Everest Group®

Cyber without Perimeters: Starting Your Zero-trust Journey with Identity

Enterprise Guide for Identity-based Zero Trust

Kumar Avijit, Practice Director
Arjun Chauhan, Senior Analyst

Contents

Introduction

Zero-trust architecture has been gaining popularity in recent years due to its ability to solve cybersecurity problems. However, to realize a full zero-trust state, enterprises need to overcome several challenges and adopt a pragmatic approach with a clear roadmap to achieve success.

Imagine a situation where security teams are tasked with securing devices and users with poor visibility of the IT landscape and an inconsistent authorization process – how well do you think they will succeed? It becomes a case of the blind leading the blind, but this is exactly what is happening with many enterprises. Security teams that were initially battling shadow IT (using software, devices, and services without explicit permission from the IT team) are additionally burdened by the complexities of cloud, such as limited visibility in the cloud environment, today. Apart from these challenges, remote-/hybrid-working models have reduced the significance of perimeter-based security and compelled enterprises to rethink their strategies for device, user, applications, and data security.

Zero-trust implementations started off as a mere necessity for enterprises, but with the evolution of tools, frameworks, and accelerators, enterprises are looking to move from entry level zero-trust to advanced zero-trust state. Moreover, providers are also leveraging solutions, such as integrated security technologies and tools, to enable enterprises transition to an advanced zero-trust state. Zero trust can help enterprises limit a breach's blast radius, contain supply chain attacks, mitigate insider threats, protect the remote workforce, and facilitate the evolving regulatory compliance landscape.

In addition, governments worldwide are also emphasizing on zero trust and promoting its importance – in 2021, the US government released an executive order[1] that required federal agencies to advance toward zero-trust architecture by September 2024; in 2021, UK's NCSC agency released zero-trust architecture design principles[2]. It's evident from these examples that zero trust will soon become a well-recognized and vital security standard for industries worldwide.

In this viewpoint, we take a closer look at identity-based zero-trust approach and examine the key drivers behind its growing popularity and increased enterprise adoption.

1 Executive Order on Improving the Nation's Cybersecurity
2 Zero-trust architecture design principles

Rise of zero

The pandemic compelled people to work from home, which rendered enterprise investments in perimeter-based security defenses such as firewalls, VPN, and honeypots futile. With the redundancy of perimeter-based security approach, security teams and Chief Information Security Officers (CISOs) were put in a tight spot and clients were left with limited options. This facilitated the shift to a zero-trust architecture. Some clients confuse zero trust as a one-time technology upgrade or a security tool that can be procured. However, it is important to understand that zero trust is not a single technology solution, but a security framework driven by the core principle of **never trust, always verify**. Zero trust has been around for almost two decades, but it's the pandemic-driven adoption of hybrid workplace models that has brought them in the limelight.

There are several other factors that have contributed to the increased adoption of zero trust:

- **Digital transformation initiatives:** Transformation initiatives result in a tool sprawl and, in many cases, expanded digital footprints, which increases attack surfaces and heightens the risk to supply chain attacks. To tackle these issues, zero trust provides an overarching layer of security that restricts the adversaries in case of suspicious behavior. Additionally, large scale digital transformation initiatives, with zero trust at the core, enable enterprises to embed the critical principle of **security by design** early in their transformation journeys
- **Increased breach costs due to stricter compliances:** With rising breach costs and stricter compliances, enterprises worldwide are realizing the importance of data privacy and data handling. A well-implemented zero-trust architecture enables enterprises to adhere to multiple compliances by virtue of its principles of least privilege and continuous trust evaluation
- **Zero-day vulnerabilities:** Zero-day vulnerabilities are hard to mitigate due to the absence of patches in the initial phases. Employing a security strategy of well-integrated tools and technologies can preempt breaches and effectively reduce the blast radius

These factors have propelled clients to look beyond siloed tool approaches and adopt comprehensive security approach to mitigate risks across different business functions.

Enterprises looking to scale zero trust within their organizations should aim to integrate disparate cybersecurity solutions in a well-orchestrated manner to supplement the policy engine – the core element of zero-trust architecture. The policy engine forms the backbone of the entire zero-trust framework and validates if subjects (devices, applications, users, or anything that can request access to resources) can have complete/partial access to the requested resource (assets that enterprises want to protect such as workloads, applications, APIs, and databases). This validation is based on the inputs from tightly integrated tools such as threat feeds, security logs, network activity logs, and system logs.

