effective in getting funding and sponsorship. If those tactics were effective, multifactor authentication would have been pervasive in the early 2000s. The arguments and ignorance haven't changed, but the business environment and technology have.

Likely, a better approach is:


- **Speak of the change to business and the business ecosystem that is causing the need for change.**
- **Talk about the upside of new revenue streams, lowered operational costs, and increased employee productivity.**

Unless you are a government contractor, every Zero Trust request must come from a business objective/value approach that also happens to provide Zero Trust capability.

Without Zero Trust, companies will struggle more and more to achieve their business objectives and stay solvent, but using a scare tactic-styled approach won't work. It's like telling a business executive that there is a boogeyman. Many people in leadership might be a bit like the Black Knight from Monty Python and the Holy Grail - a little overconfident in their staunch refusal of adopting Zero Trust.



Source: anotherfirerunner.com

- 
- **The IT boundary disappeared** – Remember? Remember when we had company-owned buildings with fences and guards and data centers and wired and wireless networks in those buildings with firewalls? New entrants to the workforce don't. We live in a cloud-based world with digital products operated in the cloud and there are no perimeters.
 - **Workforce and work location has moved** – The pandemic changed how we get jobs done. We don't just outsource or work remotely; we now work from anywhere using devices that might be company-owned and managed or might be our own machines. We cannot use firewall rules to control the environment.
 - **Compliance regulations are more stringent** – SOX, GDPR, CCPA, HIPAA, HL7, NIST-AAL, FedRAMP, CMMC, etc. Organizations can be fined, and executives jailed for not being compliant. Regulatory compliance is growing and many of the Zero Trust principles and guidance help with achieving compliance. Organizations are increasingly being held accountable for the protection of personal and sensitive data.
 - **Attacks are more sophisticated** – From better phishing to collection and collaboration using social media to AI algorithms and automation of attacks.
 - **Data breaches are increasing** – Not only is the frequency increasing, but the average cost of data breaches is outpacing inflation, seemingly doubling year-over-year for all forms of breach.

A Zero Trust model is a business imperative right now because it provides a more proactive approach to security, reduces the risk of data breaches, accommodates remote workforces, ensures compliance with regulations, and secures cloud environments. By adopting a Zero Trust model, organizations can significantly enhance their security posture and reduce the risk of cyber threats. But that isn't likely to work. Consider using business value with the side effect of moving towards Zero Trust. With a few successes and data to prove it, you can get sponsorship and funding.



Over the past few decades, we've shifted:

From having a data center in a building with wired and wireless networks inside of controlled buildings

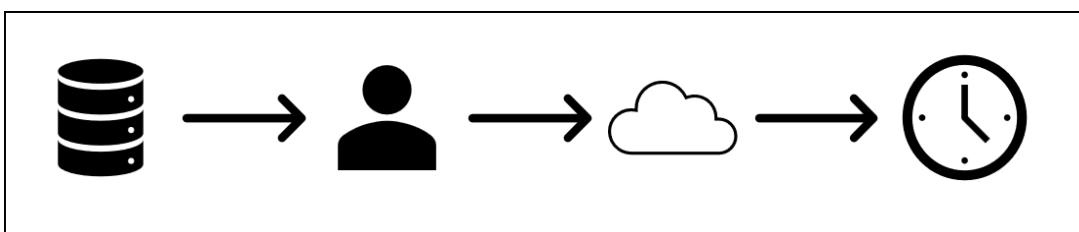


To employees working from almost anywhere using devices they might own to access data and services that could be hosted anywhere

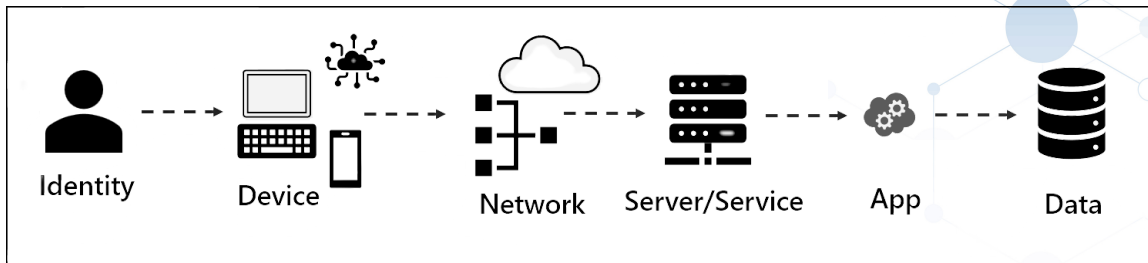
Add to that a much larger population of bad actors using more sophisticated tools that include social media, big data, and artificial intelligence to gain access, and, well, the good actors are losing. Building a bigger firewall with more constrictive rules and forcing employees to use stronger passwords that change all the time doesn't help.

