WHITE PAPER

ZERO TRUST ARCHITECTURE DECIPHERED

Abstract

This whitepaper discusses the Zero Trust Architecture (ZTA) in a simplified manner so that it can be consumed by various stakeholders in an organization - right from a security analyst to a CXO. The architecture has been elaborated starting with its foundational principles to challenges organizations face while adopting ZTA tenets, ZTA maturity model and some of the recommendations. This paper also touches upon a high-level road map for organizations willing to adopt a Zero Trust design approach in a phased manner.

Infosys®
Navigate your next

Introduction

With accelerated digital transformations, remote work model and internet becoming newer channel for business communication, the typical organization's infrastructure has become increasingly complex and distributed. The legacy perimeter-based network security is not entirely relevant anymore. It is also proving to be insufficient to facilitate cyber protection as, once attackers breach the perimeter, further lateral movement is unstoppable. Identity has emerged to become very powerful for any organization in the new distributed environment that goes beyond the enterprise data center. This complex enterprise IT ecosystem has led to the advent or development of the next generation cybersecurity model known as **Zero Trust Architecture (ZTA).**

ZTA is a cybersecurity initiative that helps organizations to prevent data breaches & protect against next generation cyber threats by eliminating 'implicit digital trust' from the organizations IT ecosystem. Founded on the principle of "never trust, always verify", Zero Trust is a very well thought and efficiently designed cyber strategy that will ensure highest level of cyber protection for any organization. The Zero Trust strategy can be achieved by deploying off-the-shelf technologies and complemented by processes, procedures, policies with additional cyber solutions having capabilities around artificial intelligence and machine learning. Zero Trust is not directly related to amalgamation of technologies but remains a cybersecurity framework through which enterprises can derive their strategy and operational environment. So, while technologies change, enhance or get replaced over time, the foundational framework and enterprise strategy shall remain the same.

Evolution Of Zero Trust

The Defense Information Systems Agency (DISA) and the Department of Defense published their work on enterprise security strategy and dubbed it as "black core". Black core emphasized on moving from perimeter-based enterprise cybersecurity model to a new model which focused on the security of individual transactions. In 2004 **Jericho Forum** publicized the idea of de-perimeterization — limiting implicit trust based on network location and the limitations of relying on single, static cyber defenses over a large network segment. The concept of de-perimeterization evolved and improved into the larger concept of Zero Trust, which was later coined by **John Kindervag** while at Forrester in year 2010.

Zero Trust started to gain traction and recognition as a new d-facto standard of cybersecurity for enterprises. The term is used to describe various cybersecurity solutions that have moved security away from implied trust based on network location and instead focus on evaluating trust on a per-transaction basis.

On 12 May 2022, the US Federal Government notified an executive order to adopt security best practices, advance toward Zero Trust Architecture, accelerate movement to secure cloud services, including Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) & Container-as-a-Service; centralize and streamline access to cybersecurity data to drive analytics for identifying and managing cybersecurity risks; and invest in both technology and personnel to match these modernization goals. The executive order further states that each federal agency shall develop a plan to implement Zero Trust architecture, which shall incorporate, the migration steps outlined by NIST in standards and guidance. As agencies continue to use cloud technology, they shall do so in a coordinated, deliberated way that allows the Federal Government to prevent, detect, assess, and remediate cyber incidents. To facilitate this approach, the migration to cloud technology shall adopt Zero Trust architecture.

Need For Zero Trust Security

Secure by design, which mandates cybersecurity as built-in solution than bolted in later, is one of the major reasons for organizations to acknowledge the need for Zero Trust architecture. Secure by design emphasizes on preventing a cyber breach proactively rather than repairing and restoring enterprise IT systems after they have been hit by a cyber breach. Zero Trust architecture is one of the models which is required to keep the pace with evolution of advance cyber threats and new attack surface due to digitization. Following are some of the key reasons to have a robust Zero Trust architecture.

