LTIMindtree

Whitepaper

Zero Trust

Elevating Cybersecurity in the Digital Age

Table of Contents

1. **Executive Summary**... 3

2. **Introduction**

   i. What is zero trust?... 4

   ii. Why is zero trust relevant today?.. 4

3. **Technology insights**

   i. Zero trust for effective security... 6

   ii. Key enabling technologies... 8

4. **Market insights**... 10

5. **Key Application Areas**.. 13

6. **Value offered by zero trust**.... 15

7. **Opportunity areas for LTIMindtree**... 18

8. **Skeptic's opinion around zero trust**.. 19

9. **Conclusion**.. 20

10. **Author**.. 22

11. **References**...24

01 Executive summary

Cybersecurity has become a top priority for businesses, leading to the establishment of robust defenses to safeguard their systems and infrastructure. Unfortunately, in recent years security measures are yet to keep up with current tech advancements, and modern cyberattacks emerging because of them.

Traditional cyber security approaches focused on securing the perimeter when data and users were confined to specific, well-defined locations. The perimeter-based security acted as the primary point for enforcing security controls. Once this perimeter is breached, most resources become accessible. However, due to the changing IT landscape and policies, including cloud applications, and bring-your-own-devices for smartphones, that may extend beyond the traditional perimeters, the traditional methods are no longer sufficient, as numerous devices within a system have internet connectivity. If a device is compromised, an attacker can access the corporate grid without traversing the perimeter. Hence, a new paradigm is necessary: Zero trust.

Zero Trust is not merely a concept anymore; governments and organizations are now focusing on zero trust principles like never before to keep up with the technologies that makes system vulnerable. However, the effective implementation of zero trust is dictated by harmonious coordination of both legacy, contemporary systems and services to offer policy-driven controls. Nevertheless, overseeing these interactions brings about fresh challenges.

This document aims to provide a high-level understanding of zero trust and explore the core use cases in which zero trust can enhance security in digital age. As per our research, to successfully implement Zero Trust, organizations must clearly understand their crown jewels, data assets and working of zero trust framework. While organizations deliberate on their future course, we undertake a comprehensive analysis of the value zero trust offers in this document. We highlight some of the most persistent obstacles regarding implementing zero trust framework in the form of skeptic's analysis. Forward-thinking organizations are focusing on integrating the elements of zero trust framework with the existing security architecture blocks to strike a harmonious balance between automatic trust and long-term security.

02 Introduction

What is zero trust?

Trust is a precarious concept in information technology, particularly when it is assumed without question or reservation. Relying solely on a fortified corporate security boundary and placing unwavering trust in everything within it has repeatedly proven to be a flawed approach.

Zero Trust operates around "Never Trust, Always Verify" philosophy, is a security framework that challenges the traditional perimeter-based security model. It establishes trust between specific resources and consumers only when necessary, allowing organizations to build more secure, configurable, and highly adaptable technology platforms. Zero trust relies on an identity-aware, context-driven, and data-centric approach that enables secure access to data and resources. Every user must authenticate their identity within the zero-trust framework to gain access.

Why is zero trust relevant today?

Previously, organizations used to believe that everything within the security perimeter was secure and relied on on-premises firewalls and VPNs to safeguard network access. Today, the traditional perimeter has undergone significant changes due to the transfer of workload to the cloud and the prevalence of non-managed devices. The traditional notion of fixed locations for applications, users, and devices has become obsolete. Data is no longer confined solely to the corporate data center.

With the use of Software-as-a-Service (SaaS) applications, cloud platforms, and other cloud-based services, data is now located outside the confines of the corporate perimeter. Also, due to the emergence of public cloud platforms, devices and services that were once operated within the corporate perimeter are now being operated externally. Workloads are migrating towards the most cost-effective processing solutions, thus increasing the gap between our data and the networks we own, control, and trust. The traditional model of a corporate system

working with static defenses fails to empower businesses to fully embrace innovations like the cloud while simultaneously safeguarding their data, users, and customers.
Simultaneously, cyber-criminals have become increasingly skilled at evading advanced security measures. They employ lateral movement techniques to infiltrate their targets, exploiting vulnerabilities. These attackers have access to sophisticated toolkits and detailed instructions on exploiting weaknesses.

