LTIMindtree

Whitepaper

Zero Trust

Elevating Cybersecurity in the Digital Age

Table of Contents

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 have yet to keep up with current tech advancements, and modern cyberattacks are emerging because of them.

Traditional cybersecurity approaches focused on securing the perimeter when organizations confined data and users to specific, well-defined locations.The perimeter-based security acted as the primary point for enforcing security controls. Once someone breaches this perimeter, they can access most resources. 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. An attacker can access the corporate grid without traversing the perimeter if a device is compromised. 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 make a system vulnerable. However, the effective implementation of zero trust is dictated by the harmonious coordination of legacy and 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 the digital age. As per our research, organizations must clearly understand their crown jewels, data assets, and workings of the zero trust framework to implement zero trust successfully. While organizations deliberate on their future course, we comprehensively analyze the value zero trust offers in this document. We highlight some of the most persistent obstacles regarding implementing the zero trust framework in the form of a skeptic's analysis. Forward-thinking organizations are focusing on integrating the elements of the 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 assumed without question or reservation. Relying solely on fortified corporate security boundaries and placing unwavering trust in everything within it has repeatedly proven flawed.

Zero trust operates around the “never trust, always verify” philosophy, 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 outside the corporate perimeter's confines. Also, due to the

emergence of public cloud platforms, devices and services once operated within the corporate perimeter are now being operated externally. Workloads are migrating toward 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 safeguarding their data, users, and customers with static defenses fails to empower businesses to fully embrace innovations like the cloud while 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)[ii]. There were 28,823 vulnerabilities documented in 2023, surpassing the 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 identifying vulnerabilities year after year.

Zero trust is crucial to mitigating 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 framework for effective security

To implement zero trust in your cybersecurity system, it is necessary to understand the zero trust security model. Zero trust security is an organizational framework designed to lower a corporate system's attack surface, reduce the risk of a data breach, and provide real-time threat detection and response capabilities. It assumes all traffic is untrusted and should be verified before accessing resources, offering a granular and contextual approach to access control. Data, identity, and infrastructure are the key principles, with automation and analytics acting as horizontal components, as shown below:

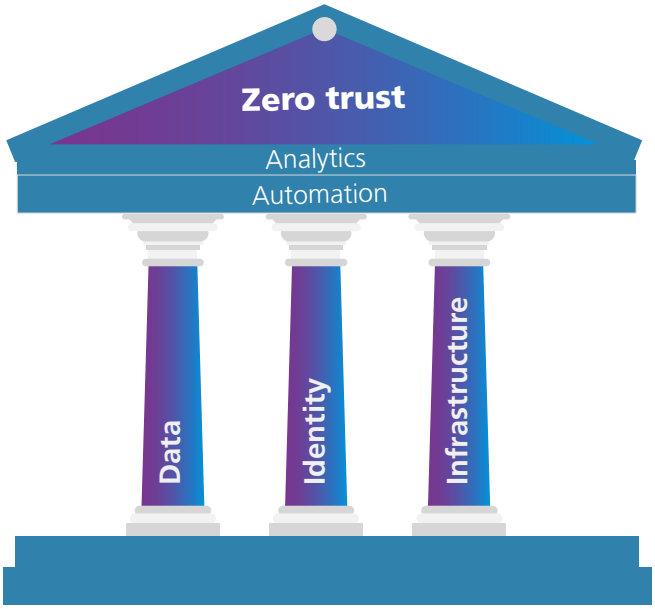

Figure 1: Pillars of zero trust security model

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 and 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 ZTA may vary as per organizational needs. However, the following technologies are essential for enabling zero trust.