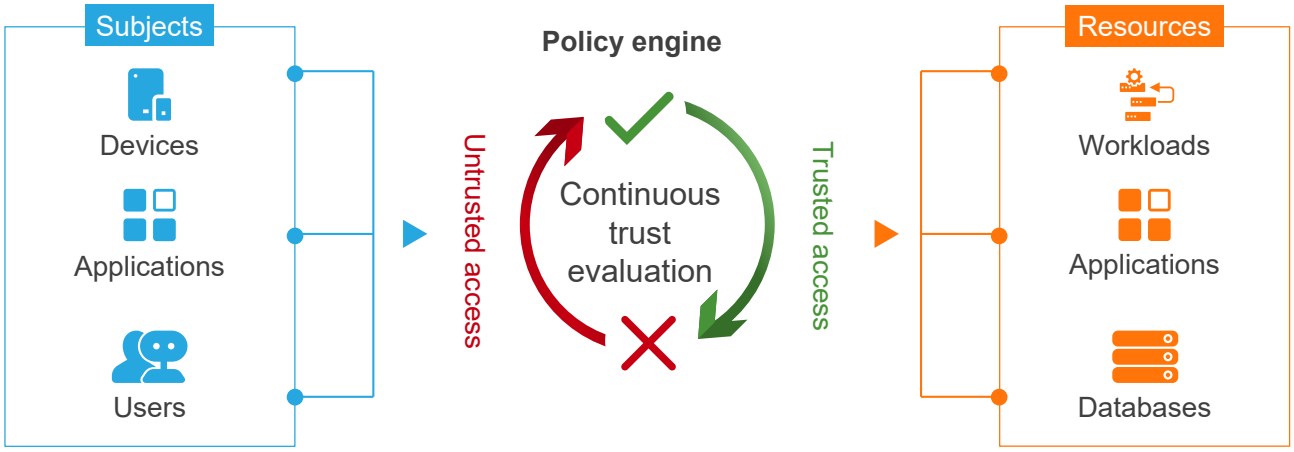
The elements of zero-trust architecture – subjects, resources, and the policy engine – are represented in Exhibit 1.

It is important to understand that zero trust is not a single technology solution, but a security framework driven by the core principle of **never trust, always verify**.

EXHIBIT 1

Elements of zero-trust architecture

Source: Everest Group (2023)

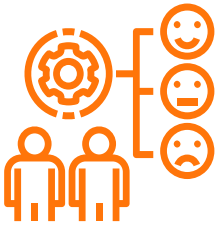


It is important to highlight that implementing zero trust can be a bit challenging in the beginning as it requires enterprises to work closely with the implementation partner and integrate all the authentication, authorization, and monitoring tools. Sometimes, the initial stages of implementation might involve modifying the existing toolset as part of vendor consolidation exercises that could result in a decline in the overall employee experience. Enterprises can adopt a phased approach for vendor consolidation and educate their employees on the nuances of an improved and efficient security posture. We believe that zero trust signifies a balance between employee experience, business enablement, and risk management. Enterprises can adopt zero-trust strategies and realize immense benefits from its offerings as is illustrated in the exhibit below.

EXHIBIT 2

Three balancing anchors for a successful zero-trust journey

Source: Everest Group (2023)



Employee experience
Improved employee experience with more automation and quick access (without passwords) to resources

Business enablement
Reduced effort in exacting security approvals for new business initiatives and securing access to partner ecosystems

Risk management
Significant reduction in security incidents and improved compliance management

Embarking on an identity-based zero-trust journey

Zero-trust implementation approaches

Since zero trust is neither a technology nor a single point solution, but a long-term journey of decoupling trust from each IT element, the idea of implementing it becomes very versatile. There are several ways to implement zero trust: each way eventually yields the same result; however, enterprises may prioritize certain aspects over the others. Choosing the right implementation technique needs evaluation of business requirements, focus areas, and investment capabilities.

