SAVIYNT

The 3 Pillars of Zero Trust Identity:

Accelerate Your Move to Zero Trust

Zero Trust was a hot topic among security stakeholders even before the events of 2020 accelerated many organizations' progress towards the cloud. But today, Zero Trust is front-of-mind for an even larger number of CISOs. 72% of respondents to **a recent global survey** reported that they either plan to adopt a Zero Trust approach in the near future or have already begun implementing one. And 37% of cybersecurity leaders polled by **Deloitte** said that their organization had sped up its Zero Trust adoption efforts during the global COVID-19 pandemic.

With the publication of the **Executive Order on Improving the Nation's Cybersecurity** in May of 2021, the concept of Zero Trust gained additional attention. Federal agencies are now required to develop a plan for building out a Zero Trust Architecture, and the National Institute of Standards and Technologies (NIST) has published an abstract model of a **Zero Trust Logical Architecture** as well as several specific deployment examples.

Moving to Zero Trust brings significant and tangible benefits, including the most obvious one: a stronger cybersecurity posture for the entire organization. Zero Trust adoption can also simplify and streamline security operations, enhance defenders' visibility of the entire attack surface, and reduce the risk posed by insider threats — all while enabling users to have the right access to the right resources at the right time.

However, embracing Zero Trust is neither simple nor effortless. The process involves a learning curve, and despite what cybersecurity vendors may want you to believe, Zero Trust isn't a technology that you can just buy. Instead, you'll need to redefine your organization's entire approach to identity and security. You'll need to move from a mindset of implicit trust to an approach that involves the continuous re-evaluation of risk and a shift in focus — away from the network perimeter security layer and towards the identity security layer.

TABLE OF CONTENTS

In general, successful Zero Trust adoption involves three key aspects:

1

Building out a Zero Trust Identity **strategy**

2

Designing a new identity-based **architecture**

3

Shifting organizational cultures and **mindsets**

In this guide, we'll take a deeper dive into each of these three areas, while maintaining a practical focus on how to accelerate your progress towards Zero Trust maturity in the real world.

What is Zero Trust Identity?

Legacy perimeter-centric network security models are no longer adequate for today's use cases. Growing numbers of organizations are embracing digital transformation in order to gain access to the cloud's many benefits, which include scalability, efficiency and cost-effectiveness. This means that computing environments are evolving into borderless IT ecosystems.

In essence, Zero Trust is a concept that involves the practical application of identity and access management capabilities to perform continuous risk assessment every time resources are accessed within an environment. The goal is to use contextual identity information to inform and optimize access policies while enforcing the principle of least privilege. Zero Trust means granting access only for the right reasons, to the right entities, for the right amount of time. This enables a stronger security posture with no negative impact on productivity or business agility.

Completing your Zero Trust adoption won't happen in a few weeks or months. The process is complex, since it requires that your organization evolve its security and compliance posture, undertake cultural change, and build a cohesive identity architecture — one that's based not on a collection of point solutions but on a holistic strategy that builds upon identity as a foundation, and integrates all layers of the ecosystem. The full process demands long-term commitment, though you'll begin to realize some value from Zero Trust almost immediately.

1 Your Roadmap to Zero Trust Identity:
Creating a Zero Trust Identity Strategy

Making the move to Zero Trust demands considerable investment. Not only will your organization need to deploy identity-aware security solutions, but you'll also need to revisit your policies and business processes. In addition, you'll need to educate business and security leaders — as well as stakeholders across the organization — on the importance of the Zero Trust mindset. And you'll need to re-architect IT environments and applications so that they can fully benefit from the cloud.

Every organization's strategic plan for Zero Trust adoption will be unique. There's no one-size-fits-all formula that will work for everyone. Instead, you'll need to personalize your timeline and approach on the basis of your current security architecture and capabilities, technology environment, and business objectives. For most organizations, the full journey to Zero Trust will take 3 to 5 years, and will progress through multiple phases.

Begin with an Assessment
The first step is to gain a thorough understanding of the IT asset and identity ecosystem that spans your organization.