With Zero Trust we rethink segmentation and borders, use stronger, more user-friendly authentication tools, and use automation everywhere. We shift from accepting single-point authentication and giving access to a large portion of our data and resources to using time-boxed verification where every point of integration requires identity verification. As an example, I can use my phone to access my bank account. When I do, I provide a password and then must enter an n-digit code into my phone to gain access. Maybe, instead of a password, my phone uses facial recognition and sends the code. Easier for me, and harder for bad actors to break the multi-factor authentication.

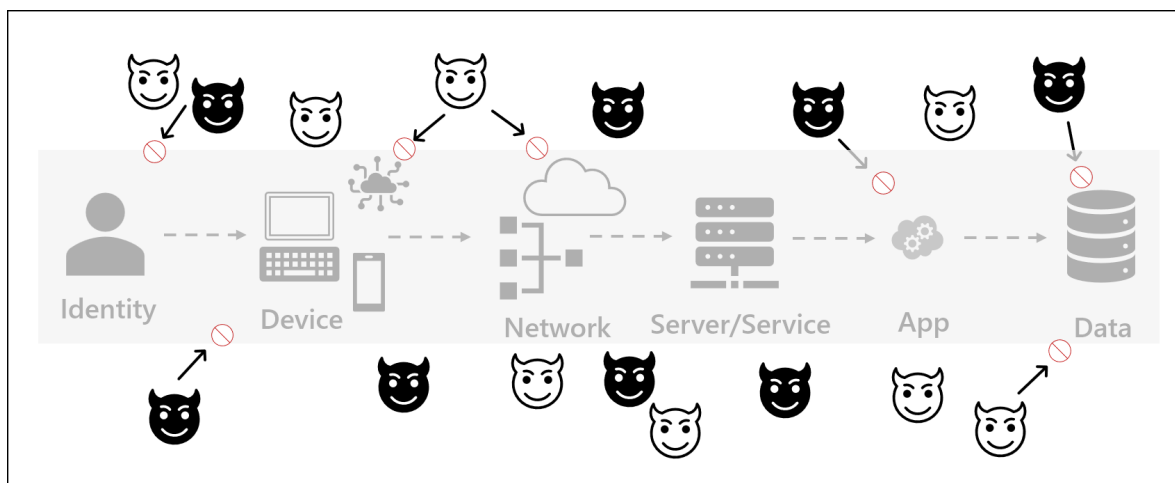
To understand that last statement, we must think about the goal of IT, the typical workflow, and the goal of IT security. In its simplest form, the goal of IT in a business is to get the right data to the right identity in the right location at the right time:



An example of the journey or interaction taken is that an identity uses a device to traverse a network to reach a server running an application to access data:



The job of security is to stop bad actors from completing that journey or any unwanted interactions at any point of the journey:



With Zero Trust, we define the metadata or attributes we want to base decisions on for each portion or point of the interaction. Then, we use an automated rules engine to determine if and what access should be granted based on the state of the combined attributes for the different portions of the journey. For example, if an employee is the identity and they are using their personal smartphone as the device across a non-encrypted public network to try and access email, then we can set automated rules to determine whether they can or not. If they attempt the same thing from the office, or with a company-managed device, or across an encrypted connection, the access might change. Each request is evaluated against the rules we put in place.

The attributes help us segment or group the points of the interaction in relevant ways for our organization. For example, identities might be segmented into administrative identities, user and partner identities, anonymous and consumer or customer identities. We can start with a simple segmentation and expand from there based on the defined attributes. From there we might use attributes to further distinguish what access is provided. So, if the identity is an admin identity, we might have different rules based on whether the identity is a human or a robot.

Zero Trust shifts us from trust always or trust but verify to always verify using stronger methods.

Defining Objectives



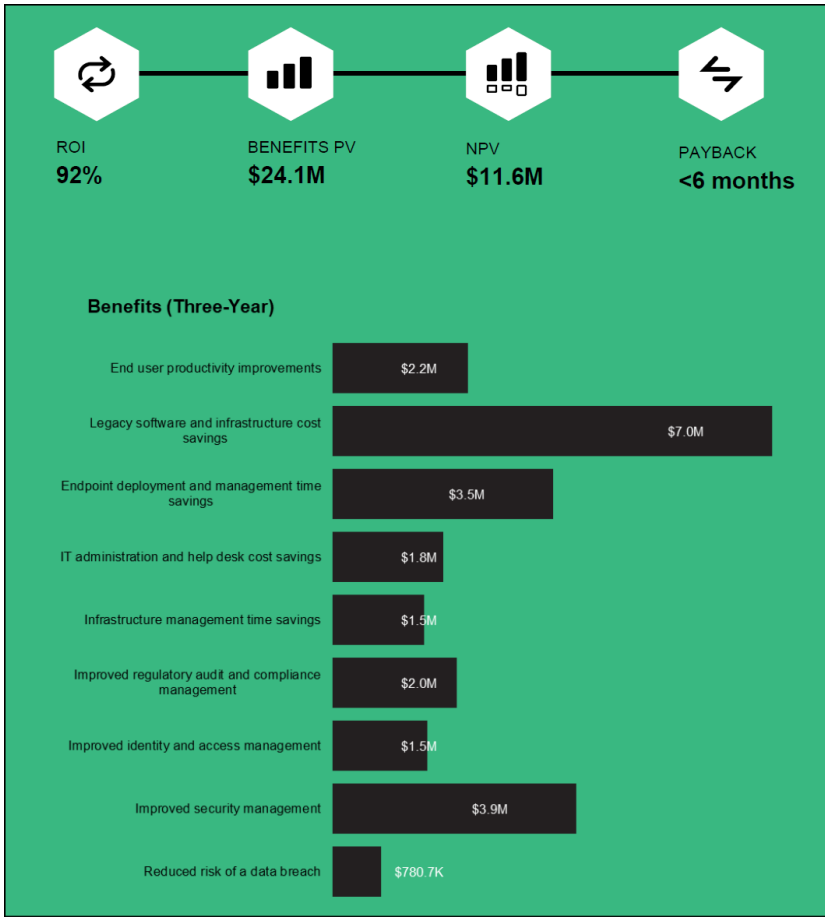
To start any big initiative, you must align with a business objective and be able to tell a story about how and when you plan to help achieve the objective.

