The Challenge of Achieving Zero Trust Remote Access in Multi-Cloud Environment

Venkata Naga Satya Surendra Chimakurthi

Solutions Architect, CDBDX-Platforms-DAM (Digital Asset Management), Cognizant Technology Solutions, Dallas, **USA**

*Corresponding Contact:
Email: chvnssurendra@gmail.com

Manuscript Received: 14 Nov 2020 - Revised: 13 Dec 2020 - Accepted: 23 Dec 2020

ABSTRACT

Zero-trust security models and architectures have recently increased in adoption due to several variables, such as the widespread use of off-premises cloud technologies, variety in IT devices, and diffusion in the Internet of Things (IoT). Users, devices, apps, and networks are all assumed to be untrustworthy in this approach, which is built on the idea of various tiers of Trust and authentication. Cybersecurity paradigms are developing, and the term "zero trust" describes the shift from static network perimeters to protecting people, things, and resources. Economic and enterprise architecture and processes can be designed using zero trust principles. In the idea of zero Trust, assets or user accounts are thought to have no implicit confidence because of their physical or network location (Internet vs local networks) or asset ownership (enterprise or personally owned). Authentication and authorization must be conducted before a connection to an organizational resource can be established. There are many different types of Cloud, including several public, private, hybrid, and on-premises. For data centres, a multi-cloud deployment strategy includes many different public cloud service providers instead of relying on a private cloud or on-premises architecture. Hybrid multi-cloud is a multi-cloud implementation that incorporates all public and private clouds and on-premises technology. This paper discusses the zero-trust security model for multi-cloud environments and applications and the obstacles to implementing it.

Keywords: Zero Trust, Multi-cloud Environment, Cybersecurity, Network Security

INTRODUCTION

Complex programs and data are moving to the Cloud because of the financial advantages of cloud computing. As a result of multi-cloud and federated Cloud, adoption security remains a major barrier to cloud adoption, particularly for apps and data that reside in the Cloud. The world is perilous. With unscrupulous actors on the prowl for opportunities to exploit flaws,

danger lurks around every turn (Pawar et al., 2015). This isn't a teaser for a new thriller movie; it's the current state of business affairs. Everything should be verified and reviewed as if it were a threat, which is the foundation of Zero Trust Security. In today's world of cloud computing, Zero Trust is essential to safeguard enterprises against data breaches. Apps and content can no longer be protected behind a network firewall in the Cloud, requiring users to access them from outside the perimeter firewall. The threat landscape might be widened if remote access is granted, giving attackers a foot in the door. Identity and access management is not centralized in the Cloud (or numerous clouds). Instead of a single detection algorithm, various apps have their unique identity system. It's no longer possible to manage or see across the multitude of different identity systems, and only superficial connections utilizing mechanisms like a federation or single sign-on are possible (SSO).

Because of the rapid pace of technology advances, a new network security architecture is urgently required. The perimeter concept was born when not all computers in an enterprise were connected to the public Internet. In today's network landscape, things are a lot more intricate and dispersed than they were a generation ago. Now, businesses must consider remote workers, BYOD plans, and cloud-based applications when constructing their network (Chimakurthi, 2017a). In addition, a security breach might cost a fortune. Every layer of a company's network must be protected from hackers, not simply the perimeter (Flanigan, 2018). These additional factors make a perimeter security method to protect a network more difficult. To address this issue, the zero-trust model proposes an innovative solution.

LITERATURE REVIEW

This is no longer an effective strategy to enforce security in today's new threat landscape. All of our network's resources can be accessed by an attacker once he gets beyond the shell. Despite our best efforts, organized cybercriminals have penetrated our defences by recruiting insiders and devising new attack tactics. Rather than relying on perimeter protection to keep out these new dangers, IT security experts must extend security throughout the entire network in order to eradicate the soft, chewy centre. Forrester developed a new paradigm for information security, termed Zero Trust, to assist security professionals in this endeavour (Kindervag, 2010). The first in a series of reports explains why the Zero Trust Model is necessary and what it entails.

As one of the first zero-trust initiatives, Google's BeyondCorp was a pioneer in the field. Device and user credentials are used instead of the privileged corporate network to establish Trust (Ward & Beyer, 2014). A VPN is no longer required to get into the privileged network because of this fine-grained control of network resources. Remote workers will appreciate the improved user experience as a result of this.

Big data security control now includes a new approach that includes three steps: zero-trust user context recognition, fine-grained data access authentication control, and full network traffic audit to identify and intercept risky data access in a big data environment. (Tao et al., 2018) called this approach "data access audit." It has been proven that a fine-grained big data security method based on the zero-trust model of a drug-related information analysis system is capable of identifying a large number of data security threats.