Furthermore, the number of vulnerabilities continues to rise, as evidenced by the **National Vulnerability Database (NVD),** there were 28,823 vulnerabilities documented in 2023, surpassing 2022 count by 3,781 common vulnerabilities and exposures (CVEs). As of May 2024, 17000 vulnerabilities have been detected, witnessing a y-o-y rise of 7.8%. This indicates a consistent upward trend in the identification of vulnerabilities year after year.

Zero trust is crucial to mitigates CVEs by enforcing "never trust, always verify" through explicitly verifying identity, enforcing least privileged access, and always assuming the possibility of a breach. Zero trust along with organization security services, platforms, and automated multi-factor authentication (MFA) for machine-to-machine connections will enable seamless application of the principle.

03 Technology insights

Zero trust for effective security

To implement zero trust in your cybersecurity system, it is necessary to understand the zero-trust security model. Zero trust security model is an organizational cybersecurity framework designed to lower a corporate system's attack surface, avoid lateral movement of threats, and reduce the risk of a data breach based on a never trust, always verify principle. It assumes all traffic is untrusted and should be verified before accessing resources. It removes the concept of trusted connectivity and offers a granular and contextual approach to access control. It enables organizations to secure their data and applications regardless of where they are hosted or accessed from and provides real-time threat detection and response capabilities. Zero trust stands on three key principles: Data, identity, infrastructure, with automation, and analytics acting as horizontal components encompassing the pillars as shown below.

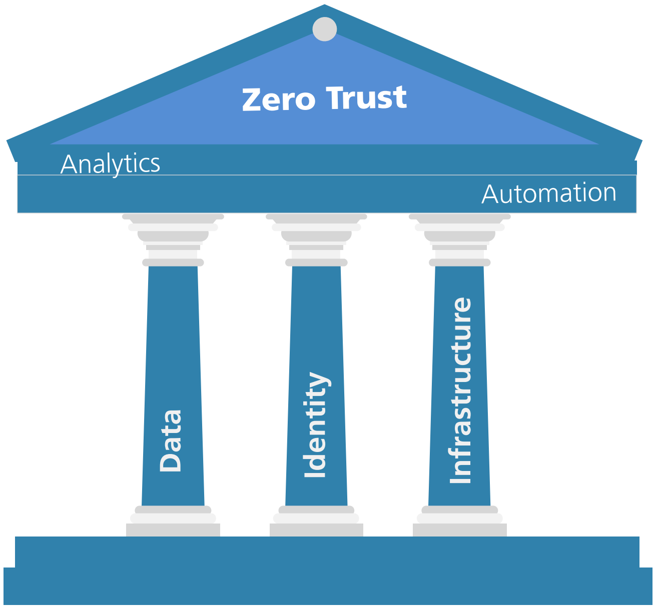


Figure 1: Pillars of zero trust security model

The first pillar focuses on data protection, data issuance, classification, identification, and deployment of exfiltration detection mechanisms.

The second pillar emphasizes the use of Identity, Credential, and Access Management (ICAM) and multifactor authentication (MFA) when interacting with services/data, confirm authentication of trusted users, and trustworthiness of user and entities on an ongoing basis. Enterprise’s managed entities are used for on-premises & cloud environment.