So how do you justify spending money on security? You must be able to include some targeted timeline, as well as what indicators and measurements you plan to use to measure success. How do you measure not being taken down by a ransomware attack that didn't occur?

With the number of cyberattacks in the news, you can justify Zero Trust initiatives as part of the cost of doing business, but you still want and need to measure impact. "More secure" sucks as a goal or business objective and is tough to measure.

Since legacy applications and their associated servers likely require upgrades, there is an opportunity to reduce costs there. If self-service password reset and single sign-on are part of your identity management solutions, then end-user satisfaction, reduction of password fatigue, and removal of the requirement to involve the helpdesk or potentially a manager to reset a password might be measurable.


But the good news is that there are several Forrester Total Economic Impact reports that you can use as a model to define business objectives and goals. A Total Economic Impact report (TEI) is a 25–50 page report that describes solutions based on specific technologies or products. All the TEI reports use the same typical enterprise-sized environment, so they are consistent and provide good, comparative cost and value data.



Here are two screenshots from The Total Economic Impact™ Of Zero Trust Solutions From Microsoft. They show high-level benefits and the breakdown over time.

Total Benefits						
Ref.	Benefit	Year 1	Year 2	Year 3	Total	Present Value
Atr	End user productivity improvements	\$602,333	\$982,800	\$1,066,000	\$2,651,133	\$2,160,709
Btr	Legacy software and infrastructure cost savings	\$2,565,000	\$2,755,000	\$3,230,000	\$8,550,000	\$7,035,424
Ctr	Endpoint deployment and management time savings	\$1,405,915	\$1,420,165	\$1,434,414	\$4,260,494	\$3,529,491
Dtr	IT Administration and help desk cost savings	\$551,000	\$744,800	\$874,000	\$2,169,800	\$1,773,095
Etr	Infrastructure management time savings	\$233,280	\$794,880	\$794,880	\$1,823,040	\$1,466,203
Ftr	Improved regulatory audit and compliance management	\$708,750	\$850,500	\$850,500	\$2,409,750	\$1,986,204
Gtr	Improved identity and access management	\$405,000	\$648,000	\$810,000	\$1,863,000	\$1,512,284
Htr	Improved security management	\$1,406,250	\$1,577,813	\$1,755,675	\$4,739,738	\$3,901,451
Itr	Reduced risk of a security breach	\$233,722	\$333,178	\$389,832	\$956,731	\$780,714
	Total benefits (risk-adjusted)	\$8,111,250	\$10,107,135	\$11,205,301	\$29,423,686	\$24,145,575





From the top list, you can see that with a little thinking about how you position it, your security projects can be connected to:

- **Improving end-user productivity** – With the RIFs and belt-tightening most companies are doing, a project that helps the retained employees fill the gap for the missing resources is a great justification. Removing friction from password management can increase productivity and end user satisfaction.
- **Legacy software and infrastructure cost savings** – What company doesn't want to save money? But leadership has heard it before, and the CFO is likely to remember and cut your future budgets by the amounts you projected your initiative would save so take care.
- **Endpoint deployment and management** – This is tougher to align with business objectives so you might want to describe this one as removing a pain point for the HR onboarding team, or offer this one up as the project to be de-prioritized.

A few words of caution though. If leadership sees these numbers, the biggest financial bang will be the only thing they see and something like Reduced risk of a security breach might fall out. Be careful what you ask for and how. Also, as you think about your initiative, think about what you can do with little or no executive support, or at least with only your executive sponsor. Get those going and show success before presenting you whole plan. For example, start by requiring MFA for your global administrative accounts, or whatever level of administrative identity makes sense for your environment. The cost and risk are low, value is high, and the insights you gain are needed as you plan a larger rollout.