This literature (Chen et al., 2018) serves as an introduction to the field of cloud computing security research. A brief look into cloud users' habits follows. In order to verify the model's accuracy, we'll simulate a cloud-based digital book platform and run simulations of our own to see how well it performs (Chimakurthi, 2017b).

ZERO-TRUST SECURITY MODEL

IT systems can be designed and implemented using a zero-trust security model (perimeterless security, zero trust architecture, ZTA, zero-trust network architecture, ZTNA). A zero-trust approach has always been about "never trust, always verify," which means that no matter how well a device is connected to a managed corporate network such as the corporate LAN, it should not be trusted by default. Authentication, authorization, and continual validation of security configuration and posture are required for all users, whether in or outside the organization's network, before they are permitted or maintained access to applications and data. No traditional network edge is presumed when dealing with Zero Trust; networks can be local as well as cloud-based, or even a hybrid of the two. In today's digital revolution, Zero Trust is a paradigm for protecting infrastructure and data. In this approach, modern organizational problems like the protection of remote workers, the use of cloud infrastructures, and the avoidance of ransomware attacks are handled. Numerous vendors have made an attempt to come up with their own definition of Zero Trust. Some established standards, on the other hand, can aid you in aligning Zero Trust with your own organization's aims.

Forrester Research lead analyst John Kindervag came up with the Zero Trust security paradigm in 2010 (Kindervag, 2010). Cloud computing's distributed identity management is made possible by Zero Trust's identity management platform. To accomplish Zero Trust, you don't need any specific piece of software or technology.

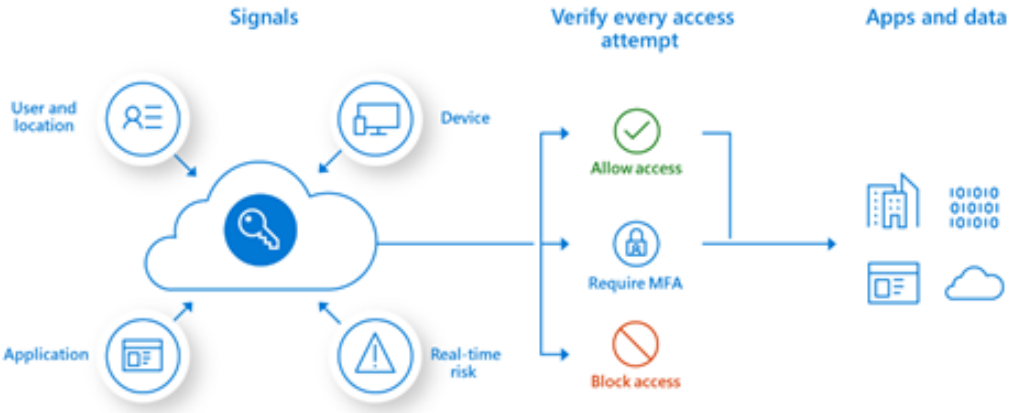

Figure 1: Zero-trust security model

When it comes to zero-trust networks, authors Evan Gilman and Doug Barth say that five basic claims are the foundation (Gilman & Barth, 2017).

- First and foremost, the Internet is presumed to be a hostile environment at all times.
- Both external and internal attacks constantly threaten the network.
- Trust in a network cannot be decided just based on the network's proximity.
- Authentication and authorization are required for all users and network traffic.
- There must be a wide range of data sources used to calculate policies.

It's not easy to build a network that adheres to these assumptions, but automation has made it much more feasible than before.

Zero Trust Architecture

This means that there is no longer a trusted interface in our devices, no longer a trusted network, and no longer trusted people, which is a crucial idea for moving packets from one location to another. If we look at the old paradigm (figure 2), we can see that there are multiple layers of the network where security devices are placed. This makes the network heavy, unmanageable, and difficult to keep secure, as well as requiring constant investment in new equipment over time.

