Volume: 10 Issue: V Month of publication: May 2022

DOI: https://doi.org/10.22214/ijraset.2022.42976

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue V May 2022- Available at www.ijraset.com

A Zero Trust Framework Security to Prevent Data Breaches and Mitigate the Cloud Network Attacks

Ms. Divya P[1], Sherin Sithara. A[2]
[1]*Assistant Professor, Nehru College of Engineering and Research Centre*
[2]*Department of MCA, Nehru College of Engineering and Research Centre*

Abstract: Due to new modes of communication, we have seen a surge in the use of wireless networks in recent years. Online safety has become a contentious issue in the community. People want to be able to access all of your applications and resources at any time and from any location. As the use of cloud computing and the Internet of Things grows, so does the number of linked devices, increasing the number of cyber crime targets. A simple shift in mindset can help secure data and the network as a whole. This article defines a Zero Trust Network and illustrates some of the concepts that underpin this architecture/philosophy. Everything inside or outside the network is not reliable unless it is confirmed, according to the Zero Trust design. Zero Trust is a sophisticated security approach in which all users, both inside and outside an organization's network, must be authorized, authenticated, and validated of their security posture and configuration on a continuous basis before being granted access to the network, data, and applications. To validate a user's identity while ensuring tight security, this strategy employs high-end security technologies such as multi-factor authentication, next-gen endpoint security, and identity & access management.

Keywords: Cyber security, Zero Trust Network,logical components, security solutions, Google Beyond Corp.

I. INTRODUCTION

Zero Trust is a framework for approaching cyber security from a different viewpoint. Based on the fundamental assumption of "never trust, always verify," Zero Trust shifts security management away from the traditional perimeter-based approach to one in which trust is built between specific resources and consumers as and when needed. Internal and external elements are used to determine trust, which is regularly re validated. The term "zero trust" was coined by Stephen Paul Marsh in April 1994 after his thesis on computational security at the University of Stirling.Zero Trust frees IT by removing burdensome and expensive security measures, allowing businesses to construct a more dynamic, efficient, and customer-focused IT platform. Zero Trust tries to propagate the idea that, even if connected to their corporate LAN or previously authenticated, companies should not trust devices or users by default. For zero trust to be effective, organisations must employ complete information security and resilience strategies. A ZTA can guard against common threats and enhance an organization's security posture by employing a managed risk approach when combined with existing cybersecurity policies and guidelines, identity and access management, continuous monitoring, and best practises.It is based on real-time visibility into user attributes such as user identity, firmware versions, endpoint hardware type, OS versions, vulnerabilities, patch levels, user logins, installed programmes, incident detections, and so on. Zero Trust is becoming increasingly well-known as a result of its strong security capabilities, and corporations have begun to adopt it, including Google's BeyondCorp initiative. According to a research, the global market for Zero Trust security would increase at a CAGR of 17.4 percent from US$ 19.6 billion in 2020 to US$ 51.6 billion in 2026. Zero Trust Application Access (ZTAA), Zero Trust Network Access (ZTNA), Zero Trust Identity Protection (ZTIP), and other Zero Trust Access terms are commonly used.

A. Network Topology

Companies were initially more "isolated" with the introduction of the first computer systems, which reduced the frequency of attacks by focusing on their efforts to restrict access solely within the company by hierarchical levels. Since then, safety models have centred on deploying layers of protection to create digital perimeters to separate "trusted resources" from "untrusted resources. "Traditional perimeter security relies on firewalls, VPNs, and web gateways, which must deal with employee skill shortages, overburdening, and an ever-increasing number of cloud apps and mobile devices, all of which enhance cyber criminals' attack surface. These boundaries have been obliterated as cloud computing and the internet of things have grown in popularity. What we can say is that the traditional approach is no longer viable. With that strategy, no matter how much we invest in our company's cybersecurity, new and more sophisticated assaults are launched against our defences, thus we must view cybersecurity as a requirement rather than an investment over time. Because of the ever-growing universe of connected people, cybercrime targets are expected to increase significantly.