Regardless of your cloud service provider(s), you can use the Microsoft TEI studies to model your objectives and goals. The details can be used to define Key Performance indicators (KPIs) and (Objectives and Key Results) OKRs. The numbers provide some examples you can use to help the finance team know when you will burn money, when you will stop burning through the budget, and when you will reduce costs or start seeing value. Notice these are describing value for various business functions, but there is also information about risk reduction, etc. A simple web search for newer or more specific studies is likely to provide you with more specific insight into your environment, but as a tool to model goals and objectives, these provide a good head start.

Principles & Commandments

A time-honored tradition for architects is creating principles, for all employees, all IT staff, or, in the case of certain initiatives, for the people involved in the initiative. Principles are created as part of the envisioning process. Some key takeaways:

- Make sure your commandments are enforceable, endorsed by leadership, and if needed, documented by HR.
- Make sure your principles are abstract enough (like software patterns) to be predictably and repeatably used.
- Make sure there are just enough of them to accomplish their goal of guiding people without demoralizing them.



Principles

You've likely heard of principles but might not have heard the term commandments used.

Principles are high-level guidance meant to guide decisions that autonomous teams and individuals follow in making decisions. They will know what decision criteria to use when making their decision but might have reason to stray from the principle. Typically, there is an exception process for those that want to stray from the guidance.

Commandments

Commandments provide a set of rules that must be followed and cannot be broken. If a person does not follow a commandment, they might face severe consequences such as being terminated.



In the early 2000s, the Jericho Forum wrote 11 identity-focused commandments to describe identity management. For example, the first one is *the scope and level of protection should be specific and appropriate to the asset at risk*. If this idea is important enough to your organization that you might take disciplinary action against a person that did not follow the guidance, then it might be a commandment you adopt.

The Jericho Forum was an international group working to define and promote de-perimeterization. The Open Group maintains the Jericho commandments now. The commandments are still, and likely even more relevant in contemporary IT than they were when written. Worth a look as you start an initiative and adopt all or the specific ones you feel are relevant to your environment.





Classic Approach – Restrict everything to a 'secure' network



Zero Trust – Protect assets anywhere with central policy

Source: <https://www.microsoft.com/en-us/security/blog/2020/10/28/back-to-the-future-what-the-jericho-forum-taught-us-about-modern-security/>

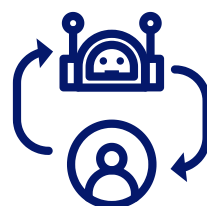


This principle might be adopted over time and there will be exceptions along the way. People know what their decision should be, but if context warrants not following *the principle*, they could.

The National Institute of Standards and Technology (NIST) has Zero Trust planning content (including principles), and a special publication (SP.800-207) that can help you as you define your principles. The Open Group Zero Trust principles also provide a good starting point for a Zero Trust initiative, and the guidance in the Security Forum is well done. Or, if you prefer, you can look at resources from SANS or any other IT security organization you follow as all are likely to have something.

Since you are likely going to use products and services as part of your initiative, review the BeyondCorp documentation from Google and the Zero Trust content from Microsoft. Both companies have three principles that are similar. These are not principles you would adopt but will help as you start building solutions. Both companies' internal teams use their principles when developing their products. That means the feature set that is available is built towards those principles.

We recommend limiting your principles to as few as possible. Keep in mind that you are writing them to help the IT staff in the org make decisions. A good target is ten to fifteen. Once they are created and endorsed, make sure they are well-published and visible throughout your organization. You can do this by sharing case studies of the proper application of your principles.



Target State



As part of getting funding or endorsement from leadership to move forward with a Zero Trust initiative, you must be able to describe what you want to do and why. Target and transitional state visions help with that and can be used to overcome resistance and hurdles. They're also needed to guide delivery and operational teams. The key takeaways:

- Make sure you are clear on the ultimate and stated target goals you want to achieve.
- Make sure your ask is sized to limit resistance, can start immediately (or even without approval), and quickly be accomplished to build trust and support.
- Don't sweat the details of the transitional state visions when you start – they'll turn into a wormhole that will stop you from getting started.



In TOGAF speak, a target state is a description of a future state you ultimately want to achieve. Transitional states are interim milestones you'll run projects and programs to achieve along the way. A favorite story/analogy my friend Jim Wilt likes to use involves elephants:

- How would five people in a dark room describe an elephant if each were touching a different portion of the animal? Very differently if one held a tail and the other a tusk.
- How do you eat an elephant? One bite at a time.

The target state describes the whole elephant and is broken into workstreams that make sense to that portion of a Zero Trust initiative. The transitional states describe the interim steps to the ultimate or aspirational goal. For example, for authentication of identities, I might set an aspirational goal of passwordless authentication. Along the way, a transitional goal might be multifactor authentication (MFA) for all internal user accounts. An immediate goal or proof-of-concept (POC) goal might be that all administrative accounts for one or more services must use MFA.

Applied to the three takeaways, how would you decide and be clear on whether you want the stated target to be MFA or passwordless? Consider the culture of the organization. Amazon and Google have 25-year visions and don't expect to see viable financial results for five-plus years. The new leadership at Twitter expect to see business impact within the quarter.