- Evolution of enterprise networks from small-scale, highly controlled and contained environments to decentralized architectures
- Traditional perimeters are complex and no longer compatible with current business models based on digital
- Advance and sophisticated cyber-attacks to exploit these distributed networks
- "Trust but verify" principle is no longer an alternative but has become an essential
- Targeted & advanced threats moving from outside to inside the corporate perimeters
- Thumb rule of "least privilege" to be extended from one time measure to per request access decisions on the face of a network viewed as already compromised

Key Principles of Zero Trust

Against the backdrop of rapid digitization, Zero Trust architecture has become essential to ensure cyber protection for organization's digital assets is fool proof. While there are multiple definitions of Zero Trust architecture depends on who is defining it, a security product OEM, a federal agency, an analyst, a security service provider, or a security advisory firm however we believe Zero Trust principles are the right foundation on which it can be well defined. Zero Trust architecture must be aligned with the fundamental principles which can be foundational pillar of next generation cybersecurity strategy, design and operating model. Following are the Zero Trust architecture principles

- Least Privileged
- Assume Breach
- Verify Explicitly
- Context Aware Access
- Data Centric Security
- Protection Against Lateral Movement

Least Privilege

The principle of least privilege has always been a guiding principle in an enterprise identity & access management domain. The principle focuses on a security concept where a user is given minimum levels of entitlement or access needed to perform their job. Zero Trust architecture re-emphasize on this principle so that attack surface can be minimum. Principle of least privilege reduces the risk of attackers gaining access to critical systems or sensitive data by compromising an account, device, or application. Privilege itself means authorization to bypass certain security restraints as per enterprise policies. Applying principle of least privilege implies enforcing minimal level of rights, or lowest clearance level, that allows the user to perform his/her role. It also applies to processes, applications, systems & devices (such as IoT), where each should have only certain permissions required to perform an authorized activity. Implementing this principle helps condense attack surfaces, contain compromises to their area of origin and stops them from spreading to the larger ecosystem. This can simplify to achieve, and prove compliance needs as well.

Assume Breach

One of the most fundamental principles of Zero Trust is "assume breach". The traditional approach of "trusted insider" and "untrusted outsider" has been overridden by this principle. It does not assume everything behind the corporate firewall is safe. Zero Trust model assumes cyber breach and verifies each request irrespective of the origination from inside or outside the enterprise network. In this way, enterprises can have sufficient cyber protection for every kind of access from anywhere.

Verify Explicitly

Implicit trust is one of the default approaches traditionally followed by cyber system where once a user is created and authenticated with a certain access level, is not challenged, if the right (legitimate) person is using the authentication method subsequently or right level of access he has received. Zero Trust model, regardless of request origination location, or what resource the request accesses, emphasizes to never trust, always verify. Every access request must be fully authenticated with additional authentication methods (conditional access) authorized (sometime in time bound manner only) before granting access.

Context Aware Access

Zero Trust architecture has been created to address next generation cybersecurity challenges thus context-aware access principle becomes very important considering the enterprise IT ecosystem is no longer residing inside the organizational physical boundaries. Context aware access principle provides enterprises the control over which application, user can access based on their context. For example, whether their device complies with enterprise security policy, whether user is trying to access from an unknown location with more vulnerable internet browser etc.

Data Centric Security

Various cybersecurity models have been followed from the day of acknowledging cyber protection for IT systems. With rapid dependency on IT systems for every enterprise and enterprise data becoming so significant as a digital asset, Zero Trust model subscribe the principle of data centric security rather than perimeter centric security. This Zero Trust principle states that cybersecurity controls, processes and policies must be designed based on criticality of the data instead of having one size fit all solutions. Data classification thus becomes very critical to follow data centric security principle.

Protection Against Lateral Movement

Lateral movement is a technique that adversaries or intruders use after compromising an enterprise endpoint machine and extending the access to other machines or applications. The legacy cybersecurity designs focused on perimeter security heavily looking into north south traffic (outsider > inside) for threats. These designs have not considered cyber protection within the same subnet and largely considered internal network as trusted by default.