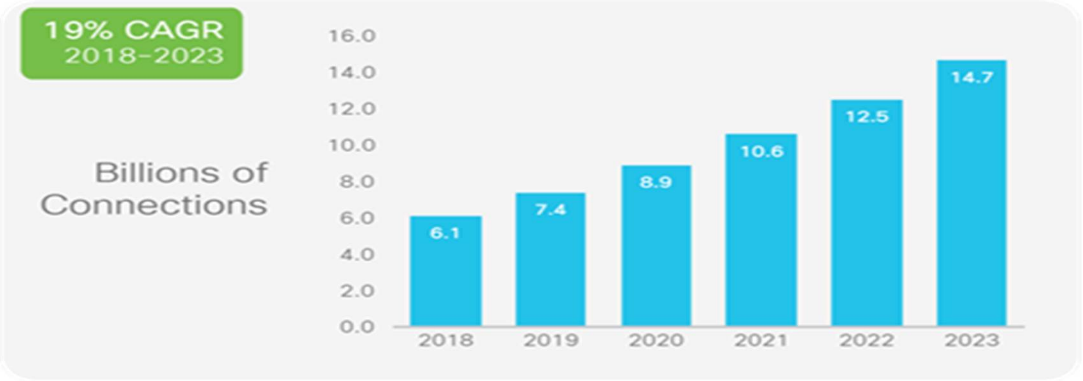

Figure1: connections in global population

B. *Cyber Security*

Cybersecurity strives to safeguard and secure information from a variety of perspectives, including social, political, and personal. Cyber-attacks appear to be gaining a greater grip on the world as time passes, and recent occurrences of data breaches and ransomware notwithstanding cybersecurity raise major concerns.Cyber attackers have a distinct set of skills and tools at their disposal, making it their duty to identify computer security dangers and weaknesses not just in technology but also in human behaviour. Cybersecurity is a constantly evolving scene, with new technologies emerging on a daily basis, offering chances for hackers who are always seeking for new methods to abuse individuals and organisations alike.

Cyber threat can take various forms; these are a few of the most common:

1) Malware refers to harmful software programmes in which a hacker employs a file or programme – such as a worm, virus, spyware, or trojan horse – to harm a user's system or to proxy illicit acts.
2) Ransomware is a sort of Malware that encrypts a victim's computer system and data and demands money to unlock them.
3) Social engineering is the use of human behaviour to deceive a user into violating a company's security measures, disclosing sensitive information such as logins or passwords.
4) Phishing is a sort of fraud in which a user gets a false email that appears to be from a trustworthy source, with the purpose of stealing personal information such as login credentials or credit card information.
5) DDoS (Distributed Denial-of-Service) attacks occur when thieves temporarily disable a device or network resource by flooding the victim with requests from various sources, so overloading the system. The goal is to keep regular consumers from doing business with the company

II. LITERATURE SURVEY

Romans Vanickis, Paul Jacob, Sohelia Dehghanzadeh, Brian Lee researched on Access Control Policy Enforcement for Zero-Trust-Networking[1]: define a policy enforcement framework to handle several of ZTN outstanding problems for risk-based access control develop the needed policy languages, including a general firewall policy language for expressing firewall rules Create a method for mapping these rules to particular firewall syntax and installing them on the firewall[1]. With a tiny proof-of-concept, we may demonstrate the feasibility of our idea.The uncertainty caused by such dynamicity adds to the unpredictability in the access control process, emphasising the requirement for risk-based access control decision making. As a result, the old perimeter-based security paradigm is progressively being replaced with "zero trust networking" (ZTN)[1]. ZTN networks are segmented into zones, with varying levels of trust required to access zone resources based on the assets secured by the zone. All sensitive information access is subject to strict access restriction based on user and device profile and context.