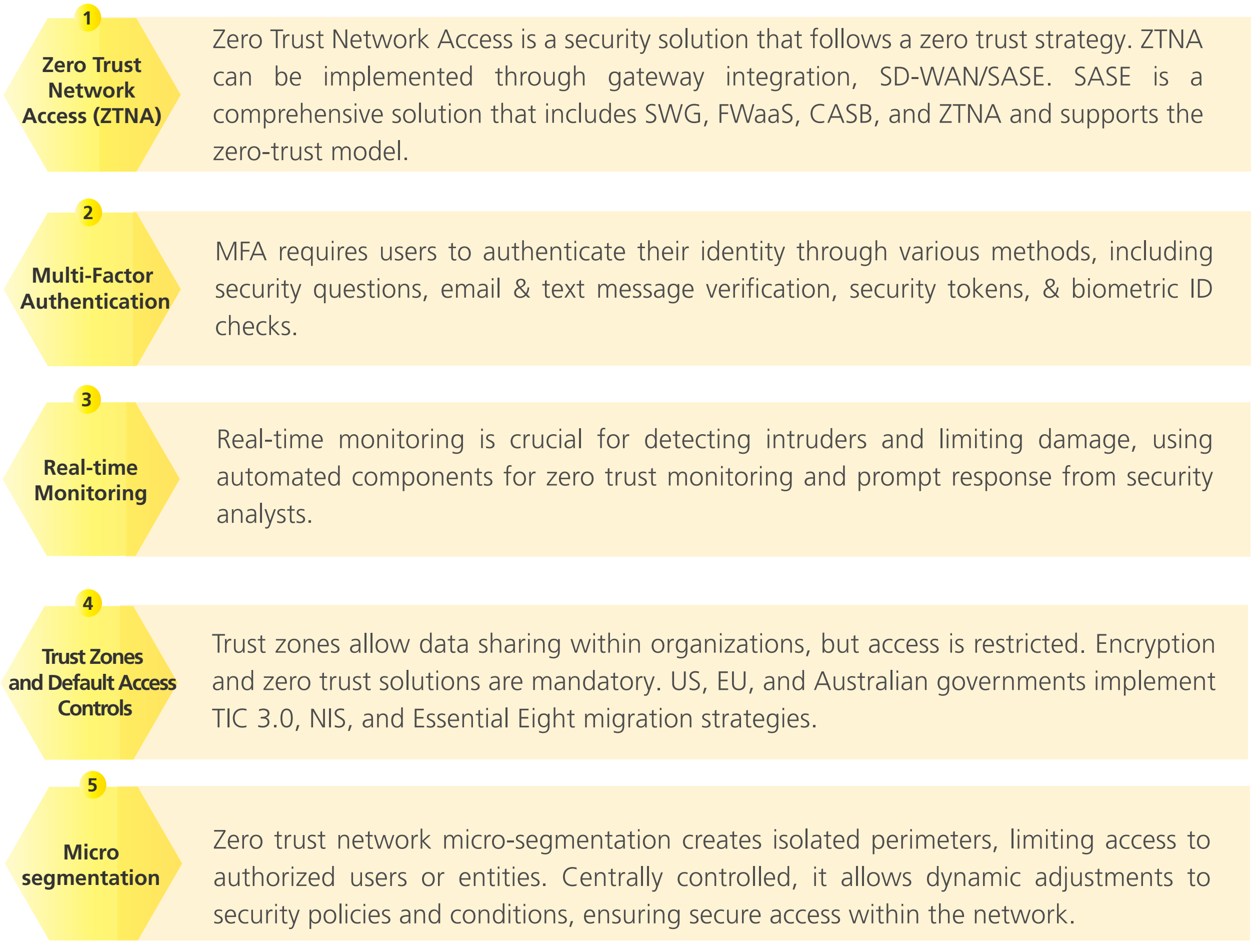
The third pillar puts stress on configuration management & software updates to ensure that deployed infrastructure meets security and policy needs. It also moves perimeters in from the network edge and segments and isolates critical data from other data. Cloud has blurred the boundaries between traditional infrastructure and application and therefore a layer of convergence, hence It is critical for securing and effectively managing the application layer by authorizing application access on regular basis, integrating threat protection into application workflows and perform application security testing throughout development/deployment process.

The horizontal layer of Automation security uses security automation response tools and security orchestration to manage disparate security systems and reduce manual effort, whereas the analytics security, uses advanced analytics platforms leveraging artificial intelligence and big data to enable real-time observation and proactive security measures.

Zero Trust provides critical protection against cyberattacks carried out by generative AI. Generative AI can be employed to craft emails resembling those from a reputable company or to create convincing fake websites. This tactic thereby increases the chances of users disclosing sensitive information or entering their login credentials, which is called credential phishing. Zero Trust acts as a barrier that prevents cybercriminals from performing credential phishing by restricting their access to infected accounts only. It also limits the attacker's access to other applications despite accounts being connected to multiple other systems and applications. Zero Trust can enable consistent monitoring of user behavior to identify potential threats at an early stage, thereby reducing both external and insider risks.

Key enabling technologies

The mode of implementation of zero trust may vary as per organizational needs, however following technologies are identified as essential components for enabling zero trust.



1 **Zero Trust Network Access (ZTNA)**

Zero Trust Network Access is a security solution that follows a zero trust strategy. ZTNA can be implemented through gateway integration, SD-WAN/SASE. SASE is a comprehensive solution that includes SWG, FWaaS, CASB, and ZTNA and supports the zero-trust model.