The key objectives of zero trust are strong authentication, effective monitoring, and fine grain authorization. Enterprises can realize these objectives and opt for application-centric approaches that provide granular control on application access through API layer controls via technologies such as app servers and application/container micro-segmentation. Some other popular approaches to implement zero trust are:

- **Sophisticated identity:** Subjects' identity is the primary component of this approach, and factors such as device location, device status, user privileges, and behavior patterns alter the policy engine's overall confidence level
- **Network segmentation:** This approach has network access at its core, and telemetry data from endpoints and routers play a vital role in policy engine's overall confidence level
- **Overlay network:** This approach leverages software defined parameters as a broker service to grant or deny access, with continuous trust evaluation, to subjects and alters the confidence score of the policy engine

> Based on Everest Group's estimates, around 65% clients opt for identity-based zero-trust implementation approach and 35% opt for the overlay network approach.

For most clients, identity becomes a default starting point in search of a single source of truth. In fact, they can also choose to begin with the network segmentation approach to take the explicit trust out, but if the identities are not trusted, the outcomes and zero-trust maturity will remain limited in the organization.

Rising popularity of identity-based zero-trust approach

As mentioned above, there are different ways of implementing zero trust and each way prioritizes certain elements. However, enterprises seem to be more inclined toward the identity-based zero-trust approach. This approach has gained popularity due to certain factors, some of which are discussed below:

- **Manageable identities:** Deploying and managing a centralized Identity and Access Management (IAM) service is comparatively easier than managing complex network architectures through API layers

- **Cost effective:** Identity-based zero trust employs a centralized IAM service that does not require high capital investments as most clients already have an IAM solution, which can be extended to the entire organization through license upgrades
- **Granular controls:** Identity-based zero-trust approach provides more granular telemetry data for the policy engine, which improves accuracies and enables enterprises to have more confidence in the policy engine

Zero-trust implementations can start from small Proof of Concepts (PoCs), progress to easy-to-shift workloads, and then finally target more complex workloads. All this is possible if there is a well-defined approach and long-term roadmap for implementing zero trust that considers all the complexities and investments made by enterprises. Zero trust is more likely to succeed if it is implemented in a phased manner.

Potential pitfalls to avoid

Enterprises looking to adopt identity-based zero-trust approach need to be mindful of the following:

- **Complexity in implementation:** National Institute of Standards and Technology (NIST) compliant identity-based approach is not easy to implement. Enterprises following NIST guidelines on zero trust must be aware that NIST's zero-trust identity approach that meets all the requirements of NIST SP 800-207 is difficult to implement as it requires identifying the person, device, location, and behaviors of all interactions with the enterprise IT environment. Moreover, most next-generation tools have limited technical capabilities making it difficult for enterprises to have a robust NIST compliant identity approach
- **Integration with legacy systems:** Integrating modern IAM tools with legacy infrastructure can be challenging and result in poor configurations that can affect enterprises' security posture. So, enterprises need to move cautiously while integrating IAM tools with the legacy infrastructure

Identity-based zero-trust maturity assessment framework

Enterprises often complain about the lack of understanding around their current identity-based zero-trust maturity state. Very often, they end up investing in tools and technologies that either have a short shelf life or result in vendor lock-in scenarios. In addition, several enterprises take a long time to progress from the basic zero-trust state to an advanced zero-trust state. Hence, it is vital for them to have an accurate understanding of their current state, their future state, and all the enabling tools and technologies they may need to transition from the current state to the future state. Enterprises can embark on their identity-based zero-trust adoption journeys through two approaches, both of which have their own benefits and challenges. They are described in detail below.

Approaches to identity-based zero-trust adoption

Leveraging inhouse capabilities

Enterprises can adopt zero trust by leveraging their inhouse security teams. However, the major challenge in this scenario is inhouse resources' limited experience in implementing large scale zero-trust projects. Some enterprises can also choose to adopt zero trust through a technology provider. In this case, it is the enterprise's responsibility to avoid vendor lock-ins. Additionally, most technology providers are keen to sell their own products, even if their product is not the right fit. This can result in high technical debts and a painful product switching experience for enterprises.

Leveraging providers' experiences

Leveraging a cybersecurity service provider that has experience in implementing zero-trust engagements is the most pragmatic approach to zero-trust adoption. Enterprises can opt for a provider with similar goals and cultural values, nuanced capabilities, appropriate resources, focus on employee experience, and a partner ecosystem that can support zero-trust adoption.