- ✓ **Where does mission-critical, sensitive, and regulated data reside?**
- ✓ **Which users have access to those assets?**
- ✓ **Among those users, how many have elevated privileges?**
- ✓ **Are these standing privileges?**

Most likely, you'll determine that most human and machine identities have excessive amounts of access, which is common in most organizational IT environments. If anything, the problem has gotten worse in recent years as cloud adoption has increased. One study of cloud entitlements found that more than 90% of identities regularly use fewer than 5% of the permissions that are granted to them.

More than 90% of identities regularly use fewer than 5% of the permissions that are granted to them

Next, you'll want to examine how access policies are administered and enforced. The least mature organizations are those that configure access and assign attributes manually, that enforce static security policies, and that lack integrated governance and privileged access management.

Organizations that are further along the road to Zero Trust will be cultivating: the ability to enforce least-privilege access automatically, the ability to continuously analyze access patterns and validate identities, and centralized visibility, identity management, and policy governance

Once you've centralized policy administration and governance, the next step is cleanup. Conduct an organization-wide discovery and analysis to determine where access is excessive. You'll then be able to limit and ultimately remove it.

The goal should be to implement security policies in a least-privilege manner.

Adopt a Zero Trust Maturity Model and Use it to Guide Decision-Making

We recommend that organizations follow a set of well-defined guidelines when evolving their Zero Trust capabilities and controls. The U.S. Department of Defense created a good example of this sort of roadmap in its **Zero Trust Reference Architecture**. The DoD's model establishes three levels of Zero Trust maturity. Organizations can advance from one to the next by implementing additional capabilities and controls. You can begin by working towards "baseline" adherence, then progress towards "intermediate," and finally achieve an "advanced" state of Zero Trust maturity.

Baseline

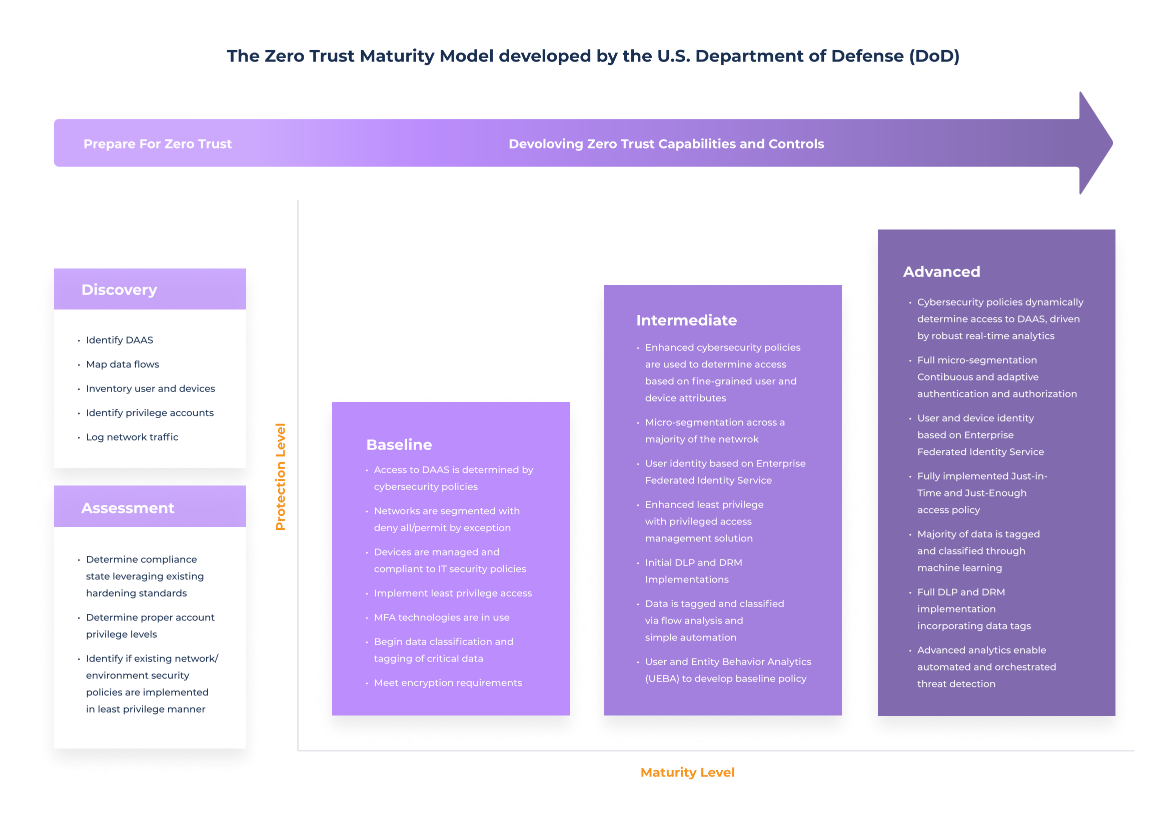
At this level, all network access takes place according to pre-established cybersecurity policies, and all devices are managed to ensure compliance with these policies. Multi-factor authentication (MFA) is in use, and least-privilege access policies are implemented. In addition, networks are segmented, with "deny all traffic" as the default, and resource access is permitted only after authentication.