2 **Multi-Factor Authentication**

MFA requires users to authenticate their identity through various methods, including security questions, email & text message verification, security tokens, & biometric ID checks.

3 **Real-time Monitoring**

Real-time monitoring is crucial for detecting intruders and limiting damage, using automated components for zero trust monitoring and prompt response from security analysts.

4 **Trust Zones and Default Access Controls**

Trust zones allow data sharing within organizations, but access is restricted. Encryption and zero trust solutions are mandatory. US, EU, and Australian governments implement TIC 3.0, NIS, and Essential Eight migration strategies.

5 **Micro segmentation**

Zero trust network micro-segmentation creates isolated perimeters, limiting access to authorized users or entities. Centrally controlled, it allows dynamic adjustments to security policies and conditions, ensuring secure access within the network.

Figure 3: Zero trust components

Key recommendations before implementing ZTA

The implementation of a zero trust must be seamless across systems and Original Equipment Manufacturer (OEM) applications, with minimal horizontal integration services. OEM applications provide the necessary zero trust components and attributes but integrating them into zero trust models is challenging. The aggregation method must operate securely in shared, homogeneous environments. The following figure provides some key recommendations at a granular level.

Authentication

To effectively implement Multifactor Authentication, assess current systems, identify gaps, define MFA requirements and policies, select compatible solutions, integrate MFA with IAM, implement MFA across all access points, roll out MFA in phases, educate and train users, monitor and enforce compliance, and adapt and evolve.

Microsegmentation

To implement microsegmentation, assess and map the network, define security policies for each segment, use next-generation firewalls & SDN, implement identity-based segmentation, continuously monitor & analyze traffic, test & refine segmentation strategies, and educate & train IT staff on microsegmentation principles and technologies.

Least Privileged Access

To ensure security, users must have the minimum level of access needed for their task. This method prevents lateral movement and limits potential harm from breaches. It also prevents internal misuse of company data.

Device Discovery & Protection against Identity Theft

IT administrators must know which devices are working on the network, and credentials associated with each device, in a zero-trust model. This will provide a benchmark for normal traffic in the network. In this way, all anomalies could be easily identified, dealt with and flagged by the IT team.

Figure 4: Zero trust recommendations

Within the domain of cloud services and SaaS platforms, implementing Zero Trust principles requires the deployment of cloud access security brokers (CASBs). These brokers serve as vigilant gatekeepers, monitoring and managing the exchange of information between identity, infrastructure, and cloud servicess. They offer a clear view of activities within the cloud and apply security measures uniformly, regardless of the location of the data or the source of the access request.

04 Market insights

Zero trust has transformed from a Virtual Private Network (VPN) based security system to a crucial element of security architecture for remote and branch users. Despite high costs and existing investments in application-based solutions, large and midmarket organizations are strongly embracing Zero Trust as a concept as well as its architecture. According to **Gartner**, the adoption of Zero Trust Network Access, which is a part of Zero trust architecture remains robust among organizations with over 25,000 employees. Adoption is highest in North America and Western Europe, while Asia-Pacific has a lower adoption rate due to a focus on on-premises solutions.

According to **Markets and Market's** latest forecast, the overall zero trust architecture market is projected to witness an impressive growth of **17.3% CAGR between 2023 and 2028.** The forecast predicts the market size to grow from **$17.3 Bn to $38.5 Bn between 2023 and 2028.** The market is shifting towards SASE based architecture, which uses a zero-trust framework to establish secure connections between business users and essential applications. However, there is also a growing demand for agentless-based deployments, particularly for unmanaged devices and third-party access scenarios.

To address the diverse needs of organizations, security and risk management leaders must select a vendor that supports both approaches, enabling comprehensive coverage of the most common use cases. Tech and security leaders can assess potential vendors by examining their market presence, depth of security services and the type of offerings provided, such as domain-specific solutions, general-purpose platforms, and libraries of Application Programming Interface (APIs) and API services. Based on these factors, potential vendors can be divided into three groups: large vendors, medium vendors, and small vendors.

Following table provides a list of vendors and their zero trust products. This is not an exhaustive list but only highlights major players.