Zero Trust model focuses on protection against lateral movement as a foundational principle as these are difficult to detect because it is not easy to differentiate between legitimate and malicious network traffic.

Enterprise Challenges in Adoption of ZTA

With adoption of Zero Trust strategy, to highly improve cyber resiliency and protection, multiple notches have been widely acknowledged across enterprises but there are multiple challenges in executing it on ground. Some of these challenges are

- Enterprises IT ecosystem has been built on legacy systems which are designed and rely on "Implicit Trust" principle. This is fundamentally against the foundational Zero Trust principle of "verify explicitly". Some of these systems and applications will need full revamp to comply with zero trust model.
- It needed significant investments to rebuild or replace Zero Trust aligned IT infrastructure from the existing legacy systems
- At one side Zero Trust architecture is becoming the new de facto across enterprises and at other side there is no consensus on formal adoption of Zero Trust architecture across industries
- The current Zero Trust architecture adoption is focused on either network layer or identity layer. There is lack of holistic approach to address Zero Trust as whole.
- One of the common challenge enterprises are facing while envisioning Zero Trust architecture adoption is having varied definition & security control matrix. There are multiple Zero Trust architecture recommendations based on Original Equipment Manufacturers (OEMs) own solutions coverage. Those definitions are aligned to the OEMs solution coverage which is an issue as an OEM might not have wholistic coverage from Zero Trust architecture perspective.

Defense in depth approach of cyber security design has been basis for most of the organizations' cybersecurity systems. Zero Trust further enhances and complements it to meet the new cyber challenges. Therefore, organizations opting to adopt Zero trust must consider that defense in depth approach will still needed with Zero Trust taking it further.

Zero Trust Security Framework

The diagram below encapsulates Zero Trust Architecture framework that could be referred by enterprises looking to adopt a comprehensive ZTA program for their IT environments. While as stated above, Zero Trust architecture must be based on the fundamental principles however, as per various definitions ZTA has 5 key sub domains which are essentials to be looked at from the perspective of readiness against any next generation threats. Those 5 key tenets highlighted in the below architecture are

- Secure Identity
- Secure Device
- Secure Applications
- Secure Networks
- Secure Data
- Cyber Governance

In this paper we have tried to cover all the tenets of ZTA and associated security controls which are needed to adhere with ZTA security model however there can still be a lot many controls, processes, policies enhancement needed based on customers IT footprint and threat appetite. We have focused majorly on the critical and prominent security controls only for this reference architecture. Zero Trust maturity can be attained without enhancing security processes, policies, and procedures however the reference architecture is majorly focused on the technology or control domain only.

Secure Identity

Secure Identity infers how the ZTA principle of Least Privilege, Verify Explicitly and Context Aware Access shall be followed with the help of various identity and access management security solutions. In the current scenario where internet has almost become the primary transport medium for enterprises, Identity has become most powerful therefore can be considered the new perimeter for cyber design. Identity is the most critical tenets of ZTA therefore security controls like conditional access based on device security posture, location & behavior identity protection based on user behavior analytics AI & ML based Cloud Infrastructure Entitlement Management (CIEM) are some of solutions which are recommended to achieve Zero Trust maturity.