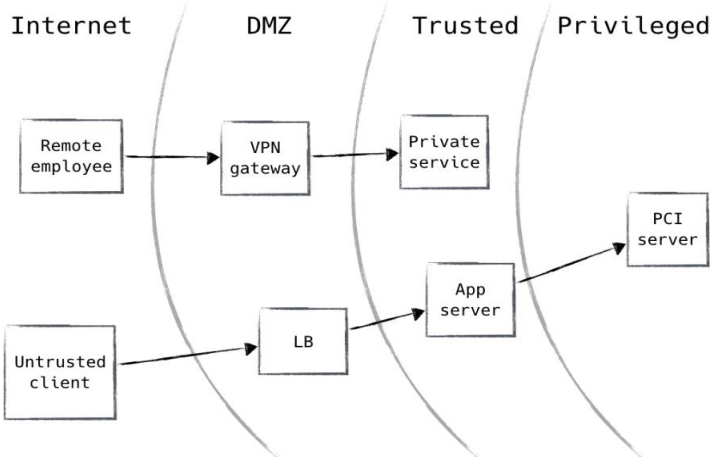

Figure 2: Traditional Security Architecture

As a result of the zero-trust paradigm, the network is redrawn, and the concept of a segmentation gateway is introduced. Content screening, access control, firewalls, cryptographic engines, and package forwarding are just some of the components that this concept aspires to integrate into a single modern network infrastructure. Any organization can use this segmentation because it is modular, scalable, and can be applied to any network configuration. A network that is built from the bottom up seems to be the only way for a firm to have an infrastructure that adapts and evolves and a security ADN that permits all packets to be securely transmitted.

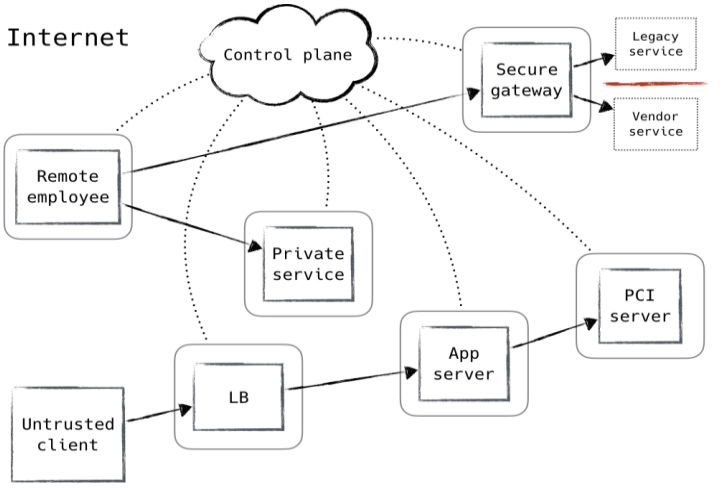

Figure 3: Zero-trust architecture

In order to increase network micro-segmentation while simultaneously being scalable, adaptable to multiple business models, and virtualization-friendly, this segment gateway technique is known as an emerging firewall (Chimakurthi, 2018).

In the figure shown, a segmentation gateway is depicted in a simple manner, making the separation in micro-segmentation (MCAP) easy to check all the network data. By segmenting the network and using next-generation firewalls, we can regulate who, when, what, and where people connect to the network in a more granular manner. Once a user has been verified, their access rights must be strictly controlled. This is done in order to limit the harm that can be done to the network after it has been breached. The use of the term "firewall" in this context should not be interpreted as implying that we're looking for a location near the network's perimeter. (Cordeiro Filho et al., 2019).

Table1: Features of Zero trust

Feature	**Zero Trust**
Agility	High
Use cases	Multiple
Security	High: identity-based
New User Set up	Easy
implementation	Quick & easy