Nikolaos Papakonstantinou, Douglas L.Van Bossuyt, Joonas Linnosmaa, Britta Hale, Bryan O'Halloran discussed in the concept of Zero Trust Hybrid Security and Safety Risk Analysis Method[2]. They presented using a fictitious case study of a spent fuel pool cooling system. The case study findings revealed that integrating security and safety increased the total risk of losing one important system component when compared to merely considering safety incidents.Calculating security-related probability is a dynamic and challenging procedure that is significantly influenced by the domain and present global security climate[2].The Zero Trust paradigm is used, which states that all people, whether internal or external to the system, represent a security risk. The evaluation of security-related probabilities allows for the calculation of a combined safety and security overall risk for the possibility of losing certain essential components or safety functions.

Christoph Bucka, Christian Olenbergerb, André Schweizerc, Fabiane Völterd, Torsten Eymanne discussed on the concept of Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust: substantial contributions to the area by giving fresh insights on zero-trust in a methodical manner To assist scholars in this endeavour, we intend to synthesise current information concerning zero-trust and identify gaps in the literature. As a result, we perform a multivocal literature review, examining both academic and practical publications. Because of its promise to meet difficult new network security needs,zero-trust is gaining traction in both research and practise. Despite its benefits over traditional methods, zero-trust has struggled to replace established systems.

William R. Simpson,Kevin E. Foltz made researched on Resolving Network Defense Conflicts with Zero Trust Architectures ,This research investigates a formulation that permits continuous communication while fulfilling network defence inspection and reporting requirements.

This work is a component of a larger security architecture known as the Enterprise Level Security (ELS) framework. In contrast to an end-to-end paradigm in which recognised good entities can communicate directly and no other entity has access to content until it is offered to them. Many emerging processes, such as distributed computing, endpoint designs, zero trust architectures, and enterprise level security, require end-to-end encrypted communication. The keys used for authentication, secrecy, and integrity exist only with the endpoints in an end-to-end paradigm. This research investigates a formulation that permits continuous communication while fulfilling network defence inspection and reporting requirements. This work is a component of a larger security architecture known as the Enterprise Level Security (ELS) framework.

Dayna Eidle, Si Ya Ni, Casimer DeCusatis, Anthony Sager discussed on Autonomic security for zero trust networks it describes Identity management with automated threat response and packet-based authentication were integrated with dynamic management of eight different network trust levels in testing. To coordinate and integrate threat response from firewalls, authentication gateways, and other network devices, we developed log parsing and orchestration software that works with open source log management tools. Threat reaction times are measured and proved to be significantly faster than traditional approaches. There has always been a demand for better cybersecurity through automation of threat signature detection, categorization, and response. Based on the Observe, Orient, Decide, Act (OODA) paradigm, the experimental test bed represented the building blocks for a proposed zero trust cloud data centre network.

III. METHODOLOGIES

A. Objectives

1) Verification is continuing. Always, always, always verify access to all resources.
2) Reduce the blast radius. If an external or insider breach occurs, minimise the impact.
3) Collect and respond to context automatically. For the most accurate response, incorporate behavioural data and obtain context from the complete IT stack (identity, endpoint, workload, etc.).

B. Proposed Methodologies

1) *Continues Verification:* At any time, there are no trusted zones, credentials, or devices due to continuous verification. As a result, the phrase "Never Trust, Always Verify" has become popular. Because continuous verification is required for such a large number of assets, several critical pieces must be in place for this to work effectively:

➢ Conditional access depending on risk. This ensures that the workflow is only disrupted when risk levels change, allowing for continuous verification without compromising the user experience.
➢ Rapid and scalable deployment of dynamic policy models. Because workloads, data, and users move frequently, the policy must account for not only risk, but also compliance and IT needs. Organizations are nevertheless subject to compliance and organizational-specific standards even if they have zero trust.

2) *Set a Blast Radius Limit:* If a breach does occur, it is vital to minimise the damage. Zero Trust restricts an attacker's credentials or access paths, giving systems and people time to respond and neutralise the attack.