Secure Device

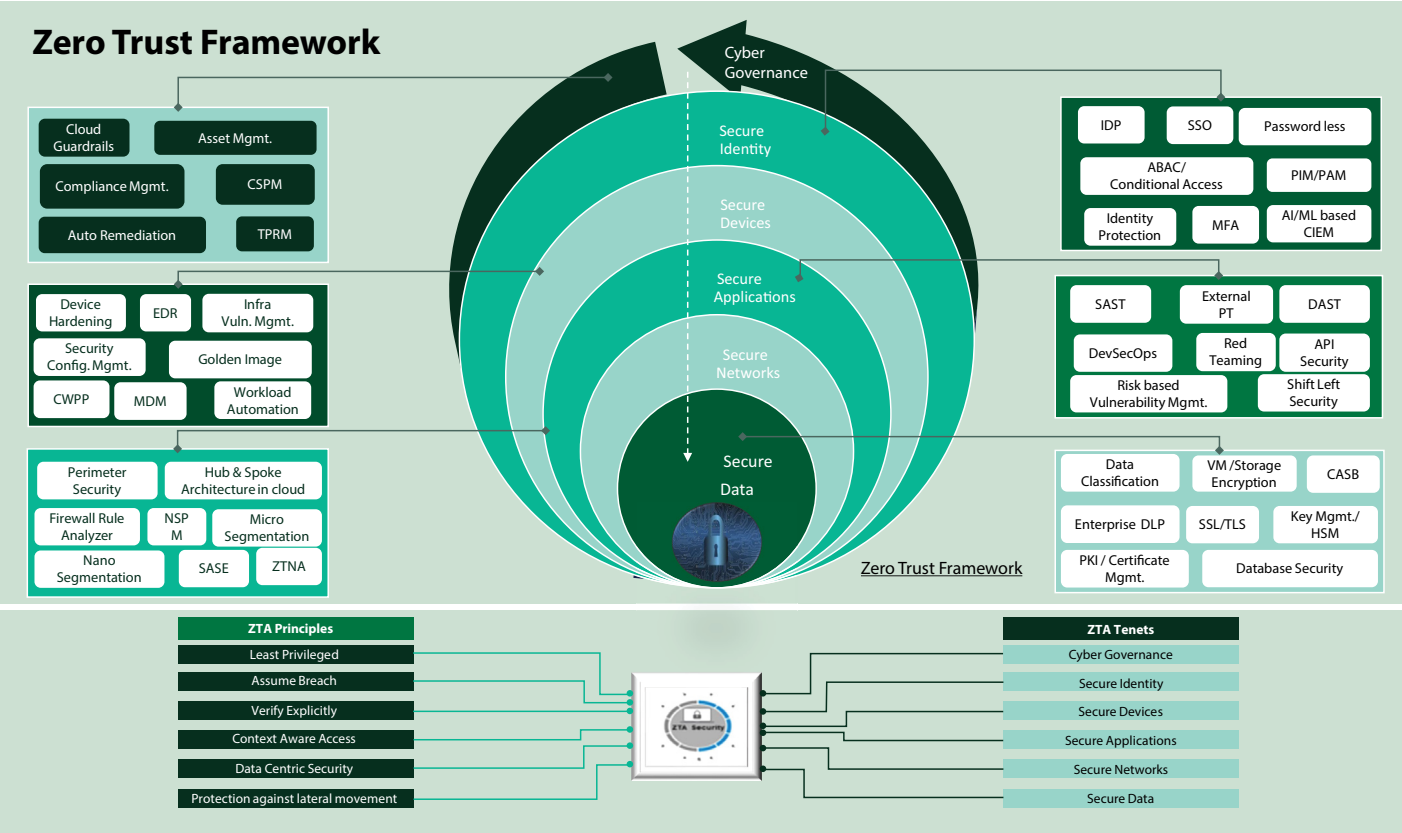
With secure remote access emerging, one of the enterprises need for their business to operate, secure devices become key focus area. ZTA principle of Protection Against Lateral Movement, Verify Explicitly, Data-centric Security all comes in a play while deriving device security solutions. Security solution like compliance management through hardening, vulnerability management, golden image, Cloud Workload Protection Platform (CWPP) are some foundational controls. For devices to adhere to Zero Trust architecture, incorporating advance security solutions like shift left (CI/CD) approach in cloud workload automation, Extended Detection & Response (XDR) & enterprise mobile device management are additional controls must be considered.