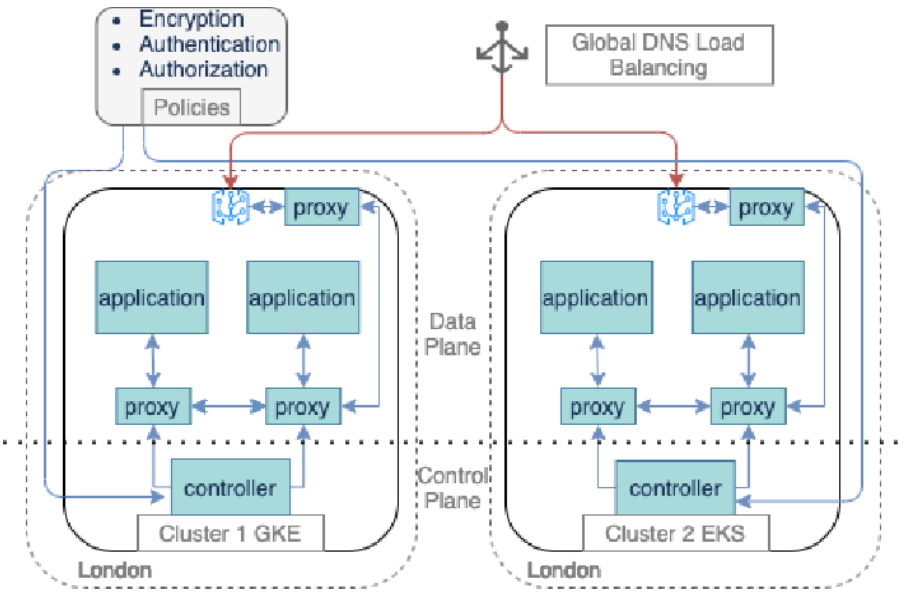

Figure 4: Zero trust architecture in the multi-cloud environment

CONSTRAINTS ON ACCESS

Despite its virtues, the zero-trust paradigm has its drawbacks. Before implementing such a network model, there are various security aspects to be aware of. Because the zero-trust approach relies significantly on user and device verification, identity theft is an important factor to consider. The approach does seek to address this problem by using user and device verification in combination, and there is something to be said of other methods.

This is an issue that is common across the sector, and many are striving to address it. Additionally, a Distributed Denial of Service (DDoS) attack must be thwarted. DDoS attacks cannot be mitigated by the zero-trust architecture alone. Hence extra security measures are required. Upstream traffic screening protections are commonly used as part of this safeguard. Traffic filtering in zero-trust networks is facilitated by the fact that the network retains a great deal of information about what to predict.

By monitoring the network, an attacker can create a diagram of the system's architecture in zero-trust models. This was not possible with the conventional perimeter model because all traffic was routed through VPN endpoints. The zero-trust approach does not include network privacy, but site-to-site tunnels can provide it (Gilman & Barth, 2017). Zero Trust poses certain new security issues, but it also eliminates many of the problems associated with the perimeter approach.

ZERO TRUST'S FUNDAMENTAL PRECEPTS

Figure 5: Zero trust security principles

Zero trust devices: There are no trusted or safety devices on the corporate network under a zero-trust security policy. Zero trust security involves the ability to recognize danger and separate those that have been compromised in order to implement it.

Zero trust data: One of the key goals of a zero-trust security policy is to improve data security. For zero-trust to be implemented, it is necessary to identify and map common data flows and define access rules that are based on business necessities. A company's whole IT infrastructure, including desktops, mobile devices, database and application servers, and cloud deployments, must adhere to the same security regulations.

Zero trust networks: Corporate cybersecurity or zero-trust security policies cannot be adequately protected by simply protecting the perimeter of the company's network. It is possible to create a zero-trust network by micro segmenting it and defining boundaries around the company's most important assets. In order to prevent threats from moving laterally through the network and to limit and isolate a suspected breach, it is possible to conduct security inspections and apply access controls at these boundaries.

Zero trust workloads: Containers, functions, and virtual machines (VMs) are attractive targets for cybercriminals because of their scalability and flexibility (Chimakurthi, 2018).

The public Cloud necessitates granular zero trust monitoring and access controls to protect these assets.

Zero trust people: Because compromised credentials are the most common cause of data breaches, using usernames and passwords alone is no longer sufficient for ensuring account security. Strong MultifactorMultifactor authentication and zero-trust network access are necessary for zero Trust.

ORGANIZATIONS' TRUST IN ZERO TRUST

The first nine months of 2019 saw a 33.3 per cent increase in data breaches as compared to previous years (Security, 2019).