Intermediate

Once an organization has progressed to this level, fine-grained user and device attributes are used to determine access policies. Least-privilege access is enhanced with the addition of a privileged access management (PAM) solution, and behavioral analytics are employed to fine-tune policy development. At this stage, micro-segmentation is enforced across a majority of the network, and data is tagged and classified for the initial implementation of a data loss prevention (DLP) solution.

Advanced

An organization has attained this state once it's able to enforce dynamic policies that determine access to resources on the basis of real-time analytics. Continuous and adaptive authentication and authorization will be in place, and Just-in-Time and Just-Enough access policies will have been implemented. Full micro-segmentation of the network will have been achieved, and advanced analytics will enable automated and orchestrated threat detection.



The Zero Trust Maturity Model developed by the U.S. Department of Defense (DoD)

Prepare For Zero Trust

Devoloving Zero Trust Capabilities and Controls

Discovery

- Identify DAAS
- Map data flows
- Inventory user and devices
- Identify privilege accounts
- Log network traffic

Assessment

- Determine compliance state leveraging existing hardening standards
- Determine proper account privilege levels
- Identify if existing network/ environment security policies are implemented in least privilege manner

Baseline

- Access to DAAS is determined by cybersecurity policies
- Networks are segmented with deny all/permit by exception
- Devices are managed and compliant to IT security policies
- Implement least privilege access
- MFA technologies are in use
- Begin data classification and tagging of critical data
- Meet encryption requirements

Intermediate

- Enhanced cybersecurity policies are used to determine access based on fine-grained user and device attributes
- Micro-segmentation across a majority of the netwrok
- User identity based on Enterprise Federated Identity Service
- Enhanced least privilege with privileged access management solution
- Initial DLP and DRM Implementations
- Data is tagged and classified via flow analysis and simple automation
- User and Entity Behavior Analytics (UEBA) to develop baseline policy

Advanced

- Cybersecurity policies dynamically determine access to DAAS, driven by robust real-time analytics
- Full micro-segmentation Contibuous and adaptive authentication and authorization
- User and device identity based on Enterprise Federated Identity Service
- Fully implemented Just-in-Time and Just-Enough access policy
- Majority of data is tagged and classified through machine learning
- Full DLP and DRM implementation incorporating data tags
- Advanced analytics enable automated and orchestrated threat detection

As organizations continue to implement emerging technologies and move growing numbers of applications and resources to the cloud, they'll need to revisit their processes, improve their workflows, and rethink their Zero Trust strategy continuously. In this sense, digital transformation is providing today's businesses with an unprecedented opportunity to modernize their approach to identity and security. Delaying Zero Trust adoption will only make the process more challenging and difficult.