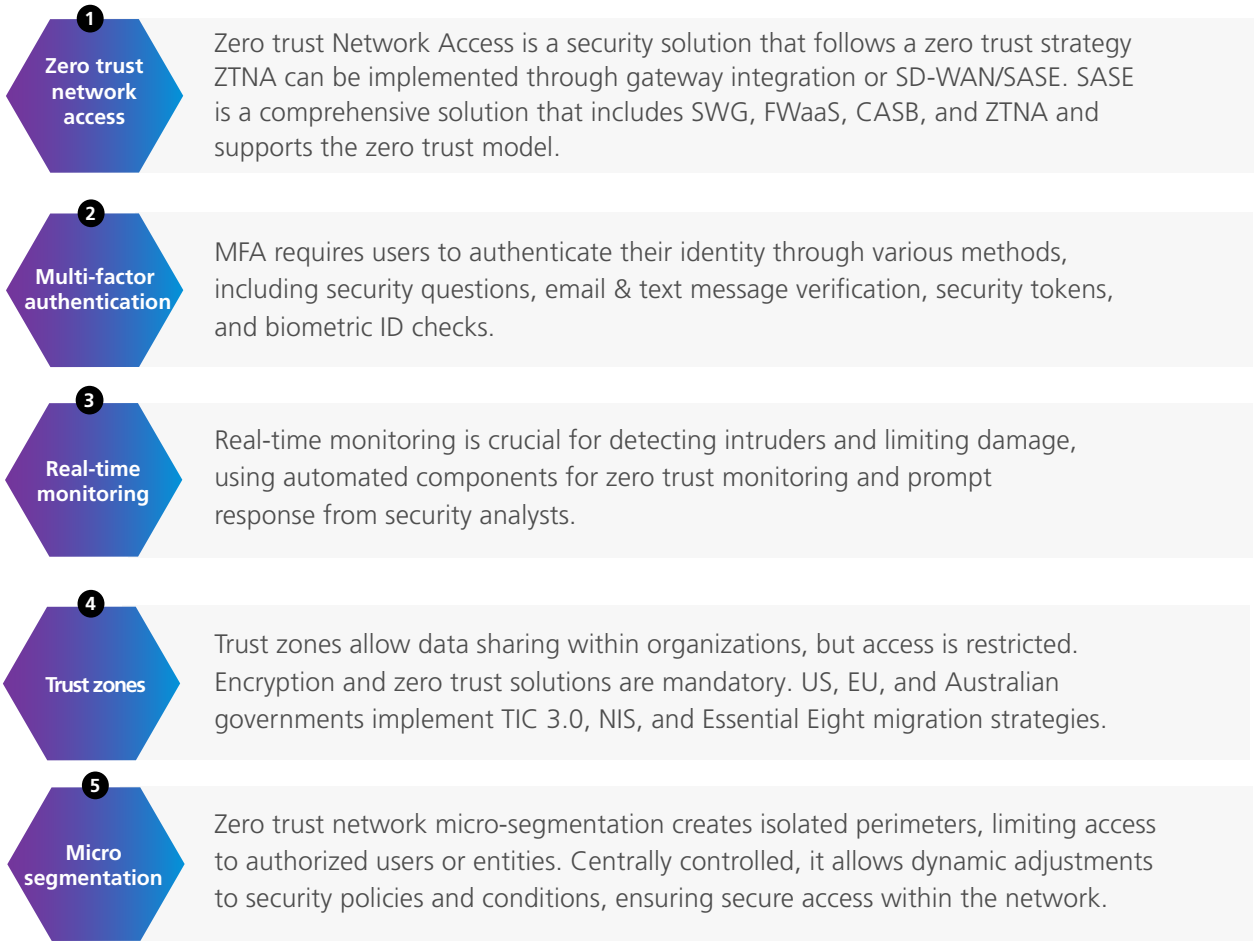

Figure 3: Zero trust components

Key recommendations before implementing ZTA

Implementing 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.

Multifactor 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 and 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

Implementing zero trust principles within the cloud services and SaaS platforms requires deploying cloud access security brokers (CASBs). These brokers serve as vigilant gatekeepers, monitoring and managing the exchange of information between identity, infrastructure, and cloud services. 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 Network Access (ZTNA). According to Gartner[iii], the adoption of ZTNA remains robust among organizations with over 25,000. 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[iv] 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 choose a vendor, security and risk management leaders should consider market presence, depth of security services, and the types 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 large, medium, and small categories. Zero trust market trends are shifting towards vendors offering enhanced Zero trust platform capabilities. Vendors are incorporating AI/ML functionalities to streamline security controls and improve the orchestration of security policies.

05 Key application areas

The main reasons for adopting zero trust are to support hybrid workforces, secure data traffic, prevent unauthorized lateral movement, simplify security costs, 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.

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.

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 and 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.

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), and Endpoint Detection and Response (EDR), etc.)