➢ Using identity-based segmentation to limit the radius. Because workloads, users, data, and credentials change often, traditional network-based segmentation can be difficult to maintain operationally.
➢ Principle of least privilege. It is vital that all credentials, including those for non-human accounts (such as service accounts), have access to the minimum capacity required to accomplish the operation. The scope of work should change as tasks change. Many attacks take use of privileged service accounts, which are rarely checked and frequently have excessive permissions.

3) *Context Collection And Response Automation:* More data can help you make more effective and accurate judgments if it can be processed and acted on in real time. NIST offers advice on how to use data from the following sources:

- User credentials — human and non-human
- Workloads, including virtual machines, containers, and hybrid deployments
- Any device used to access data is referred to as an endpoint.
- Network
- Data

C. Pillars of ZTA

The zero trust paradigm has been adopted by industry and security professionals as a good strategy to secure businesses. The ZTA pillars presented in this guide are a synthesis of numerous Zero Trust security models now in use by top industry suppliers and academic sources. security models include five to seven pillars. In order to facilitate an investigation, GSA selected to symbolise a mix of distinct pillars from an acquisition standpoint. Each pillar is described in detail in the table below. Summaries the six pillars of a zero trust security approach that are built on a foundation of data:

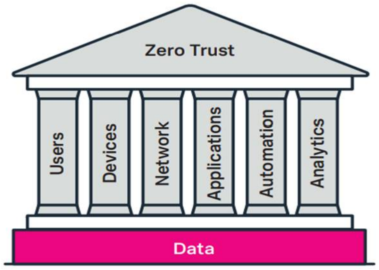

Figure 2: six pillars of zero trust security model

1) Pillar #1 - Users People/Identity Security

The continual authentication of trustworthy users, as well as the monitoring and validation of user trustworthiness in order to manage their access and rights.ZT prioritizes ongoing authentication of trustworthy users. This includes using technologies such as Identity, Credential, and Access Management (ICAM) and multi-factor authentication to regulate user access and rights, as well as continually monitoring and confirming user trustworthiness. Traditional web gateway solutions, for example, are vital for safeguarding and protecting user interactions.

2) Pillar #2 - Devices Device Security

Measuring the cyber security posture and trustworthiness of devices in real time.A ZT approach's basic feature is real-time cybersecurity posture and device trustworthiness. Mobile Device Managers and other "system of record" solutions give data that might be relevant for device-trust evaluations. In addition, for each access request, further evaluations should be performed.

3) Pillar #3 - Network Network Security

The ability to segment, isolate, and govern a network.includes software-defined networks and software-defined infrastructure Internet-based technologies and wide area networks,Network security is growing as organisations extend their networks in preparation for a partial or complete transition to Software Defined Networks, Software Defined Wide Area Networks, and internet-based technologies. Controlling privileged network access, managing internal and external data flows, preventing lateral network movement, and having insight to make dynamic policy and trust decisions on network and data traffic are all crucial. The capacity to segment, isolate, and govern the network remains a critical security element and is required for a Zero Trust Network.

4) Pillar #4 - Applications Application and Workload Security

Assuring the security and correct management of the application layer in addition to containers and virtual machines,The security and management of the application layer, as well as compute containers and virtual machines, is critical to ZT adoption. The ability to recognise and regulate the technological stack allows for more granular and precise access decisions. Unsurprisingly, multi-factor authentication is becoming an increasingly important component of providing appropriate access control to apps in ZT contexts.

5) Pillar #5 - Automation Security Automation and Orchestration

SOAR (security automation, orchestration, and response) enables enterprises to automate functions across products via work flows and to provide interactive end-user supervision.Cost-effective and harmonious ZT fully utilities security automation response solutions, which automate operations throughout product rough processes while providing for end-user monitoring and engagement. Other automated technologies are often used in Security Operation Centers for security information and event management, as well as user and entity behaviour analysis. Security orchestration integrates these tools and aids in the management of different security systems. When used together, these technologies may significantly reduce manual work, event reaction times, and expenses.