Hewlett Packard Enterprise (Axis Security)	Atmos ZTNA
Amazon Web Services	AWS Verified Access
Google	BeyondCorp Enterprise Google Cloud Platform Identity-Aware Proxy
Citrix	Citrix Secure Private Access
Cloudflare	Cloudflare Access
Cisco	Duo Premier, Cisco+ Secure Connect, IoT Operations Dashboard
Akamai Technologies	Enterprise Application Access
Microsoft	Entra Private Access
Forcepoint	Forcepoint ONE ZTNA
Zscaler	Private Access
Broadcom	Symantec Zero Trust Network Access
Fortinet	Universal Zero Trust Network Access

Figure 5: Vertical wise potential vendors

The Zero trust market trends are experiencing a shift from standalone providers to vendors offering augmented solutions with enhanced Zero Trust platform capabilities, with some focusing on secure access requirements in cyber-physical systems and others expanding security functions.

Zero trust framework vendors are improving their offerings to cater to outcome-driven use cases. Potential buyers are seeking vendors who can provide a range of zero trust functionalities and seamlessly integrate with their existing technologies, eliminating the need to replace their current investments. These vendors are now incorporating AI/ML functionalities to streamline the devices, applications, and users with security controls.

This move adds significant value to zero trust solutions, by automating and enhancing orchestration of security policies. It improves employee and analyst experience by reducing the complexity and steps required to manage and maintain security controls in a dynamic organizational environment.
Some recent developments by top vendors in Zero Trust Space:

Cisco Secure Access Edge (SASE)

Cisco's SASE is a cloud-based zero trust solution that grants protected access to applications and data from anywhere. It uses a variety of technologies, including micro-segmentation, identity-based access control, and threat intelligence, to protect users and resources.

Fortinet FortiNAC

Fortinet's FortiNAC is a Network Access Control (NAC) solution that helps organizations to enforce zero trust security policies. It uses various methods, including NAC, asset discovery, and user behavior analytics, to identify and control devices that are connected to the network.

Zscaler Zero Trust Exchange

Zscaler's Zero Trust Exchange is a cloud-based security platform that provides secure access to applications and data from anywhere.

05 Key application areas

The adoption of zero trust is not motivated by trendy, cutting-edge technology; rather, it is motivated by practical business needs. The primary reasons why most businesses are embracing zero trust are to enable and protect hybrid workforces, monitor, and secure data traffic within the enterprise, prevent unauthorized lateral movement, and streamline the costs and complexities associated with multiple point products and outdated systems. The following Zero Trust application areas are the ones that customers frequently seek and that zero trust vendors address.

Enable and protect hybrid workforce

- Detect, register, validate, authenticate, authorize, monitor, encrypt, and log workforce and endpoints from anywhere
- ZTA can enhance security and streamline ‘bring your own device’ initiatives by minimizing the need for complete device management and facilitating secure direct access to applications using Security Service Edge (SSE)
- AI/ML-based user, device access management, Deliver self-service functionalities, and Integrations with endpoint security tools Endpoint Protection Solutions (EPP), Endpoint Detection and Response (EDR) , etc.)

Prevent lateral movement of unauthorized activity

- Enforce application-aware controls around protected segments; limit threats to apps/services from exploitable lateral dependencies
- ZTA enables end-to-end encryption, creating user personas based on behavior, allowing legitimate access for users with devices in different countries while blocking compromised devices.
- Asset discovery with dependency mapping, Detect communication anomalies between workloads/applications, and Hybrid/multi-cloud support

Enforce the least privilege on all entities

- Create, manage, and authenticate human/non-human entity access rights through contextual, risk-based policies
- ZTNA secures enterprise applications by minimizing insider threats and administrative access division, utilizing persistent outbound listeners on port 443 to eliminate inbound access from public networks
- Agentless functionalities, 10T/Bring your own Device (BYOD) support, and User behavior analytics

Centrally manage key security controls

- Centralize, orchestrate, and automate management and configuration of network, data, application, and/or access controls
- ZTA simplifies access management for acquired organizations, managing administrative access to applications without expensive Privileged Access Management tools, and granting application-specific access to IT service providers and remote employees
- Native Data Loss Prevention (DLP), AI/ML-based user, device access management, and Cloud-agnostic deployments

Figure 6: Core use cases

06 Value offered by zero trust

There is great hype surrounding zero trust, with vendors making bold claims about its potential benefits. However, should we trust the hype? While it is not a magical solution, zero trust can offer numerous opportunities for organizations by aligning security with their business practices, mitigating risks, enhancing agility, and reducing operational expenses. Nevertheless, these advantages are not easily attained and necessitate support and dedication from all levels of the organization to materialize fully.