Secure Applications

Zero Trust architecture is not complete without contextualizing secure enterprise applications in it. All the six Zero Trust principles are applicable for enterprise applications. Enterprise strategy of migrating from conventional monolithic to cloud native applications, micro services and containers has added DevSecOps as a key tenets of secure application development. Agile approach of application development further accelerates to adopt the shift left approach of security through various application security solutions in the DevSecOps life cycle. Risk- based application vulnerability management, Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST) and container & API security are some of the controls must be part of the Zero Trust secure application tenets.

Secure Networks

While identity has become focal point for the enterprise cybersecurity design due to digitalization, usage of cloud services, cloud apps, network and infrastructure still are the very important tangent. Zero Trust principles of Assume Breach, Protection Against Lateral Movement and Context Aware Access leads to secure network & infrastructure for enterprises through various controls. The basic controls of perimeter security, hub & spoke model in distributed cloud environment to advance controls like firewall rule analyzer, nano / micro segmentation, Zero Trust Network Access (ZTNA), Secure Access Service Edge (SASE) does create the secure network and infrastructure aligned to Zero Trust architecture.



Secure Data

Data is one of the most important assets for enterprises in this digital era.

Protecting it from unauthorized access or leakage to internal or external users can have humongous business and brand impact. Sensitive or compliance specific data leakage of the enterprises can result in financial loss, reputational harm, consumer trust degradation, and brand erosion. It shall also impact the regulatory penalties depending on the domain of the business, geography & country etc. One of the major shifts from conventional to Zero Trust approach is to follow data centric security rather than "perimeter-based security. To follow data centric security, data classification becomes one of the foundational elements so that based on sensitivity the data security controls can be designed and deployed. Using data leakage prevention for devices, emails, files, folders, cloud apps, cloud storage along with encryption, PKI, key management are some of the essential data security solutions. API security, database activity monitoring, security masking, tokenization, secure data disposal etc. are custom solutions enterprises need to have depending on compliance and data security requirements

Cyber Governance

Apart from secure applications, cybersecurity governance is one of the overarching constructs which shall provide strategic view of how efficiently an organization's zero security controls, processes, procedures, risk & compliance management are working. Setting up enterprise security policies i.e., cloud security guardrails to create the secure landing zone for a distributed cloud environment having multiple subscriptions, or accounts is one of the solutions under cyber governance specially for the hybrid or multi cloud environment. Cloud asset inventory management on a real time basis, misconfiguration management and auto remediation are some of the other security elements must be considered part of the Zero Trust architecture. Compliance management for the enterprise is one of the regulatory requirements must be met for Zero Trust to achieve regulatory adherence.

Zero Trust Adoption Methodology

Zero Trust is not a destination but a journey where the enterprise Zero Trust maturity can be enhanced from cyber exposed stage to cyber resilient. We suggest before taking the path of Zero Trust enterprise should first do the evaluation of their cybersecurity systems including technology, processes & policies to determine what is the current zero trust maturity level. Once the evaluation or an assessment has been conducted next stage is incubation. Wherein the Zero Trust concept must be followed to implement by creating Zero Trust test beds across on premise or hybrid/multi cloud environment. The lessons from incubation stage must be applied on to further resources of greater business importance. The next stage is prototype which includes rolling out Zero Trust strategy to build and implement Zero Trust aligned solutions for a particular department or business function e.g. Implementing a SASE, ZTNA, CIEM, CSPM, micro segmentation, conditional access etc. The lesson learnt from this smaller deployment than must be percolated to across the enterprise covering all six tenets of Zero Trust architecture.

Zero Trust Maturity Model

Enterprises are very keen to adopt Zero Trust however with varied definition and understanding, it is challenging to understand where their current Zero Trust maturity lies. The below table has covered some of the Zero Trust tenets and the maturity level with consideration of various parameters. This maturity model is based on ground level working experience, the research we have done based on already available text from analysts, government agencies & OEM. The maturity model has four stages from Level 0 to Level 3 which can be defined as cyber exposed level to cyber resilient stage. The highest level of Zero Trust maturity state be called as self learning & risk behavior-based continuous optimization having focus on predictive/ AI+ML based policy recommendation based on self-learning and suggests auto remediation based on the learning rather than static policy definition. This is fifth stage of Zero Trust where the industry shall reach with greater evolution not only from technology perspective but the way we operate the technology.