6) Pillar #6 - Analytics Security Visibility and Analytics

Security information and event management (SIEM), advanced security analytics platforms, and user and entity behaviour analytics are examples of visibility and analytics solutions(UEBA) allow security specialists to watch what is going on happening and intelligently orient defences. ZT employs technologies such as security information management, sophisticated security analytics platforms, security user behaviour analytics, and other analytics systems to enable security specialists to watch what is occurring in real time and intelligently position defences. The emphasis on the study of cyber-related event data can aid in the development of proactive security measures before an issue happens.

D. Zero Trust Architecture

A subject requires access to an enterprise resource in the abstract model of access. A policy decision point (PDP) and related policy enforcement point allow access (PEP).

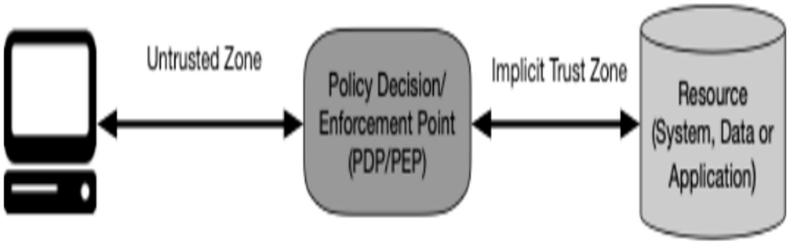
Untrusted Zone
Policy Decision/ Enforcement Point (PDP/PEP)
Implicit Trust Zone
Resource (System, Data or Application)

Figure 3 : Zero trust access

A ZTA deployment in a business is made up of several logical components. These components can be used as on-premises or cloud-based services. Figure 2 demonstrates the essential link between the components and their interactions in a conceptual framework model. It's worth noting that this is a hypothetical model that depicts logical components and their interactions.

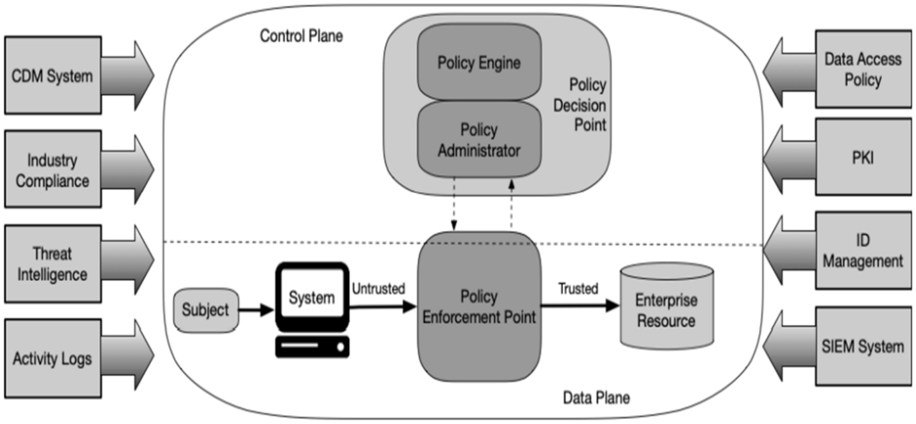

Figure 4 :Core Zero Trust Logical Components

The component descriptions:

1) The policy engine (PE) is in charge of deciding whether or not to offer access to a resource for a specific subject. The PE applies corporate policy as well as information from external sources to a trust algorithm to grant, deny, or revoke resource access. The PE is linked with the policy administrator component. The policy engine makes and logs the decision (as authorised or rejected), and the policy administrator implements the decision.
2) Policy administrator (PA): This component is in charge of creating and/or terminating the communication route between a subject and a resource (via commands to relevant PEPs). It would produce any session-specific authentication and authentication token or credential used by a client to access an enterprise resource. It is closely related.
3) PEP: This system is in charge of enabling, monitoring, and finally terminating connections between a subject and an enterprise resource. The PEP interacts with the PA in order to convey requests and/or receive policy changes from the PA. In ZTA, this is a single logical component that may be divided into two parts: the client (e.g., agent on a laptop) and the resource side (e.g., gateway component in front of resource that regulates access