Enterprises need to understand that when selecting a technology stack, they need not choose the best-in-breed products. In fact, they should select tools that can communicate efficiently with each other and easily integrate with the policy engine. To assist enterprises in their identity-based zero-trust implementation journeys, we have developed a framework (see Exhibit 3, below) that can help gauge their maturity across the fundamental blocks of users, devices, and applications. We have further categorized these blocks as basic (beginning state of zero-trust implementation), medium, and advanced (highest level of zero-trust implementation).

EXHIBIT 3

Framework for current state assessment of identity-based zero trust

Source: Everest Group (2023)

	Basic zero trust	Medium zero trust	Advanced zero trust
Devices	• Access policy employs basic parameters • Missing device risk score integration • Devices are not connected with IdM solution • Missing MDM solution • Missing centralized monitoring of devices	• Access policy captures data from two or three parameters • Basic device risk score integration • Some devices connected with IdM solution • Certain group of mobile devices is enrolled on the MDM solution • Device monitoring is centralized but all devices are not compliant to policies	• Access policy captures data from multiple parameters such as location, time, user risk, etc. • Well-integrated device risk score • Devices are completely connected with IdM solution • Mobile devices are enrolled and actively maintained on the MDM solution • All devices are compliant, and monitoring is centralized
Applications	• Policy engine is usually basic SIEM or EDR • Legacy authentication protocols are enabled • Basic integration of policy engine and IAM solution(s) • Resource access is controlled via RBAC • All applications are not integrated with the security platform	• Policy engine is usually SIEM and EDR • Partial disablement of legacy authentication protocols • Partially integrated policy engine with IAM solution(s) • Resource access is controlled via CAC • All on-prem applications are integrated with the security platform	• Policy engine is a mix of SIEM, XDR, CASB, and others • All legacy authentication protocols are disabled • Deeply integrated policy engine with IAM solution(s) • Resource access is controlled via ABAC or PBAC • All applications – on-prem and SaaS, are connected to the security platform and monitored
Users	• MFA restricted to admin only • Basic authentication without passwords • SSO is implemented for employees • Real-time user and sign-in risk detection not implemented	• MFA covers group of users • Some degree of authentication without passwords • SSO is implemented for employees and partners • Some degree of real-time user and sign-in risk detection implemented	• MFA covers all set of users • In-depth authentication without passwords • SSO is implemented for employees, vendors, partners, and customers • Implemented real-time user and sign-in risk detections

Automation, monitoring, and analytics

> The zero-trust model's **never trust, always verify** approach results in significant changes to an organization's mindset regarding how resources are accessed, as it requires enterprises to adopt a coordinated and structured approach to cybersecurity. Organizations must shift to a culture based on processes and procedures that support continuous verification, only then can each entity within a company's IT environment be trusted at any given point in time.
>
> – Vice President of cybersecurity at a service provider firm

The assessment framework lists zero-trust characteristics of each fundamental category across all maturity levels – basic, medium, and advanced. Enterprises can use this framework and prioritize different characteristics based on their zero-trust outlook and the pitfalls they want to avoid during the initial stages of their adoption journeys. In addition, on all three levels of maturity, it is important to realize different degrees of automation, monitoring, and analytics. An advanced zero-trust stage will have automated response capabilities such as automated device isolation or intelligent network segmentation to minimize the blast radius. Similarly, the analytics and monitoring capabilities of an advanced state can include AI-enabled asset visibility, next-generation threat correlation capabilities on logs from multiple security solutions, and automated onboarding of devices and users. Even for a basic zero-trust state, some level of automation, analytics, and monitoring is required to qualify as zero trust. Enterprises looking to implement efficient zero-trust strategies need to integrate all these tools with the policy engine, so that it can make an informed decision.

Enterprise adoption of zero trust across different industries

It is evident that identity-based zero-trust strategies have gained popularity in recent years. Enterprises ranging from banking to healthcare sectors are readily adopting zero trust to strengthen their cybersecurity posture. The following section highlights the benefits of zero-trust adoption realized by different industries.