> "Inaction is not an option. It's better to start small than not at all, and now is the best time to begin."
>
> Paul Mezzera,
> Vice President of Strategy, Saviynt

2 **Building Blocks:** The Basic Foundation of a Zero Trust Identity Architecture

When it comes to Zero Trust, moving from strategy to implementation — or theory to practice — will require you to deploy new identity-based solutions so that you can build out an identity-centric security architecture. You'll need a mechanism for enforcing policy administration and governance for each of the various cloud resources and services your organization leverages, including Software-as-a-Service (SaaS) and Infrastructure-as-a-Service (IaaS). In addition, you'll need access control and administration that's engineered to secure modern development pipelines. And you'll need a way of ensuring that your modernized identity solutions can integrate seamlessly with existing security and compliance tools. This means that solutions should be seamlessly interoperable.

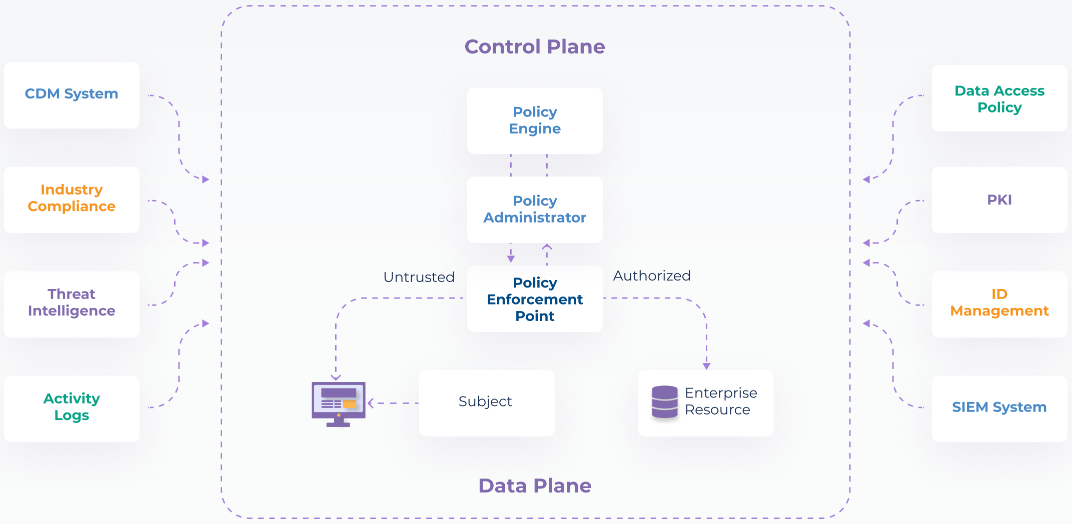
NIST's Zero Trust Architecture Model

Of course, creating this architecture is easier said than done. To make it easier for organizations to understand how to implement a Zero Trust-based approach to information security, NIST created its Zero Trust Logical Architecture.

Within this model, a Zero Trust Architecture should incorporate three core components. These are:

- **a policy engine**, which decides to grant, deny or revoke access to resources for all entities requesting it. The policy engine calculates trust scores or confidence levels to serve as a basis for each of these decisions.
- **a policy administrator**, which establishes and terminates the connection between an entity and a resource. The policy administrator relies on decisions made by the policy engine to determine whether to allow individual sessions to proceed. It generates authentication tokens or credentials for each session.
- **a policy enforcement point**, which enables and monitors ongoing connections between entities and enterprise resources.

NIST Abstract Zero Trust Logical Architecture



Within this architecture, all interactions are to be achieved in the most secure manner possible, which means that they need to be continuously reassessed. Each time access to a resource is granted, this is done for only one session, and for that resource alone. Every access request is evaluated dynamically based on organizational policies and a risk assessment. And each request is checked to ensure that the entity making the request should be granted access, that the system or device involved is behaving appropriately, and that the requested resource has the right characteristics.

To achieve the requisite degree of visibility and control, you'll need centralized access management as well as identity governance and privileged access management. It's critical that endpoint devices, computing resources, and networking and infrastructure components are all able to exchange information with one another. Plus, all components within the security architecture must work together with security analytics tools to inform policy decisions.

Core Capabilities of a Zero Trust Security Architecture

To obtain all the capabilities you need to achieve holistic visibility and control, you'll need multiple solutions with overlapping and tightly integrated capabilities. The policy engine must be able to interact with applications, security and access management solutions, and a broad array of resources across the IT ecosystem. This enables it to gather the intelligence that will inform the behavioral analytics it uses to assess and reassess risks on an ongoing basis.