- If the organization has a habit of making decisions based on quarterly and annual results, MFA would be very aspirational, and focusing on administrative or privileged accounts might be a better target.
- If the organization has a habit of supporting multi-year projects, like replacing a CRM over three years, then perhaps setting a goal of passwordless works, and the POC can be administrative accounts with transitional state of all internal accounts being MFA within a fiscal year.



How would you size your ask to limit resistance and hurdles?

- If organizational culture encourages free thinking and the political clout of the CIO is strong, perhaps you initiate a POC for global admins that is positioned to provide awareness rather than requesting approval from any stakeholders. Pitch a plan for rollout to all internal users using the existing tools for starting new experiments or initiatives. Include self-service password reset as a carrot to minimize disruption and work with stakeholders to gain broader endorsement. At a minimum, that stakeholder list must include anyone associated with IT or physical security, HR, internal support, and operations.
- If organizational culture encourages a do-as-your-told-or-else mentality, perhaps you ask your CIO for approval to run an MFA experiment with global administrators that are part of their direct reports. Use the data for cost, time, user training required for adoption, support staff training estimations, and document challenges, and lessons learned. Partner with either sales or marketing to position the solution as part of an initiative to retain existing customers or gain new customers.

Why not sweat the details that need to be hashed out in order to be successful? You don't have enough information, and waiting to start until you have enough information is ill-advised given the current state of IT.

To get to the details, gather a team or collection of architects to define administrative and privileged accounts and set boundaries for what qualifies initially as administrative. If someone runs a Teams site that provides external identities access to content, is that privileged or administrative? If someone manages a mission-critical internal app like a CRM would that identity be part of the POC or the initial wave of users for the endorsed program? What about an interactive campus map employees can use to locate themselves and someone they are meeting with, the meeting location, and ETA for each attendee to arrive? The discussions will surface the information needed to create a roadmap that can be implemented.

Create a Roadmap



Goals, OKRs, KPIs? Check. Principles/tenets/axioms? Check. Target state and transitional states? Check. You based your resource request on them, so now it's time to create a roadmap, lay out workstreams, and start defining the associated projects.

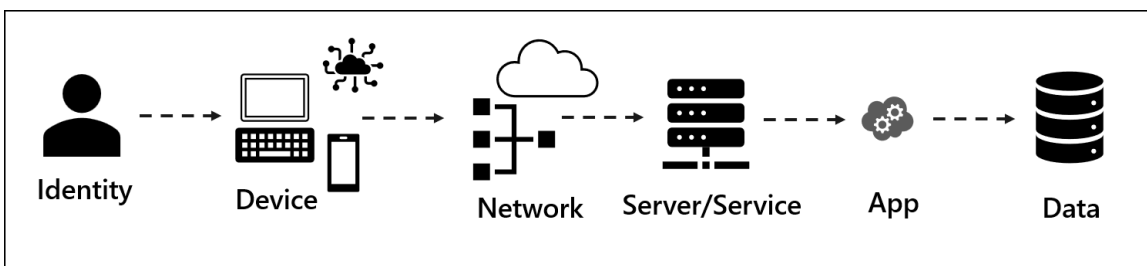
The order and prioritization of your roadmap will be based on your organization's business imperatives and current state. You'll likely start in the area where your security measures are most being tested. The roadmap we'll show here is based on a greenfield and represents what we think is an ideal approach to take. Consider using it to double-check your roadmap for completeness. Some key points:

- **Balance your workstream structure between the org structure/teams needed and the technology areas – hopefully they are aligned.**
- **Start on long timeline efforts quickly and try to break them into smaller, achievable chunks.**
- **Get some projects started immediately to show quick wins and value. They'll help you with endorsement and give you great insight into the cost, level of effort, and value measurement.**
- **Put target states out there for each workstream but think in agile sprints as you create the roadmap.**





Achieving a Zero Trust security posture requires transforming from a network-based, implicit trust model to assets and data-centric (or asset-centric), explicit trust security model. The customer journey from an identity making a request for data to it being fulfilled requires an **identity** to use a **device** or endpoint to traverse a **network** to reach **infrastructure** running an **app** that provides access to the **data**.



The same is true for the Internet of Things (IoT) space and it is part of Zero Trust, but likely is a separate workstream that we will not cover here.

To start laying out a roadmap, combine identity and devices into one workstream, network and infrastructure into another workstream, and finally data and apps into another workstream. This will (hopefully) align well with your org structure and ease the friction generated by having groups that don't work together often collaborating for Zero Trust. This approach also aligns with the pillars shown in the customer journey of the data requests. Add your target state and any transitional states you've defined. Determine what a minimum viable product (MVP) is for each workstream and add it. We've used MFA and passwordless to populate.

Workstream	Phase 0	Phase 1	Phase 2
Identity	Core admins MFA		Passwordless – all accounts
Device			
App			
Data			
Infrastructure			
Network			

For your core team, this is a first cut. Set the expectation that they refine it based on discovery.