E. Google Cloud's BeyondCorp Approach

BeyondCorp Enterprise is intended to provide end-to-end protection that is continuous and real-time, as well as scalable DDoS protection and built-in, verified platform security. It includes embedded data and threat protection built into Chrome (which has already been quietly updated) to prevent malicious or unintentional data loss and exfiltration, as well as malware infections from the network to the browser,phishingresistant authentication and continuous authorization for all interactions between a user and BeyondCorp -protected resources.The notion of zero trust is founded on the premise that there is no inherent confidence in a network and that all network access must be guarded, approved, and allowed based on knowledge about identities and devices. BeyondCorp refers to Google Cloud's zero-trust access strategy, which it began exploring in 2011. It is the technology suite that Google employs internally to safeguard its apps, data, and users, allowing its own staff to operate from untrusted networks on a range of devices without the usage of a client-side VPN.

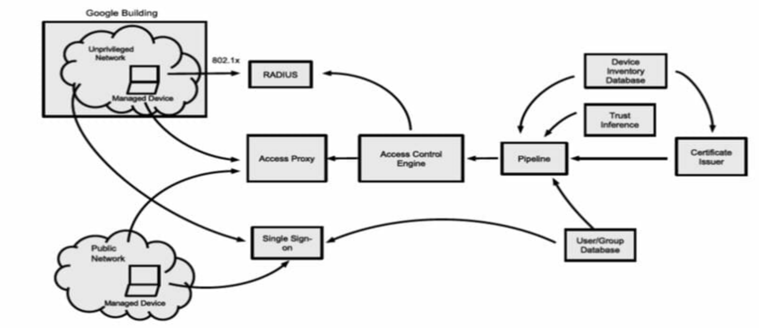

Figure 5 :Beyondcorp traffic\access flow

BeyondCorp is used as an example of a real-world Zero Trust implementation. While Google is a for-profit company, many of its internal components should be known to any business. This illustration is supplied solely for illustrative reasons and does not indicate support or suggestion for adoption by any other entity. BeyondCorp is founded on the original Zero Trust thesis, which states that standard perimeter-based security is insufficient to safeguard internal networks and data. Google also acknowledges and encourages the advancement of cloud technology and the migration of applications from on-premise data centres to cloud-based apps and services.

BeyondCorp Enterprise is a Zero Trust system that provides safe access with integrated threat and data protection that can:

1) Give important apps and services protected access.
2) Protect data with integrated threat and data protection.
3) With an agentless approach, you can simplify the experience for administrators and end users.
4) Increase visibility into potentially dangerous user behavior.
5) Improve your security posture by implementing a contemporary Zero Trust platform.
6) Which services you may access should not be determined by your connection to a specific network.
7) We give access to services depending on what we know about you and your device.
8) All service access must be verified, approved, and encrypted.

IV. RESULT ANALYSIS

Zero trust tenets may be implemented in any corporate context. Most firms have zero trust aspects in their corporate infrastructure or are on their way to implementing information security and resilience policies and best practises. A zero trust architecture is well suited to a variety of deployment situations and use cases. ZTA, for example, has its origins in firms that are geographically dispersed and/or have a highly mobile workforce. Having said that, a zero trust design may benefit any company.

A. Enterprise with Satellite Facilities

The most prevalent case is a company with a single headquarters and one or more geographically separated sites that are not linked by an enterprise-owned physical network connection.

Employees in remote locations may not have a fully corporate-owned local network but require access to enterprise resources to complete their duties. The enterprise may have a Multiprotocol Label Switchlink to the corporate HQ network, but it may not have the bandwidth to handle all traffic or may not want traffic meant for cloud-based applications/services to pass through the company HQ network.