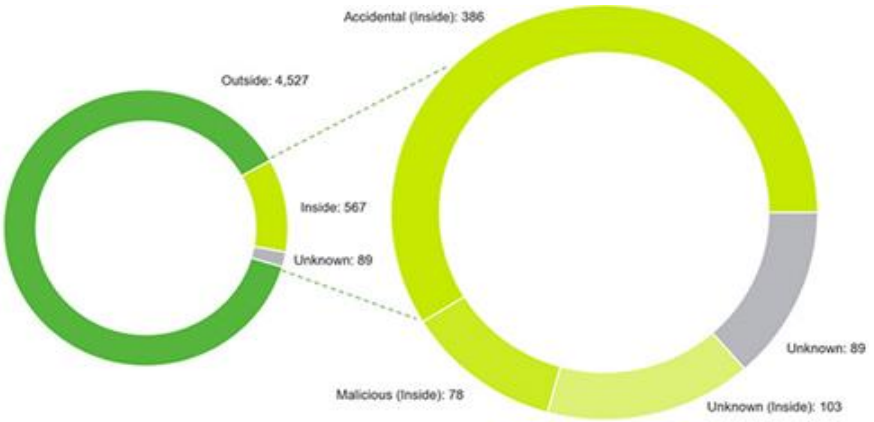

Figure 6: Attack increment ratio in 2019

Zero Trust is gaining traction despite the fact that security professionals have been sluggish to adopt it. Cloud and networking titans Cisco and Verizon, as well as leading hyperscales like Amazon, Google, and Microsoft, have all unveiled zero-trust designs for their respective platforms. Zero Trust has already been implemented by a number of enterprises IT firms, including IAM, multifactormultifactor authentication, and some level of policy controls, beyond the major hyperscalers. Their approach to east-west traffic is also becoming more and more focused on micro-segmentation. Zscaler's Zero Trust adoption survey found that 78% of security IT teams want to adopt a Zero Trust model within the next few months.

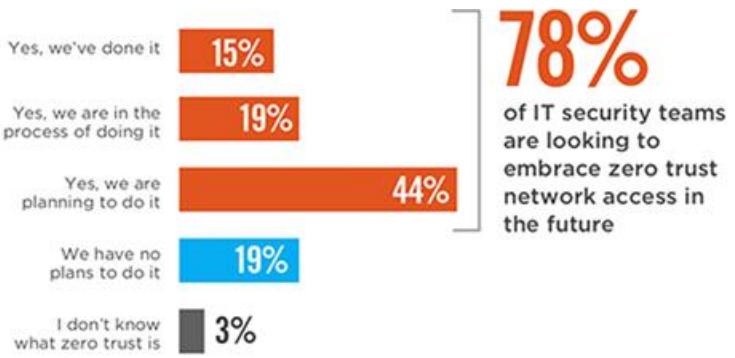

Figure 7: Growth in zero-trust adoption

Having said that, establishing a Zero Trust strategy requires more than just putting these tools in place. It's also about enforcing the principle that no one and nothing can have access unless they have proven themselves to be trusted users by employing these new capabilities.

SECURITY WITH ZERO-TRUST: THE ADVANTAGES

With the Zero Trust Model of information security, attackers have a harder time getting into your network and having a harder time wreaking havoc once inside. New user populations, customer interaction models, accelerated cloud adoption and IoT devices and sensors are all supported by Zero Trust's network infrastructure. As a result, more and more enterprises are turning to Zero Trust with their next security architectures. Implementing Zero Trust networks has a slew of advantages for both business and security, but eight stand out in particular.

- **Network visibility, intrusion detection and vulnerability management are all enhanced:** September 7th, 2017, was the day Equifax announced that hackers had stolen the personal information of more than 143 million of its customers (Bernard et al., 2017). It was only on July 29th, months after the attackers had accessed the company's crucial systems and user data, that the firm detected the breach. Sadly, Equifax isn't the only one: We've seen time and time again that security professionals were unable to detect the breach for weeks or even months. Security professionals can do the following with Zero Trust:
    - All network traffic should be inspected for suspicious activity.
    - Data breaches can be prevented or minimized.
    - Reduce the suffering caused by problems with vulnerability management.
- **It Prevents Malware from Spreading:** Malware can't spread on Zero Trust networks because of their intrinsic security. A malicious actor uses the command and control (C&C) channel to direct malware across the current routing and switch architecture in a traditional network. In most cases, malware needs humans on the other end of the C&C link to help lead it along with the network. Enterprises in more than 150 countries worldwide, including the US city of Atlanta, were impacted by WannaCry ransomware and its derivatives, which cost $17 million to mitigate and recover from (Blinder & Perlroth, 2018). Security professionals can do the following with Zero Trust:
    - Protect vital systems against the spread of malware using Zero Trust.
    - Users and vital systems should be shielded from the spread of malware.
- **Capital and Administrative Expenses are reduced:** Regarding the topic of safety; as a result, you've spent a great deal of money on new controls to fix holes and manage the complexity of your outdated network. It used to be referred to as "protection in-depth," but in fact, it became "expensive in-depth," an exercise in which more and more equipment and software are added on top of one another with the aim of blocking undiscovered attacks. For the sake of securing sensitive data and the programs that use it, this approach fails miserably. Security professionals can do the following with Zero Trust:

- Streamline the management of a plethora of security tools scattered around the network.
- Management costs can be reduced.

- **It limits the potential and compliance costs:** Initiatives Segmenting your network reduces the breadth of your organization's conformity efforts because many laws only apply to certain types of data. An excellent illustration of this is PCI, which claims that "the entire system is in the realm of the PCI DSS evaluation without sufficient network segmentation" Security professionals can do the following with Zero Trust:

  - Streamline rules in the industry.
  - Make compliance audits a little easier.