First up for the core team is defining:

- How you want to segment and partition your pillars (identity, devices, network, infrastructure, apps, data).
- What states you want to validate for each defined grouping for each pillar.
- Is there a good/better/best to achieve the target state or transitional states that you can use to phase change?
- What rules you want to enforce for each combination of states that are part of the data fulfillment journey.
- How you want to catalog assets risk and value. For the levels assigned for risk and value, we recommend something simple like low/medium/high or -1/0/+1 unless there is a compelling reason to capture more detail.
- How to prioritize the collection of data and the rollout of rules. For agile environments, determine the smallest groupings and rules that will have a positive impact on security posture and organizational tacit knowledge and set that as your first milestone gate.

Now that you have an idea of what you want to do with your primary pillars you have an idea of the technology leg of the people/process/technology stool you are building. To get to the people and process efforts, you must think through the transformation.

To transform to data/asset-centric and explicit trust, your target state should include having a complete list of your IT assets uniquely defined so that you can create and enforce governance rules in an automated fashion.

Since you can't do everything at once, you'll want to assign business values to the assets so you know the exposure of business continuity and risk to the business upon exploit. That should help to prioritize your initiatives.

Use the data to help with the decision matrix for prioritizing projects and initiatives. The business value data is also valuable for defining security operations center (SOC) response priorities and escalation paths for informing stakeholders. To start laying out a roadmap for these areas, add workstreams for:

- Asset cataloging
- Governance
- Operations
- Skills management
- Automation



These should also fit well with your org structure. There is also a good chance that your operations teams already have the greatest experience with automation, so hopefully the automation workstream can be represented by the operations workstream.



Identify the efforts that are likely to take the longest time and add them to the first phase of your initiative. For example, if you don't have a catalog of applications and their supported business processes, that effort will take quite a while, and other projects will be dependent on the data that effort produces. It would be near the top of the list. For bigger efforts like this, also break them down using the MVP technique of the smallest grouping to drive positive impact. Then lay out the additional groupings to complete the collection.

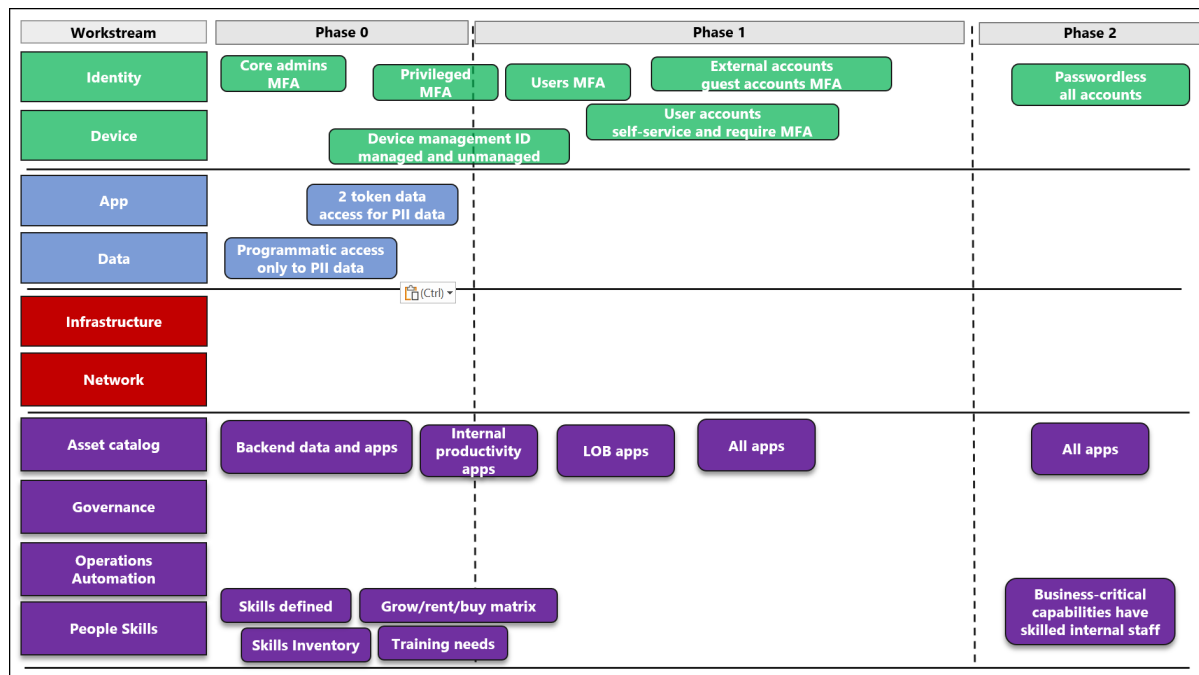
Workstream	Phase 0	Phase 1	Phase 2
Identity	Core admins MFA	Privileged MFA	External accounts guest accounts MFA
Device	Device management ID managed and unmanaged		User accounts self-service and require MFA
App			
Data			
Infrastructure			
Network			
Asset catalog			
Governance			
Operations Automation			
People Skills			