B. Multi-cloud/Cloud-to-Cloud Enterprise

An business that uses various cloud providers is an increasingly prevalent use case for adopting a ZTA. In this use case, the organisation has a local network but hosts applications/services and data with two or more cloud service providers. The application/service is hosted on a different cloud service from the data source. Instead of forcing the application to tunnel back through the corporate network, the application housed in Cloud Provider A should be able to connect directly to the data source located in Cloud Provider B for improved performance and administration.

C. Enterprise with Contracted Services and/or Nonemployee Access

on-site visitors and/or outsourced service providers that require restricted access to company resources to accomplish their task These visitors and service providers will require network access in order to do their jobs. A zero trust company might support this by granting these devices and any visiting service technician internet access while concealing enterprise resources.

D. Collaboration Across Organizational Boundaries

Employees from both firms may not be situated on their organisations' network infrastructures, and the resource they want may be hosted within one corporate environment or in the cloud. This implies that sophisticated firewall rules or enterprise-wide access control lists aren't required to enable specific IP addresses from Enterprise B to access resources in Enterprise A depending on Enterprise A's access restrictions.

The technology used determines how this access is achieved. A PE and PA hosted as a cloud service may give availability to all parties without the need for a VPN or something similar.

Outcome

An agency must first designate a protect surface before deploying a ZTA. The protect surface contains the most valuable Data, Assets, Applications, and Services (DAAS) of the agency, which **Some Zero Trust Security Solutions**

The following are some examples of Zero Trust networking software:

1) *Okta:* It makes use of the cloud while also enforcing stricter security regulations. The software works with your organization's existing identification systems and directories, as well as 4000+ apps.
2) *Perimeter 8:* Is a software-defined perimeter with a robust architecture that provides expanded network visibility, full interoperability, smooth onboarding, and 256-bit bank-grade encryption.
3) *SecureAuth Identity Management:* Is known for providing users with a flexible and secure authentication experience that works in a variety of settings.

BetterCloud, Centrify Zero Trust Privilege, DuoSecurity, NetMotion, and other Zero Trust Networking software solutions are also worth mentioning.

E. Implementing Zero Trust in stages

Although each company's requirements are different, CrowdStrike recommends the following stages for implementing a mature Zero Trust model:

- *Visualize* - Comprehend all resources, their access points, and the hazards they entail.
- *Lessen* - Detect and halt threats, or mitigate the impact of a breach if it cannot be stopped immediately.
- *Optimize* – Extend protection to all aspects of the IT infrastructure and all resources, independent of location, while improving the end-user, IT, and security teams' experiences.

There are several use cases where Zero Trust in the cloud can be applied:

1) *Zero Trust for Private Apps in the Public Cloud:* Secure access is critical when programmes migrate from on-premises data centres to the cloud. Managed or unmanaged devices require strong policy enforcement, providing access to required apps based on user role while simultaneously preserving security and protection. You must also keep regular track of what data is being accessed and by whom.
2) *Zero Trust for SaaS Apps:* Collaboration has become easier with employees located anywhere, as well as contractors and third-party vendors, thanks to the rise of popular SaaS apps like G Suite, Box, and Office 365; however, this can result in unauthorised users having access to data or apps that do not pertain to their job requirements. Securing SaaS apps necessitates preventative methods as well as policy enforcement. It is critical to provide different degrees of access to workers and contractors in order to keep users pleased and data safe.
3) *Zero Trust for DevOps in the Cloud:* Zero Trust relies heavily on least-privileged access. The DevOps team is constantly constructing and pulling down API-powered cloud apps. However, ensuring that those APIs are accessible by the proper people and that the information being exchanged is safeguarded is critical — with granular visibility. By requiring authentication at the security service layer, unauthorised users are prevented from attempting to authenticate to an API, lowering the risk of an attack.
4) *Challenges in Implementing Zero Trust*