- **Eliminates Intersilo-Finger-Punching:** CIOs in almost every technology firm have a wide range of silos: network teams, operations teams, memory teams, computer processing teams, application programming teams, security personnel, and so on. Team members each have their own unique set of goals and motivations that naturally collide with those of other teams. When things like network outages occur, this is most apparent. The facade of inter-team cooperation is shattered in a split second. It is at this stage that the blaming begins. Security is blamed by the network team, and the network team is blamed by security. Technology organizations are compelled to break down the walls between their diverse teams because of Zero Trust. Security professionals can do the following with Zero Trust:

  - Maintain close ties with other technical teams and organizations.
  - Break down the silos between departments

- **It raises the level of data consciousness and insight:** It's possible to gain visibility into your content and how it passes through your network by using a Zero Trust network. Detecting and tracking the sorts of data in transit in your network is made easier by Zero Trust's ability to view everything inside your packets. Security professionals can do the following with Zero Trust:

  - Involvement in data privacy projects should be encouraged.
  - Identify and classify all sensitive information.

- **It prevents malicious attackers from obtaining sensitive information:** Breach and intrusion are frequently used interchangeably by those in the security industry. Intruders are those who break into a network without the permission of the network administrator. An intrusion is not a security breach. It is a word of art that has been defined by law and regulation. A breach happens when a malicious actor gains access to sensitive data (personally identifiable information (PII) of consumers or workers, provides complete or intellectual property) on your networks or systems. Due to their impact on the company, breaches are important. Breach-related resignations at big corporations like Sony, Bangladesh Bank and Target have become common. The Director of the US Office of Personnel Management resigned following the leak of more than 20 million records on government workers, suppliers and others. These security lapses are also extremely expensive, running into the tens of billions of dollars. Equifax paid

$575 million to settle with the FTC alone. Zero Trust aims to prevent data leakage. Security professionals can do the following with Zero Trust:

- The intellectual property and future revenue of the company can be safeguarded with a Zero Trust network.
- When a breach occurs, it can have an emotional and financial impact on clients.

- **It facilitates the digital transformation of businesses:** Your digital business exists wherever your consumers interact, your workers or partners engage with your offerings, and your data is used today because there is no defined perimeter in today's digital business. It's time to abandon a perimeter-based strategy to security in support of a cloud-based, beacon-equipped, and internet-of-things-enabled approach to protecting our businesses and physical environments. Security professionals can do the following with Zero Trust:

  - Become a co-creator of the digital future.
  - IoT adoption should be accelerated.

CHALLENGES TO ZERO TRUST

There are a lot of good ideas out there, but because of the following problems that practically every business faces, many of them are impossible to implement in practice.

Debts in the system

You have technical debt if your company creates its own software for internal use, even if it is only a few years old. Internal application redesign, recoding, and re-deployment can be expensive and disruptive. For these kinds of projects to be worthwhile, there must be a compelling business case. It's not always possible to add security parameters to already-existing programs in order to make them trustless. It's likely that your current applications don't support zero Trust. Because of this, the degree to which you are dependent on bespoke applications determines whether or not you can embrace zero faith in those processes and hence the amount of time and money required. Microperimeter-compatible apps, or those that lack application programming level interfaces to facilitate automation, are particularly problematic in these cases.

Systems of the Past

Legacy systems, architecture, and applications do not take zero Trust into account. These systems have no concept of lateral mobility or the concept of least privilege, and they do not have dynamic authentication models that can be changed based on context.

A zero-trust implementation necessitates a layered or wrapper approach. In contrast, a layered strategy involves enclosing external access to the resource so that it has no impact on the system itself. This is an affront to the zero-trust notion. A non-compatible application's behaviour can't always be monitored. Screen scraping, keyboard logging, logs, and network traffic can all be used to hunt for suspicious activity, but your ability to react is severely constrained. Only the user or other sources can limit the legacy application's external interaction; the runtime itself cannot be restricted. As a result, enterprises may be unable to even monitor network traffic due to the severe encryption requirements, such as TLS 1.3, associated with their legacy application.

Peer-to-Peer (P2P) Technologies

Peer-to-peer (P2P) networking is a feature of Windows 10 that you may not know about if you assume your company doesn't use it.