Workstream	Phase 0	Phase 1	Phase 2
Identity	Core admins MFA		Passwordless all accounts
Device			
App	2 token data access for PII data		
Data	Programmatic access only to PII data		
Infrastructure			
Network			
Asset catalog	Backend data and apps	Internal productivity apps	LOB apps
Governance			
Operations Automation			
People Skills	Skills defined		
	Skills Inventory		Business-critical capabilities have skilled internal staff

Next, add projects that have the lowest chance of failure, ease of operationalizing, and greatest impact on lowering risk. For example, configuring multifactor authentication (MFA) for core administrative roles has a low chance of failure as your core IT administrator teams will all be tech-savvy and won't need support or training. Start with an experiment, evolve to a POC, and grow to cover all the core administrative roles. Collect the data and publicize it with leadership and the entire technical community that will have a role in delivering capability.



With a strong roadmap, stakeholders will be able to better visualize what you are proposing and will see where (and when) they fit into the effort. The roadmap will also enable you to identify what teams you need to reach out to in order to form an extended team for the overall initiative and start a rhythm of war room meetings.



- The MFA project is likely to be a great success and with the right KPIs you can quantify the success.
- The data on cost and timelines will provide the information needed for planning the larger rollout.
- The feedback from the participants (your technical staff) is used to define processes and best practices for rolling out the capability to other groups.
- You'll have the data and internal subject matter experts (SMEs) needed for the internal training team to start creating and rolling out training content.
- You'll be able to tighten your roadmap based on dependencies between training people and rolling it out to the rest of the organization.

Key Points:

Leadership is focused on business, primarily driven by the top line, the overhead, and the bottom line. The architect keeps a focus on the customer, end-user experience, governance and compliance, and dealing with the way things are. Here's how a typical conversation with leadership might go:



Zero Trust Architect: A breach costs about \$5 million on average.

Leadership: And you want how much for your initiatives?? And we might still have a breach...

Zero Trust Architect: Our customers' data might be exposed so they might not do business with us.

Leadership: People are used to it. The shock isn't there and the cost to mitigate is lower than your project funding request. And you can't guarantee we won't get hacked.

Zero Trust Architect: Using cloud-based tools and processes will help bring our products to market exponentially quicker and cheaper.

Leadership: But what we already have works, and we are still in control.

Zero Trust Architect: Employees are bringing their own devices and working from home.

Leadership: That's temporary and then we'll be back to business as usual.

If an architect can position Zero Trust (better for the customer) as being a better business decision, leadership will buy in. Traditional security models are absolutely no use when addressing contemporary cyber threats on contemporary businesses:

- **IT is not overhead business capability** – Regardless of the business and industry, IT is part of every product and line of business (LOB). IT is part of the profit and loss (P&L) equation and when IT is attacked, the P&L and revenue stream is at risk.

Create a Skills Matrix



Zero trust requires innovation. Innovation without action is just a good idea so you need to know you have people skilled to take action. To be successful with any Zero Trust initiative, you must know what skills you need and in what quantity. You also must know what skills are vital to operating the business and use that insight to “rent” skills from consulting companies, “buy” skills by hiring someone or buying a company with the skills you need, or grow the skills internally. Some key points in creating a skills matrix:

- Use public certification objective domains and training curriculum learning objectives as a starting point for creating a skills matrix.
- Use a product feature list of the Zero Trust-related products you use to add specific product skills to your matrix.
- Use standards such as NIST AALs, FedRAMP, and CMMC for requirements to certify. These will describe tasks your people must be able to perform.
- Map your Zero Trust initiatives from design through sustained operation and support and validate the skills matrix covers the required skills.
- To identify who has the expertise, host meetings in groups of 10 with people that work in the same area. Ask who the top two go-to people are for each skill.
- Use an approach similar to rating business value and risk to determine which skills you’ll want to have on staff and which skills you can outsource.

There are a lot of certifications listed if you do a web search for Zero Trust certifications, and most come up as cybersecurity or cloud security certifications. Choose ones from organizations you are familiar with and respect. For example, suppose you trust Forrester and their view of Zero Trust aligns with your organization. In that case, you can use their training syllabus and certification objectives and write them as skills for your matrix. Some others: Zscaler has training and certification that aligns with their product feature set and Microsoft has the same if you are a Microsoft shop. Here's a screenshot with some of the objectives from GIAC you can use in your skills matrix:



Here's a screenshot of some of the objectives from GIAC:

Exam Certification Objectives & Outcome Statements

- Cloud Data Protection**
 The candidate will demonstrate an understanding of key management systems and the steps necessary to assess and secure them. The candidate will demonstrate familiarity with using encryption services to secure sensitive data stored in cloud platforms.
- Cloud Identity and Access Management**
 The candidate will demonstrate an understanding of cloud Identity and Access Management (IAM), its security concerns, and the steps necessary to secure IAM policies.
- Cloud Integration and Benchmarking**
 The candidate will demonstrate familiarity with the tools and services available to audit cloud environments for compliance with various benchmarks. The candidate will demonstrate familiarity with best practices for storing long-term credentials. The candidate will demonstrate an understanding of cloud end-user identity management solutions and cloud single sign-on solutions.
- Multicloud and Credential Management Fundamentals**
 The candidate will demonstrate an understanding of the security concerns of the current public cloud landscape. The candidate will demonstrate an understanding of instance metadata APIs, how they can be used in credential-based attacks, and how to assess their security.