There can be multiple parameters to assess the Zero Trust maturity and the below table is to highlight how some of these maturity stages reach to cyber resilient state.

ZTA Maturity					
S.N.	**ZTA Domain**	**Maturity Level 0**	**Maturity Level 1**	**Maturity Level 2**	**Maturity Level 3**
1	Secure Identity	Legacy authentication in use without 2nd factor	Legacy authentication in use with 2nd factor	Nextgen authentication in use with 2nd factor	NextGen authentication in use with context aware 2nd factor
2	Secure Identity	Access reviews are not done	Access reviews are done manually and periodic	Periodic tool-based access reviews without any AI/UEBA capability	Realtime tool-based access reviews (CIEM) with AI/ML/UEBA engine
3	Secure Identity	No risk measurement of identities	Manual risk measurement, limited to privileged users	Automated risk measurement, limited to privilege users	Automated risk measurement covering all the Identities, visibility of Identity risk score & attack surface dashboard based on predictive analysis
4	Secure Data	No data classification is in place	Data classification limited to non-structured data within enterprise data center	Data classification limited to non-structured data covering on-premises, cloud storage, Cloud Apps etc.	Data classification covering all kind of data (structured & non- structured) covering on-premises, cloud storage, cloud apps, cloud database etc.
5	Secure Data	No data leakage protection solution in place	Data leakage protection is available but limited to emails and web only	Data leakage protection is available for emails, web, USB, printer, cloud storage, cloud apps etc.	Data leakage protection is available for emails, web, USB, printer, cloud storage, cloud apps & structured data (DB, Big data, cloud services, cloud database etc.)
6	Secure Data	Access governance has not associated with data sensitivity	Access governance is associated with data sensitivity but only applicable for limited set of data	Access governance is associated with only "restricted classified "data as per company categorization	Access decisions governed by data sensitivity for all kind of classified data
7	Secure Data	Companies does not encrypt application traffic	Companies explicitly encrypts only critical internal applications traffic	Companies encrypts all traffic to internal applications, as well as some external traffic	Companies encrypts all traffic to internal and external facing irrespective of the business criticality
8	Secure Networks	No secure remote access solution in place	Legacy secure remote access in place without any 2nd factor authentication	Legacy secure remote access in place with 2nd factor authentication	Zero Trust Network Access (ZNTA) solution with 2nd factor authentication with no direct connection in enterprise network