Zero trust frameworks can consolidate disparate security tools under a single roof. They offer a unified solution that combines multiple functionalities, reducing deployment complexity and configuration management while enhancing user experience for auditing and reporting through customizable dashboards that consolidate events and logs. Zero trust emphasizes the defense-in-depth approach while preventing deployment of non-integrated, multi-vendor technologies with duplicated functionalities.

Zero trust is gaining prominence as the growing prevalence of remote workforces, cloud services, BYOD (Bring Your Own Device) policies, and decentralization of information systems has made systems, networks, and infrastructure protection difficult. Zero trust applies strong security measures across hybrid business and operational models. Zero trust with flexible deployment options enable organizations to implement important components of a reliable zero trust strategy, such as virtualization, micro-segmentation, and detailed risk-based controls.

Advantage

A zero-trust model offers numerous advantages, and to simplify your life, we have identified some of the key ones.

- **Enhanced control over the entire IT infrastructure:** You will have complete control within the office premises or on cloud platforms. No longer will you face challenges with users outside the corporate perimeter or struggle with remote access.

- **Consistent management and security for all users:** You can treat all users equally by eliminating the concept of inside or outside the corporate perimeter. This simplifies IT security and ensures all devices and users receive the same level of protection.

- **Security maintenance in diverse environments:** Even if you do not own or have full control over the infrastructure being used, you can still maintain security. You can establish robust security across any environment, platform, or service by leveraging identity, location, device health, MFA, and implementing monitoring and analysis.

- **Significant reduction in malware and attacker movement:** Instead of granting attackers unrestricted access to the entire network once they breach it, they will only have limited access to the compromised user's systems. By maintaining distrust towards authenticated users, additional checks will be in place between these systems, further limiting the spread of malware or attackers.

Challenges

Every organization's path toward zero trust will vary and be influenced by their unique business objectives. However, challenges and pitfalls frequently encountered must be overcome. Some of these obstacles include:

- **Embracing change:** Zero trust must be supported by a dynamic and adaptive cyber organization which embraces new working methods.

- **Integrating legacy:** Bespoke approaches are often required to enable legacy systems (Information Technology & Operational Technology) to participate in zero trust environments.

- **Having end-to-end visibility:** Zero trust requires end-to-end visibility of what you have and how it is used to provide the basis for trust.

- **Incomplete solution:** Zero trust has no silver bullet, with no vendor providing an end-to-end solution.

- **Designing for adaptability:** Zero trust is evolving rapidly. New capability arrives frequently, and a zero-trust program must be agile to keep pace.

- **Making it all work together:** The lack of common zero trust standards lead to integration challenges between solutions.

Zero trust frameworks go beyond being a mere portfolio of add-on tools. It integrates key zero trust functionalities to enable centralized management of security solutions (vendor or third-party). This empowers organizations to prioritize outcome-driven use cases rather than spending time integrating a diverse range of non-integrated technologies, thus expediting their zero-trust transformation.

07 Opportunity areas for LTIMindtree

Zero trust is expected to experience rapid growth. Considering the previous observation, we have identified a range of services that SI providers such as LTIMindtree can consider offering to their corporate customers. The services mentioned here only scratch the potential surface, but given this technology's significance and importance, the opportunities are limitless.

Strategy and technology consulting

LTIMindtree has a strong foundation in advisory services, partnering with industry leaders, and can provide comprehensive guidance for creating a zero-trust strategy, architecture, and roadmap. Our team of experts in architecture, business, technology, and experience can cover all aspects of the process to align with your objectives.

Design services

Create, construct, and develop E2E zero trust solutions - deliver ready-to-use services that can be integrated and enhanced to assist clients in reimagining their workflows, streamlining business operations, and introducing innovative strategies for enhanced security. LTIMindtree with its deep expertise in AI could create intelligent zero trust platforms with generative capabilities. These platforms could integrate Gen AI platforms for detecting anomalies, updating AI models, and continuous threat monitoring and improvement.

Deployment services

We can offer deployment services to ensure the smooth operation, improvement, and integration of existing security applications in single platforms. This is essential to keeping up with technological advancements and complying with standards, security, and government regulations. We can work closely with customers to address any upcoming changes that may impact on their applications and find solutions to mitigate any issues.