In 2015, Windows 10 included a peer-to-peer method to distribute Windows Updates among peer systems in order to reduce Internet traffic. It's possible some organizations don't even know this exists. This is an example of unchecked, privileged migration between systems. The zero-trust principle is violated by this functionality, notwithstanding the fact that no vulnerabilities or exploits have been discovered. Outside of the microperimeter, no lateral movement should be allowed. ZigBee and other mesh network technologies, on the other hand, function in direct opposition to the zero-trust model. To work, they need peer-to-peer communication, and the trust model relies solely on keys or passwords; there are no dynamic models for modifying authentication.

It is important that your firm has P2P or mesh network technologies in place, even for wireless networks, before committing to zero Trust. These are major roadblocks to implementing zero trust access and microperimeter controls.

Modernization through the use of technology

It can be challenging to adopt zero Trust even for enterprises that are in a position to create new datacenters, deploy role-based access models, and embrace zero Trust in its entirety.

It takes additional tech to segment and enforces the zero-trust paradigm in a digital transformation driven by Cloud, DevOps, and IoT. For large deployments, this can be prohibitively expensive and may even affect the capacity of the solutions to interact correctly with multi-user access. Think about the storage and licensing fees alone if you're not certain that this is a good idea for your project. When it comes to segmentation and zero-trust frameworks, it all relies on how you use the Cloud. The concept of zero Trust cannot be fully embraced by a simple cloud migration of your raised floor. If you build a new service on the Cloud, it's possible to have 0% trust in it.

However, simply migrating to the Cloud as part of your digital transformation does not guarantee that you will profit from the zero-trust paradigm. Zero Trust will not work as a layered strategy after the fact for all the reasons outlined previously in this post if you choose to embrace it and bake it into your design.

How to deal with these challenges

There are several drawbacks to a zero-trust network, yet it is nevertheless favoured by security-conscious organizations. The greatest way to reduce the dangers of zero Trust is to avoid thinking of it as a black-or-white proposition. A zero-trust architecture can be implemented without abandoning existing systems. Determine which data and workflows are most crucial to the success of your business. It is possible to apply stricter access constraints, such as two-step verification and privileged access. Standard perimeter controls apply to the majority of data, whereas only the most critical information is subject to zero-trust rules.

Zero-trust security can be introduced gradually to avoid disrupting a cybersecurity strategy. However, because companies are not completely forsaking one system for another, they are less vulnerable to threats.

Data breaches continue despite the attempts of the broad cybersecurity community. Zero-trust cybersecurity aims to secure assets themselves rather than simply entry points to combat this. Zero-trust barriers can be addressed as long as companies are aware of them.

ANALYSES OF CLOUD-BASED USER BEHAVIOR

There is a wide range of user categories and statuses to choose from when it comes to user behaviour. Cloud users' activity is recorded as N in this article for simplicity of analysis; hence the total number of cloud users can be recorded as N.

$$\mathbf{CB} = \{\mathbf{cbi}|\mathbf{i\ is\ a\ natural\ number}, \mathbf{and}\ 0 < \mathbf{i} \leq \mathbf{N}\}$$

Where cb_i is the cloud end user's ith action.

There will be mi users if i is chosen as the number of cloud end users. The following is a list of possible values for the cloud user state set.

$$\mathbf{CBS} = \{\mathbf{cbsj}|\mathbf{j}, \mathbf{i\ is\ a\ natural\ number}, \mathbf{and} 0 < \mathbf{j} \leq \mathbf{mi}, 0 < \mathbf{i} \leq \mathbf{N}\}$$

The behaviour set of cloud users has been specified, and the collection of the state of each behaviour can be used to analyze the behaviour data of cloud users. In order to speed up the evaluation process, a basic statistical method is used to analyze cloud user activity. According to our assumptions, the historical data is trustworthy. The behaviour of each cloud user is a statistical statistic based on the trusted data, and the collection of trusted states includes some higher frequency states. Pi states are common in the ith cloud user's behaviour. Pi behaviour states make up the set of user behaviour trusted states. This is the cloud user's trusted state set.

$$\mathbf{CBSTRUSTED} = \{\{\mathbf{cbstrustedj}\}\mathbf{i}|\mathbf{j}, \mathbf{i\ is\ a\ natural\ number}, \mathbf{and} 0 < \mathbf{j} \leq \mathbf{pi}, 0 < \mathbf{i} \leq \mathbf{N}\}$$

The direct trust value can therefore be calculated by simply counting the trusted state set of each cloud user's behaviour. As a matter of course, each cloud user's conduct can be taken into account when calculating the weight. Weights are assigned by an expert based on their knowledge and experience, and they can also be obtained through algorithm optimization, in which we assign weights based on each cloud user's specific behaviour.

$$\boldsymbol{\varepsilon} = \{\boldsymbol{\varepsilon}\mathbf{i}|0 < \mathbf{i} \leq \mathbf{N}\}$$

Where $\mathbf{0} \leq \varepsilon i \leq \mathbf{1}$ and $\sum_{i=0}^{N} \varepsilon i = 1$. It's possible that the weight of the behaviour could be 0 if it doesn't occur (Chen et al., 2018).