	BeyondCorp Enterprise	BeyondCorp Enterprise Essentials
FEATURES	BeyondCorp Enterprise is our zero trust access solution for all of your applications.	The Essentials plan provides zero trust access to a core set of applications.
Context-aware access for SaaS and SAML-based apps	✓	✓
Context-aware access for Google Cloud apps, APIs, and VMs	✓	
Context-aware access for non-Google Cloud apps (apps hosted on other clouds or on-premises)	✓	
Malware and ransomware prevention	✓	✓
Phishing protection with real-time URL checks based on Google Safe Browsing	✓	✓

Product features take a little more work to add to a skills matrix but provide a good source for skills. For example, this screenshot is from Google and describes their BeyondCorp features. To rewrite these features as skills, the first one would read:

"Create SAML-based SaaS apps that are context-aware."

For NIST, FedRAMP, and CMMC cybersecurity standards, you can either review their standards directly, or you can review guidance published by product and service companies. For example, Azure AD guidance to achieve CMMC compliance lists the CMMC domain practice statements and objectives with associated Azure AD guidance to achieve the objectives. This assumes you are a Microsoft shop, but even if you are not, it might be easier to translate the objectives into the skills you need people to have.



After you have assembled what you feel is a good skills list, compare the list to your roadmap and the initiatives you are planning. Verify that the skills matrix represents all the skills needed through the lifecycle of each project, from design to daily operations. Fill any gaps in your skills matrix and then map the skills to the various projects or initiatives.

To determine whether you want each skill to exist in your organization or is a skill you can use consultants to deliver, use the business value and risk information you gather as you catalog your assets. Use that insight along with the portion of the lifecycle and the skill associated with it to determine if in-house or outsourcing is the better option. We recommend strategy and design remain in-house while implementation can be outsourced. For the operating portion of the lifecycle, use outsourcing for day-to-day operations but keep SOC in-house.

As you try to collect information about who in the organization has what skills and at what level, you can meet several challenges. You'll have people that understate their skills and those that overstate their skills. We recommend setting up in-person or virtual meetings with teams in groups of 10.

Have a list of skills you would expect the team to have expertise with and ask the group who the top one or two are for each skill listed in your skills matrix. Using this approach will remove most of the bias people introduce in rating themselves. This is also a task you can easily outsource to the product teams. Or you can use it as an opportunity to start meeting and building rapport with teams across the organization. One last point:

- **If your organization is heavily siloed, consider hosting the meetings yourself.**
- **If your organization is strongly matrixed, but uses communities to enable collaboration, consider outsourcing the effort.**



With the information collected, you should be able to create a strategy and projects to skill up for design, delivery, operation, and end-user support. This assumes you already have internal readiness working on end-user training.

As you create a strategy, if there are large, consolidated areas of skills gaps, consider using M&A (mergers & acquisitions) to quickly bring in the skills. However, for M&A to work you must have a strong M&A capability in your organization that has a proven track record for assimilating purchased companies into your organization.



Additional Resources

i Zero Trust for Architects course

Sustainable Evolution's Zero Trust for Architects course is designed to help you understand how to drive an initiative to gain a Zero Trust security posture for your IT environment. The training is based on the guidance available from government entities, standards groups, and cloud-based products and services companies.

This instructor-guided online course is fourteen classroom hours long. Our typical delivery is six weeks long and includes suggested reading as homework between each session. The course starts with planning a Zero Trust initiative and takes you through the process of planning for the key pillars of a Zero Trust framework.

We share our experience and strategies on how to assemble a team, scope out each pillar, and assess your current security state. We provide links to Zero Trust content for the major cloud service providers.

i COURSE OBJECTIVES

By the end of this course, you will be able to:

- Create a set of principles to guide a Zero Trust initiative.
- Assess your current Zero Trust maturity state.
- Use Forrester TEI reports to perform cost-benefit analysis on Zero Trust initiatives.
- Use causality mapping to roadmap Zero Trust initiatives to business objectives.
- Plan Zero Trust solutions to achieve boundary and segment restructuring.
- Determine the skills needed for core and extended teams on Zero Trust initiatives.
- Set a Zero Trust strategy for identities.
- Set a Zero Trust strategy for endpoints.
- Set a Zero Trust strategy for networks.
- Set a Zero Trust strategy for infrastructure.
- Set a Zero Trust strategy for applications.
- Set a Zero Trust strategy for data access and management.
- Automate security policy management.
- Use logged information to perform manual and automated intrusion detection and response.
- Create a change management plan for Zero Trust initiatives.
- Create a communications plan for projects and initiatives related to Zero Trust.

Sign up at sustainableevolution.com/training