The policy engine must have the following four core capabilities:

1. The solution must have an up-to-date inventory of all identities (human and machine) that need to access resources so that it can formulate consistent and accurate access policies across the whole environment. Thus, it must be able to **discover and correlate identities and entitlements**. This means it will need to know precisely which employees, contractors, third-party partners and vendors, devices, applications, and machine identities interact with one another in the environment, what roles each of them play, and what rights they should have.

2. The solution must be able to **provide user and device identity and contextual information**. It will supply this information to the access management and secure access service edge (SASE) solutions that enforce policies by allowing (or denying) access to resources in the environment.

3. It must **set least-privileged access policies** based on current usage and outlier analysis – and share these policies with the solutions that will enforce them.

4. It must be able to ingest logs and data from security tools and solutions in the environment. This will enable its **advanced analytics capabilities to respond to risky activities** quickly, accurately, and appropriately.

Building this architecture can be a complex process. It requires implementing multiple solutions that can gather intelligence across the IT ecosystem to inform SASE, access management, XDR and other security tools that enforce policies. Interconnectivity and an open, standards-based approach should be core principles in the design.

3 Shifting Organizational Cultures: Zero Trust Identity is a Mindset

Moving towards Zero Trust Identity requires the right strategy, as well as the creation of an identity and security architecture that's intelligent and grounded in interoperability. Equally important to success is gaining buy-in for the concept of Zero Trust across the entirety of the organization.

In today's data-dependent, digital-first world, every company is a technology company.

Even if your business doesn't create or sell digital products, technology is at the core of most modern business processes. Stakeholders from every business unit and department of the company must have seamless and reliable access to the right technology tools at the right time if they are to get their jobs done. And, of course, this is essential for the success of the business as a whole.

Adopting a Zero Trust mindset will enable security teams to better defend complex, dynamic, and cloud-based computing environments because it makes it possible to proactively prevent inappropriate resource access. But Zero Trust also provides seamless, just-in-time access to the tools that employees need for productivity, innovation, and business success. Embracing Zero Trust means adopting technologies, ways of working, and policies that support business agility while enhancing security. To achieve this end, business leaders, security practitioners, and stakeholders across the organization must work together in support of shared objectives.

It's often said that the most effective approaches to IT security are grounded in a multi-layered model encompassing people, processes, and technology. Zero Trust is no exception. Moving towards Zero Trust requires investing in the right technologies and designing an architecture that can extend robust security across an IT ecosystem that extends far beyond the "trusted internal zone" of a corporate network.

It also requires that people throughout the organization:

- Take information security seriously
- Grasp the foundational concepts within the Zero Trust approach
- Know where sensitive and confidential data resides and how to handle it
- Understand security policies, when they should be applied, and how to follow them consistently
- Contribute to building a more cyber resilient organization

Cultivating this mindset requires buy-in from executive leadership all the way down to identity and security practitioners. Members of the board and CISOs alike must believe that a Zero Trust approach will foster business agility, improve data protection, and mitigate real-world risks. And they must be willing to implement and participate in the policies and operational processes that support this approach.

Conclusion

In today's world, taking an identity-based approach to Zero Trust is growing in popularity for good reason. It will help your organization evolve its security and compliance posture to keep pace with changes in the threat landscape as well as advances in technology. This approach will also give your team better visibility into your IT assets and resources and how they're being used. And Zero Trust can enhance business agility and productivity.

These benefits are far-reaching, but the effort required to attain them is far reaching as well. You'll have to communicate well and may need to incorporate education and training to generate buy-in. You'll also need to move from implementing point solutions in piecemeal fashion to building a cohesive security strategy. And you'll need to build a security architecture with identity at its foundation, a holistic ecosystem where all layers are seamlessly integrated.

We've never said that the process was simple, but we do believe that the benefits are more than worthwhile. After all, Zero Trust is a journey, not a destination.

Moving to Zero Trust requires adopting identity as your security perimeter. Saviynt can help.

LEARN MORE