08 Skeptic’s opinion around zero trust

Despite the potential advantages of implementing Zero Trust concepts, organizations are not fully capitalizing on them, resulting in a low adoption rate. According to Gartner, currently only 1% of large enterprises have well-established and measurable zero trust programs in place. However, there is optimism that this number will increase to 10% by 2026.

We believe that organizations are growing disillusioned with zero trust due to its constant hype and unrealistic promises. As a result, two main types of organizations have emerged.

The first type consists of organizations that have implemented isolated deployments of zero trust technologies without a comprehensive plan. For instance, during the recent pandemic, many organizations adopted ZTNA as a solution to overloaded VPN.

However, instead of using ZTNA to enhance security alongside VPNs, these organizations mistakenly used it as a direct replacement, diluting its benefits. Consequently, organizations continue to rely on traditional VPNs, leading to minimal cost reductions and, in some cases, increased expenses from running two similar capabilities simultaneously.

The second type involves organizations that have attempted to design and launch large-scale, monolithic zero trust programs. These programs aim to achieve a grand target state architecture without considering the actual needs of the business. They are planned as multi-year journeys with substantial budget estimates. However, based on our experience, these programs either fail to launch entirely or get discontinued within 12-18 months when they fail to deliver immediate value.

09 Conclusion

Zero trust offers a framework for an enterprise's cybersecurity architecture to attain a security posture driven by risk, aware of context, and adaptable. Implementing correctly equips organizations with enhanced cyber defense capabilities and resilience.

The pandemic showcased the importance of zero trust security and organizations with well-established zero trust security facilitated secure remote access for their employees, ensuring uninterrupted business operations. With the increasing prevalence of Generative AI, the risk of cyberattacks utilizing this technology is also on the rise.

The utilization of Gen AI by cybercriminals presents significant dangers to the security and integrity of organizations' data. Various risks associated with generative AI in the realm of cybersecurity encompass Credential Phishing, Endpoint exploitation (employing AI to streamline the identification and exploitation of vulnerabilities, constructing intricate attack vectors, and eluding detection), Business email compromise (BEC), and Malware creation. To combat Gen AI cyberattacks, organizations need to embrace the Zero Trust security model.

Zero Trust can incorporate an additional layer of authentication beyond passwords that can prevent unauthorized access, even in cases where attackers acquire login credentials through phishing schemes. It also removes the necessity of generating passwords, minimizing the chances of credential theft. Limiting each user's access to essential resources exclusively, zero trust can mitigate risks in the event of a security breach compromising the user's credentials.

However, it is crucial to prioritize establishing and maturing of basic security controls before embarking on zero trust initiatives. Organizations should adopt a comprehensive and practical approach to achieve their desired level of maturity. This entails building upon a strong foundation of cyber hygiene and implementing a phased, comprehensive, and practical strategy to expedite the attainment of zero trust security maturity.

Another noteworthy progress in the field of zero trust is distributed ZT, in hyper-converged infrastructure (HCI), distributed zero trust is essential as it improves security by imposing stringent, continuous verification for each user and device across the system. By reducing the risks connected with centralized security approaches, this strategy makes sure that the integrated environment is well-defended against lateral threats. Zero trust's micro-segmentation and granular access controls are crucial for sustaining a safe, robust architecture when HCI incorporates several components.

10 Authors

Chandan Pani (CISO)

Associate Vice President, Corporate Security

Chandan Pani is a Cybersecurity expert with more than 25+ years of experience in cyber risk mitigation, security forensics, and regulatory compliance. Chandan has been associated with responsibility for setting up information security programs, technology risk evaluation large, offshored programs, including governance, policy, awareness, project management, audit, assessment, incident response, operations, technical investigations, business continuity and disaster recovery. He is also an avid reader and closely follows technology. He recommends having zero trust as a principle and states: Never trust, always verify." This phrase emphasizes that in a zero-trust environment, no user, device, or application is inherently trustworthy. Every access attempt needs to be continuously verified.