There are numerous reasons why establishing Zero Trust is difficult for businesses, including:

a) For corporate operations, several legacy systems such as tools, programmes, network resources, and protocols are used. Identity verification is insufficient to safeguard them all, and re-architecting them would be prohibitively expensive.
b) *Limited Visibility and Controls:* Most organisations lack complete visibility into their networks and users, or they are unable to enforce rigorous protocols around them for whatever reason.
c) *Regulations:* Because regulatory authorities have yet to adopt Zero Trust, businesses may have difficulty passing security audits for compliance.

V. CONCLUSION

Zero Trust is making waves in the security field, despite its early stages. With more and more cyberattacks occurring around the world, a secure solution like Zero Trust is required.By authenticating all of your devices and users at each access point, Zero Trust provides a stronger security architecture with identity and access controls to your data and transactions. It can defend businesses against all types of cyber threats, including persons and programmes from both inside and outside the country.

To address the distributed nature of your modern IT environment, Zero Trust is an architectural approach that lets you look at security differently. It focuses on policy, identity, and posture to granularly regulate connections between users, systems, applications, and data rather than being "within" the perimeter.Zero Trust can help you improve your security and meet your organization's security standards, certifications, and best practises.Zero Trust is a set of rules, processes, and technologies that enable you to deploy many of the capabilities that you presumably already need to satisfy the modern campus's cybersecurity requirements.Zero Trust is a game-changing business enabler. You can confidently deliver new capabilities to students, instructors, and staff with the ability to safeguard every connection, giving them greater freedom and productivity.Zero Trust is a journey that will require the participation of the whole university to begin and continue. As a result, it may cultivate a diverse set of institution-wide connections to increase knowledge, ownership, and involvement, all of which offer advantages beyond increased security.

REFERENCES

[1] Romans Vanickis, Paul Jacob, Sohelia Dehghanzadeh, Brian Lee researched on Access Control Policy Enforcement for Zero-Trust-Networking,(2018)oonas Linnosmaa, Britta Hale, Bryan O'H

[2] Nikolaos Papakonstantinou, Douglas L.Van Bossuyt, Jalloran discussed in the concept of Zero Trust Hybrid Security and Safety Risk Analysis Method(2021)

[3] Gilman E., Barth D.: Zero Trust Networks, O'Reilly, (2017)

[4] Williams C.: Zero Trust Security, Centrify Special Edition.John Wiley & Sons,Inc., Hoboken, New Jersey (2019)

[5] Kindervag J.: Build Security Into Your Network's DNA: The Zero Trust Network Architecture, Forrester (2010)

[6] T. Dimitrakos et al.,"Trust aware continuous authorization for zero trust in consumer internet of things", 2020,

[7] Akamai: "The 6 Business and Security Benefits of Zero Trust." White Paper (2018)

[8] Kindervag J.: Clarifying What Zero Trust Is and Is Not (2018)

[9] A. P. Patil, G. Karkal, J. Wadhwa, M. Sawood and K. Dhanush Reddy, "Design and implememtation of a consensus algorithm to build zero trust model," 2020,

[10] Sivaraman R.: "Zero Trust Security Model". S3tel Inc, White Paper (2015)

[11] S. Rose, O. Borchert, A. Mitchell and S. Connelly, "Zero trust architecture, NIST special publication 888-207," NIST,(2020).

[12] Ward R., Beyer B,: "BeyondCorp A New Approach to Enterprise Security". Usenix, vol. 39:6 (2014)

[13] Morgan S.: "Cybersecurity Market Reaches $75 Billion In 2015; Expected To Reach $170 Billion By 2020", Forbes (2015)

[14] J. Kindervag, "No more chewy centres: The zero t rust model of information security," Forrester Research,(2016)

[15] S. H , "Zero trust architecture design principles," National Cyber Security Centre (NCSC), (2021)