CONCLUSION

With about 90 percent of the world's population predicted to be online by 2030, cybersecurity has emerged as a new area of worry for the security of the Internet, which has grown exponentially over the years. Since the sophistication of attacks and the disappearance of network perimeters have made traditional security models increasingly unworkable,

It is clear that modern technology and workplace structures have brought new obstacles to the network security architecture known as the zero-trust network model. It is predicated on the premise that the network is inherently hostile, and this is the foundation of the system. To put it simply, corporations are still grappling with how to adapt the zero-trust approach in terms of network security. Zero trust model principles have already been

adopted by certain cutting-edge technological organizations, such as Google, while others are still in the process of adapting to them. The zero-trust model is effective in addressing the issues it is designed to. A growing number of firms are implementing part or all of the zero-trust network security model's concepts, and this is an essential trend to keep an eye on.

REFERENCES

Bernard, T. S., Hsu, T., Perlroth, N., & Lieber, R. (2017). Equifax Says Cyberattack May Have Affected 143 Million in the U.S. *The New York Times*. Retrieved from https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html

Blinder, A., & Perlroth, N. (2018). A Cyberattack Hobbles Atlanta, and Security Experts Shudder. *The New York Times*. Retrieved from https://www.nytimes.com/2018/03/27/us/cyberattack-atlanta-ransomware.html

Chen, Z., Tian, L., & Lin, C. (2018). Trust evaluation model of cloud user based on behavior data. *International Journal of Distributed Sensor Networks*, *14*(5), https://doi.org/10.1177/1550147718776924

Chimakurthi, V. N. S. S. (2017a). Cloud Security - A Semantic Approach in End to End Security Compliance. Engineering International, 5(2), 97-106. https://doi.org/10.18034/ei.v5i2.586

Chimakurthi, V. N. S. S. (2017b). Risks of Multi-Cloud Environment: Micro Services Based Architecture and Potential Challenges. *ABC Research Alert*, *5*(3), United States. https://doi.org/10.18034/abcra.v5i3.590

Chimakurthi, V. N. S. S. (2018). Emerging of Virtual Reality (VR) Technology in Education and Training. *Asian Journal of Humanity, Art and Literature*, *5*(2), 157-166. https://doi.org/10.18034/ajhal.v5i2.606

Cordeiro Filho, R., Carvalho, A. A., Carvalho, R. A., Cordeiro, M. P., Cordeiro, G. S., Teixeira, C. D., … Pedro, R. N. (2019). Endourologic Treatment for Aggressive Angiomyxoma of the Bladder. *Journal of Endourology Case Reports*, *5*(1), 19–21. https://doi.org/10.1089/cren.2018.0106

Flanigan, J. (2018). *Zero Trust Network Model*. Retrieved from https://www.cs.tufts.edu/comp/116/archive/fall2018/jflanigan.pdf

Gilman, E., & Barth, D. (2017). *Zero trust networks: building secure systems in untrusted networks*. Sebastopol, Ca: O'reilly Media.

Kindervag, J., & Balaouras, S. (2010). No more chewy centers: Introducing the zero trust model of information security. *Forrester Research*, 3.

Pawar, P. S., Sajjad, A., Dimitrakos, T., & Chadwick, D. W. (2015). Security-as-a-Service in Multi-cloud and Federated Cloud Environments. *Trust Management IX*, 251–261. https://doi.org/10.1007/978-3-319-18491-3_21

Security, R. B. (2019). Data Breach QuickView Report 2019 Q3 Trends. Retrieved from pages.riskbasedsecurity.com website: https://pages.riskbasedsecurity.com/data-breach-quickview-report-2019-q3-trends

Tao, Y., Lei, Z., & Ruxiang, P. (2018). Fine-Grained Big Data Security Method Based on Zero Trust Model. *2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS)*. https://doi.org/10.1109/padsw.2018.8644614

Ward, R., & Beyer, B. (2014). BeyondCorp: A New Approach to Enterprise Security. *Login*, *39*(6), 6–11. Retrieved from https://research.google/pubs/pub43231/

--0--