9	Secure Networks	Network segmentation is only for north south traffic based on F/W access list etc.	Network segmentation is based on subnets utilizing firewall & other network security services	Micro segmentation solution is available however coverage is limited to few critical network zones	Micro segmentation solution and strategy in place to protect lateral movement via east west traffic for the entire IT landscape (DC, Cloud etc.)
10	Secure Networks	Companies baselines their threat protections primarily on some of the known threats and static traffic filtering	Companies baselines their threat protections primarily on all known threats & static traffic	Companies includes basic analytics to proactively discover threats	Companies integrates machine learning-based threat protection and filtering with context-based signals
11	Secure devices	Legacy signature-based endpoint security solution is in place	Nextgen endpoint security solution with UEBA/ML capability w/o EDR	Nextgen endpoint security solution with UEBA/ML capability with EDR but without integration between EPP/EDR	Integrated Endpoint Protection (EPP) & Endpoint Detection And Response (EDR) solutions covering across endpoints, cloud workloads and using the AI/ML/UEBA capabilities
12	Secure devices	No mobile device management for internal, external or BYOD systems	Mobile device management solution with compliance and IT configuration policies	MDM granting access to enterprise network for external or BYOD systems which are compliant with IT configuration policies	Mobile device management for all systems (internal, external, BYOD etc.) enforcing policy to grant access to enterprise networks only after meeting IT configuration policies & risk score
13	Secure devices	Incomplete device asset inventory without endpoint vulnerability management	Complete device asset management in place but no vulnerability management for endpoint devices	Complete device asset management in place & vulnerability assessment for endpoint devices being done regularly	Endpoint device inventory for complete life cycle & integration done with vulnerability management solutions. Regular vulnerability remediation & governance for endpoint in place.
14	Secure devices	Organizations have no visibility into device compliance against baseline or industry standard	Organizations have limited visibility into device compliance against enterprise baseline or industry standard	Organizations have put compliance enforcement mechanisms for most devices against enterprise baseline or industry standard	Organizations always monitors and validates device security posture using analytics & AI/ML algorithms
15	Secure application and Governance	No secure SDLC processes, policies and controls	Only Dynamic Application Security Test (DAST) is being conducted	Dynamic Application Security Test (DAST), Static Application Security Test (SAST) and penetration test being conducted following Secure SDLC	DevSecOps method of agile application development with security integrated in CI/CD pipeline covering SAST, DAST, PT, vulnerability for cloud automation templates
16	Secure application and Governance	Cloud security governance for limited set of subscriptions/ accounts through native solution based on criticality	Cloud security governance for all subscription/accounts through native solution based on criticality	Cloud security governance for all the subscriptions/ accounts through CSPM solution providing visibility, auto remediation, compliance management kill chain, threat intelligence etc.	Cloud security governance for all the subscriptions/accounts through 2nd generation CSPM providing integrated view of misconfigurations, identity, cloud assets, compliance, data criticality, kill chain using AI/ML
17	Secure application and Governance	Some critical on-premises DC applications are directly and securely accessible to users over the internet, with all others available through a Virtual Private Network (VPN)	Some critical on-premises & some critical cloud applications are directly & securely accessible to users over the internet, with all others available through a VPN	All cloud applications and some on-premises applications are directly & securely accessible to users over the internet, with all others available through a VPN	All applications are directly and securely accessible to users over the internet
18	Secure application and Governance	Access to applications is primarily based on local authorization and static attributes	Some application access with local authorization and critical apps through centralized authentication	Access to applications relies on centralized authentication, authorization, monitoring, and attributes	Organizations continuously authorizes access to applications, considering real-time risk analytics

Conclusion

Zero Trust is a forward looking path-breaking cybersecurity model for business to make them cyber resilient. In a simplified manner the 6 principles and Zero Trust tenets where its applicability is elaborated above must be looked upon as foundational pillars to understand if a particular technology, process, design, or an architecture is aligned with Zero Trust or not. Zero Trust is essentially a journey enterprise are moving in but to first understand their current Zero Trust maturity level and then define the roadmap in various maturity stages is the only way forward.

About the Author

Darshan Singh
Principal Consultant having rich experience in cybersecurity domain of more than 17 years

He is currently a part of the Infosys Cyber Innovation, Strategy & Excellence Team which dwells into next generation cybersecurity solutions and strategies. In his earlier role he was heading the delivery of Cloud Security & Emerging Technologies Security. Darshan has versatile experience in multiple subdomains of cybersecurity i.e. in the field of cloud security, infrastructure security, data security, OT security, vulnerability management, security monitoring & analytics etc. Darshan is an engineering graduate from the College of Engineering Roorkee.

References

1. https://www.forrester.com/blogs/the-definition-of-modern-zero-trust/
2. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWJJdT
3. https://docs.microsoft.com/en-us/security/zero-trust/
4. https://www.securityforum.org/solutions-and-insights/demystifying-zero-trust/
5. https://csrc.nist.gov/publications/detail/sp/800-207/final

For more information, contact askus@infosys.com

Infosys®
Navigate your next