Vijay Rao

Principal Director – Architecture, GTO

Dr. Vijay Rao is a distinguished expert in R&D and innovation leadership with a robust academic and professional background. He holds a PhD and completed his Postdoctoral research at the prestigious TU Delft in the Netherlands. Dr. Rao has extensive industry experience, particularly in the fields of communication and the Internet of Things (IoT). His career is marked by significant contributions to advancing technologies and driving innovation within these domains. Known for his strategic vision and leadership, Dr. Rao continues to push the boundaries of what is possible in communication and IoT, making a notable impact in the industry.

Bharat Trivedi

Principal Architect, GTO

With 20+ years of experience, Bharat is a product developer by heart, he has been instrumental in introducing high tech in areas like Retail Banking, Capital Markets, Online Trading and the Regulatory Space. His unique way of looking at technology makes him an able mentor to the aspiring.

Hakimuddin Bawangaonwala

Senior Consultant, GTO

Hakimuddin is a seasoned consultant with over 4 years of experience in the industry. Specializing in investigating beyond-the-horizon technologies, Hakimuddin has worked on a diverse range of technologies, helping organizations to create use cases for quick incubation and industrialization leveraging these technologies. Hakimuddin holds a master's degree in design engineering and has published numerous articles and whitepapers on emerging technologies. In addition to consulting, Hakimuddin enjoys collaborating on deep research projects and contributing to the community.

Namrata Sharma

Senior Consultant, GTO

Collaborative and vigorous with a propensity to solve problems, Namrata Sharma brings noteworthy amount of experience within the management consulting and research domain. Namrata's areas of expertise include strategic planning, creating market intelligent studies, data modelling, and domain critical evaluation. In her tenure as a Senior Consultant, Namrata is currently working on analyzing potential technologies, market opportunity assessment, and creating Deep Point of Views and Beyond the horizon areas.

11 References

- *Zero Trust Essentials eBook***,** Microsoft, Zero Trust essential e-book, Microsoft, 2022: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWIrfk
- *Trust architectures and digital identity*, August 2022: https://www2.deloitte.com/uk/en/pages/risk/articles/zero-trust.html
- *Technology Trends Outlook 2022:* Trust architectures and digital identity, McKinsey, August 2022: https://www.mckinsey.com/spContent/bespoke/tech-trends/pdfs/mckinsey-tech-trends-outlook-2022-trust-arch-digid.pdf
- *From Zero to Hero: Why Zero Trust Adoption is Struggling,* Charlie Hosner, Matt Dibble, Hasan Muchhala, Sophie Cole & Lachlan George, BCG, June 2023: https://media-publications.bcg.com/flash/dotbcg_other/Zero-Trust_vF.pdf
- *The Forrester Wave™: Zero Trust Platform Providers, Q3 2023,* Carlos Rivera, Heath Mullins, Joseph Blankenship, Dan Beaton, Kara Hartig, Forrester, 2023: https://reprints2.forrester.com/#/assets/2/108/RES179872/report
- *The Why and How of adopting Zero Trust Model in Organizations*, Nair, Anita, (2021): TechRxiv.: https://www.techrxiv.org/doi/full/10.36227/techrxiv.14184671.v1
- *Demystifying Zero Trust, SOPHOS, 2020:* https://www.sophos.com/en-us/whitepaper/demystifying-zero-trust
- *Rise of Zero Trust: Separating the Reality from the Myths,* Juniper Networks, 2019: https://www.juniper.net/-content/dam/www/assets/white-papers/us/en/security/the-rise-of-zero-trust.pdf
- https://media.bitpipe.com/io_15x/io_158372/item_2560584/the-big-book-of-ztna-security-use-cases-.pdf
- *Implementing a Zero Trust security model at Microsoft,* Oct 23, 2023,: https://www.microsoft.com/insidetrack/blog/implementing-a-zero-trust-security-model-at-microsoft/

LTIMindtree is a global technology consulting and digital solutions company that enables enterprises across industries to reimagine business models, accelerate innovation, and maximize growth by harnessing digital technologies. As a digital transformation partner to more than 700 clients, LTIMindtree brings extensive domain and technology expertise to help drive superior competitive differentiation, customer experiences, and business outcomes in a converging world. Powered by 82,000+ talented and entrepreneurial professionals across more than 30 countries, LTIMindtree — a Larsen & Toubro Group company — combines the industry-acclaimed strengths of erstwhile Larsen and Toubro Infotech and Mindtree in solving the most complex business challenges and delivering transformation at scale. For more information, please visit https://www.ltimindtree.com/.