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

Zero trust is receiving much attention, with vendors touting its potential benefits. While not a cure-all, zero trust can align security with business practices, reduce risks, enhance agility, and lower operational costs. It requires support and dedication to realize these advantages fully. Zero trust frameworks streamline security tools, offering a unified solution that simplifies deployment and management while improving the user experience for auditing and reporting. Zero trust is gaining prominence due to increased remote workforces, cloud services, BYOD (Bring Your Own Device) policies, and decentralized information systems, making system and network protection challenging. Flexible deployment options enable organizations to implement key components of a reliable zero trust strategy.

Advantages and benefits

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 also ensures that 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, multi-factor authentication (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

Disadvantages and 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 (IT & OT) 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 leads to integration challenges between solutions.

Zero trust platforms 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 Skeptic's opinion

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, only 1% of large enterprises currently have well-established and measurable zero trust programs[iv]. However, there is optimism that this number will increase to 10% by 2026.

> We believe 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 Zero Trust Network Access (ZTNA) as a solution to overloaded VPNs. 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.

Type 1, being tactical, rarely yields the comprehensive benefits that zero trust can offer. We believe that a different approach is needed to fully leverage zero trust's potential.

08 Conclusion

Zero trust offers an enterprise's cybersecurity architecture framework to attain a security posture driven by risk, awareness of context, and adaptability. Implementing correctly, it 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 rising. 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 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 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 ensures 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.

09 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.

09 Citations

i. *Zero Trust Essentials eBook***,** Microsoft, Zero Trust essential e-book, Microsoft, 2022: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWIrfk

ii. *NIST, National Vulnerability Database, U.S. Department of Commerce, 2024:* https://nvd.nist.gov/vuln/search/statistics?form_type=Basic&results_type=statistics&query=vulnerability+data&search_type=all&isCpeNameSearch=false

iii. *Market Guide for Zero Trust Network Access, Gartner, August 14, 2023:* https://www.gartner.com/doc/reprints?id=1-2EPRREFB&ct=230815&st=sb

iv. *Gartner's new prediction about Mature and Measurable Zero-Trust Program, January 23, 2023:* https://www.gartner.com/en/newsroom/press-releases/2023-01-23-gartner-predicts-10-percent-of-large-enterprises-will-have-a-mature-and-measurable-zero-trust-program-in-place-by-2026

v. *Markets and Markets, Zero Trust Architecture Market, November 23, 2023:* https://www.marketsandmarkets.com/Market-Reports/zero-trust-architecture-market-207388489.html

vi. *Trust architectures and digital identity*, August 2022: https://www2.deloitte.com/uk/en/pages/risk/articles/zero-trust.html

vii. *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

viii. *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/ZeroTrust_vF.pdf

ix. *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

x. *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

xi. *Demystifying Zero Trust, SOPHOS, 2020:* https://www.sophos.com/en-us/whitepaper/demystifying-zero-trust

xii. *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

xiii. https://media.bitpipe.com/io_15x/io_158372/item_2560584/the-big-book-of-ztna-security-use-cases-.pdf

xiv. *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/

09 Glossary

- OEM – ORIGINAL EQUIPMENT MANUFACTURER
- SD-WAN - A SOFTWARE-DEFINED WIDE AREA NETWORK
- SASE - SECURE ACCESS SERVICE EDGE
- SWG – SECURE WEB GATEWAY
- FWAAS – FIREWALL AS A SERVICE
- CASB – CLOUD ACCESS SECURITY BROKER
- ZTNA - ZERO TRUST NETWORK ACCESS
- MFA – MULTI FACTOR AUTHENTICATION
- TIC – TRUSTED INTERNET CONNECTIONS
- NIS – NETWORK AND INFORMATION SYSTEMS
- SDN - SOFTWARE-DEFINED NETWORKING
- VPN – VIRTUAL PRIVATE NETWORK
- SSE – SECURE SERVICE EDGE
- PAM -PRIVILEGE ACCESS MANAGEMENT
- API - APPLICATION PROGRAMMING INTERFACE
- BYOD – BRING YOUR OWN DEVICE
- IT – INFORMATION TECHNOLOGY
- OT – OPERATIONAL TECHNOLOGY
- Y-o-Y- Year-on-Year

About LTIMindtree

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 81,000+ talented and entrepreneurial professionals across more than 30 countries, LTIMindtree — a Larsen & Toubro Group company — solves the most complex business challenges and delivers transformation at scale. For more information, please visit https://www.ltimindtree.com/.