Banking, Financial Services, and Insurance (BFSI)

Reduced risk of breach

BFSI firms need to protect their IT systems at various touch points such as employees, customers, and partners. Since the touchpoints are constantly expanding, securing them with the traditional perimeter-based approach has become a major challenge. The issue was further aggravated by the pandemic, which increased digital interactions between banks and end users. To counter this challenge, BFSI firms can adopt zero trust to improve their overall security posture and restrict lateral movement, thereby reducing the risk of breach.

Improved data protection and compliance posture

BFSI firms are usually at the mercy of regulatory bodies. They not only need to adhere to the expansive set of regulations but also adjust to their dynamic nature, which makes it challenging to standardize everything. Implementing a zero-trust architecture deepens security controls, allows extensive monitoring, and provides resource access to people with the right level of authorization. These capabilities offer improved compliance posture to enterprises and enable them to comply with PCI DSS, FISMA, GDPR, CCPA, and other core data privacy and security laws.

Unified global security strategy

Large BFSI firms usually have several offices worldwide, but they lack a coherent global security strategy. There have been instances where different technology stacks were being employed in two different locations for large BFSI firms. In such situations, zero-trust adoption can improve enterprises' security posture, assimilate their technologies, tools, and policies, and enable them to build a unified global security strategy.

> We adopted zero trust not just to improve our security posture, but to also improve our overall compliance positioning and reduce the risk of data breach as we are very conscious of our brand's reputation.
>
> – CISO, Fortune 500 financial services company

Public sector industries

Deeper controls with minimal network architecture changes

Public sector enterprises, barring federal agencies, lack a well-defined network architecture and deeper control on resources and subjects. Zero-trust adoption will allow public sector enterprises to gain deeper control and improved incident response capabilities without any radical changes in the network architecture

Mitigating insider attacks

Public sector enterprises frequently use personal identifiable information to pass subsidy benefits, verify official work, and provide better healthcare. However, these processes are always at a risk of insider threats and human errors. Adopting zero trust will provide resource access only to individuals with the right authorization. The access will also be dynamically monitored, thereby significantly reducing the risk of insider attacks.

Reduced risk of zero-day exploits

Public sector enterprises are quite lax in patching zero-day vulnerabilities, especially when it comes to open-source products. This delay in patching can increase the risk of cyberattacks. By adopting zero-trust architecture, enterprises can contain the blast radius and limit attackers' lateral movements through attribute-based analysis.

> With rising ransomware attacks and increased risk from zero-day vulnerabilities, we wanted to adopt an approach that helps us tackle this multifaceted challenge. Zero trust did just that.
>
> – Head of cybersecurity at a public sector firm from APAC

Healthcare and Life Sciences (HLS)

Reduced third-party costs

HLS firms do not always have an inhouse cybersecurity team, owing to the talent crunched cybersecurity market. They usually employ third-party providers to manage their cybersecurity posture, which can be premium priced. However, partnering with providers also comes with its own set of challenges such as resource onboarding, defining KPIs, measuring SLAs, and tracking contractual obligations. Adopting zero-trust architecture will streamline HLS firms' cybersecurity posture and reduce operational costs by employing well-integrated toolsets that require less resources for their management.

Reduced risk of unauthorized access to patient data

HLS firms are required to share patient data with doctors, nursing staff, administration officials, suppliers, and partners. Since the business touch points are different for different providers, managing their authentication and authorization can be a daunting task. This increases the risk of unauthorized access to patient data. For HLS firms, zero trust can provide an additional layer of security between suppliers and end users to reduce the risk of unauthorized access.

Improved authorization posture

HLS firms rarely employ a robust authorization process. This practice can enable anyone from the hospital staff to access confidential patient data that is only authorized for doctors. This inconsistent approach can also result in complications with different compliances and data privacy regulations. By adopting zero trust, enterprises can realize deep control and data visibility to implement correct authorization.

> "Even at the early medium state of zero-trust adoption, we were able to realize the cost benefits through reduced dependence on our outsourcing partners.
>
> – CFO of a healthcare company in Europe

Guiding principles for implementing zero trust

As discussed above, zero trust is a security strategy that is governed by certain implementation principles. With an aim to standardize the approach, NIST has defined seven implementation tenets for zero-trust[1] architecture. The tenets are well accepted by technology and service providers and are as follows:

- **All data sources and computing services are considered resources:** Enterprises need to consider every device, user, and application, both trusted and untrusted, as a resource
- **All communication is secured regardless of network location:** Resources on enterprise owned and non-enterprise owned networks should be treated the same, that is, all networks are considered hostile
- **All resource authentication and authorization is dynamic and strictly enforced before access is allowed:** Enterprises need to possess technical capabilities and ensure continuous authentication to adapt to evolving conditions or requirements
- **Enterprises monitor and measure the integrity and security posture of all owned and associated assets:** Do not inherently trust resources, that is, all resources (devices, users, and applications) must be dynamically monitored to meet the basic criteria of trust, otherwise they are classified as untrusted
- **Enterprises collect as much information as possible about the current state of assets, network infrastructure, and communications and use it to improve their security posture:** Enterprises need to collect information to inform actions and approaches to guard security, which is a constantly improving cycle
- **Access to individual enterprise resources is granted on a per-session basis**: Evaluate resource's trust before granting access to a subject with minimum privileges to complete the task
- **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:** Resource authorization is based on privileges granted at that point in time and can change due to altered conditions or requirements

Enterprises must understand that these tenets are not mutually exclusive and there could be some level of overlap among them. However, if we were to look at them from a mutually exclusive perspective, we can segregate them under three broad categories: authentication, authorization, and monitoring. Below exhibit illustrates these categories clearly.

EXHIBIT 4

Three categories of NIST's tenets on zero trust

Source: Everest Group (2023)

1 Zero-trust Architecture - NIST Technical Series Publications

Conclusion

We can see how identity plays a vital role in enterprises' zero-trust adoption journeys. However, as discussed above, we must not push for best-of-breed products for identity and only select tools that can easily communicate and integrate with each other.

Zero-trust maturity assessment is perhaps a good starting point for any enterprise and can serve as a precursor to choosing the right technology stack and implementation partner – inhouse or third-party provider. We strongly believe that partnering with providers who have extensive experience in implementing zero trust in different organizations is vital for success as it demands careful attention, planning, discipline, and intention. Such providers will ensure smoother implementation, consider employee experience as a critical KPI, and, most importantly, share enterprises' cultural and corporate values. At the same time, managing the cultural change is vital. Enterprises can educate employees about their zero-trust journey and promote the cultural shift by recognizing small victories, reducing friction, and implementing a rewards system. In addition, enterprises must understand that zero trust is not a single technology upgrade but a gradual journey toward an architecture that not only provides primary benefits, but multiple secondary benefits such as:

1) Improved employee experience
2) Reduced legacy technical debt
3) Decreased third-party risk and costs

CEOs, CMOs, CFOs, and other non-technical executives need to understand that zero trust is not just a CISO mandate as it brings in immense secondary benefits such as reduced support cost, deepens control on assets, improves compliance positioning, reduces the risk of insider attacks, improves data governance (vital ESG component), and allows enterprises to shift from a siloed security approach to a more unified one. Zero trust can solve multiple problems that are not necessarily a CISO challenge.

C-suite executives frequently ask, Is zero trust just a technical change?. We believe that zero trust is all-encompassing as it impacts the broader corporate strategy. Zero trust is more about a corporate and cultural behavior change than just a technical upgrade. For the success of zero trust, it is imperative for organizations to commit to the process and identify approaches to remove implicit trust from all their security controls.

Everest Group®
With you on the journey

Everest Group is a leading research firm helping business leaders make confident decisions. We guide clients through today's market challenges and strengthen their strategies by applying contextualized problem-solving to their unique situations. This drives maximized operational and financial performance and transformative experiences. Our deep expertise and tenacious research focused on technology, business processes, and engineering through the lenses of talent, sustainability, and sourcing delivers precise and action-oriented guidance. Find further details and in-depth content at **www.everestgrp.com**.

This study was funded, in part, by NTT DATA

For more information about Everest Group, please contact:

+1-214-451-3000
info@everestgrp.com

For more information about this topic please contact the author(s):

Kumar Avijit, Practice Director
kumar.avijit@everestgrp.com

Arjun Chauhan, Senior Analyst
arjun.chauhan@everestgrp.com