Zero Trust Security- Understanding Networking and Architecture

Understanding the previous architecture:

Previously, we had the castle-moat type of security, which was perimeter based, centralized security system. Anything that was within the defined network perimeter, was trusted and devices/users outside the perimeter were untrusted. This gave the insiders the freedom of lateral movement, and they had free access within the perimeter. This proved to be a major setback, as if a malicious attacker compromised a single device within the perimeter, he could gain all the information he wanted through lateral movement, and this breach could take days to detect, since the activity within the perimeter was not monitored.

We also had a centralized security system previously, as most of the traffic was internal. The vast majority of data and applications was at the data centre or the Head Quarters and that was where the traffic went to and fro most often. So the networking and security infrastructure revolved around the data centre or Head Quarters. The traffic through internet where most of the malicious users are/ attacks happen was very less. Internet was previously used just for browsing, or very light traffic, and could be easily controlled through a security stack and anyone wanting to access the internet could go through the security at the central data centre and Head Quarters.

But now, with the changing workplace environment, and digitalization, and everything being remote, things have changed. The type of traffic across a network has changed. Many organizations are hosting more and more of their applications on cloud, and with Saas (Software as a Service) applications, Infrastructure as a Service, private clouds, increased amount of browsing, has lead to an increased volume of internet traffic.

Now with a complete inversion in the type of traffic, it changes the dynamic of setting up the network and security system. It causes a lot of problems as well, like the cost and maintenance, the no. of tools required and integrations that are

needed for it goes up, and it affects the performance of the network as well. The VPN and MPLS communication setup also gets expensive while managing such huge traffic. So this is indirect traffic, where all of it is going through a data centre, and then out to the internet through a single checkpoint and security appliances/devices had many drawbacks as it kind of creates a bottleneck when such huge amount of traffic is being centrally directed.

So, instead of the indirect centralized way, people shifted to a decentralized system of security. In this more modern approach, we allow direct internet access, whether its applications that are available as Infrastructure as a service, or Saas apps, or cloud storage. Since that is where a lot of performance sensitive traffic is going, we allow direct internet access, to keep up the performance. So now we run a security check at the edge of the cloud and then direct the traffic to its destination. This decentralised system, now has a better performance, as the delay from the bottleneck in the previous centralized system has been eliminated. It does not need much maintenance and is less expensive compared to the Centralized Security System. But when we make the switch from the old model to this new one, there could be gaps in security. We are now no longer going through the centralized security stack, and there could be differences with regard to roaming users and branches about how to securely connect and maintain a secure network. And now, with Direct Internet Access, the perimeter that was previously defined is no longer effective, and the castle moat security system becomes very inefficient.

This is where Zero trust security comes in. The zero trust threat model is centred around the idea that data breaches and other security threats result from misplaced trust in internal networks. According to Kindervag, traditional IT security systems make the mistake of accepting that network users are no longer a threat once they've been verified and granted access to the network. In contrast, the zero trust model dictates that nothing outside or inside the network perimeter should be granted complete trust.

Report on understanding and knowledge gathered about Zero-Trust Security framework and architecture:

Coming to the term, "Zero-Trust" is quite self-explanatory. Zero-Trust does not mean that we do not trust, it means we don't blindly trust. This type of security needs the users to verify and authenticate their identity every time and do not

rely on previous verifications either. It means starting from a position of no trust, assessing the trustworthiness of the other, and granting just enough access to get a specific job done.

Cybersecurity is becoming a more important business requirement. The cybersecurity specialist's duty of keeping corporate and personal data safe is affecting more people than ever before as technology becomes more integrated with the professional and personal lives. Professionals in the field of cybersecurity are more likely to concentrate just on the defensive side of the equation. After all, it is the essence of the job to defend when attackers attack.

However, defence is really only half the story. Hackers are constantly refining their skills. They're looking for innovative ways to get into systems and networks, and they're growing rather skilled at evading defences. With all of the new strategies, techniques, and procedures that attackers are employing, the conventional defence-only approach to cybersecurity is no longer sufficient. Many companies are recognizing the importance of creating offensive and defensive tactics, zero trust being one such cyber security tactics. But, now the question arises that which is more important: playing offense or defence?

The offensive aspect

The threat landscape has dynamically changed throughout the years. Hackers are evolving threat craft effectively. As they say in war ‘Know thy enemy’, it holds true for cybersecurity as well. It is important to know your adversary and it is important to understand the tactics, techniques, and procedures, or the TTP. Knowing the adversary is best done through threat intelligence and offensive security. This is one of the key reasons why organizations are keen on changing their cybersecurity landscape from an offensive to a defensive one.

With the explosion of digital transformation and its initiatives, the attack surface has increased exponentially. Systems, data, and the users are not just in the data centres now, like in older times, they are everywhere. To compound all of it, there is a demand for an anytime and anywhere access. So what basically happened is that it is virtually getting impossible to prevent bad things to happen in such a highly distributed and dynamic environment. Early detection and rapid response are two things that can be done to tackle cyberattacks and minimize the scale of damage. This is where offensive security comes into play again.

Offensive strategies also help and improve defensive strategies in terms of bringing in all the learnings and feeding them back as an input to build the defence mechanism. They are used to identify weaknesses in defensive strategies in the form of threat hunting, red teaming, or anything otherwise. Imagine that in a chess game, you want to go offensive. For that, you need to have a solid defence before you go offensive. The feedback that you get from going offensive is then fed back into fortifying the defences. The mindset of organizations has changed. They are no longer only trying to prevent cyber attacks from occurring but to head-on tackle them. The offensive and defensive strategies are used in conjunction to help protect and enable businesses.

Red teaming strategies

Before talking about strategies, let us talk about the different teams in brief. A red team is a team that is trying to emulate an external threat, like someone who's trying to hack into a house. A white team is a team that oversees the engagement between the red and blue teams. Likewise, a blue team is an in-house team that monitors the security controls and defences against attacks. So, what's the work of a red team here? Ideally, its work is to assess the security posture of the organization, the effectiveness of control put in place, the gaps in control, quantify businesses into most real terms, identify weaknesses and help fortify them. The strategy people use here in most of the cases depends on the organization actually.

When a red team isn't successful at being holistic, it does not mean they failed entirely. The very next day they can enable the threat actors to breakthrough. When businesses are blocked with red teaming, it needs to be converted into a white team exercise while providing access to the internal networks and then checking if the situation can be traversed laterally. A lot of feedback can be gathered here if the defence is not strong.

Another stage here is the amalgamation of the red and blue team- known as the purple team. An ideal purple team works together for the sole purpose of improving and strengthening the cybersecurity of a business. This is an advanced version of threat modelling but here it is about practicing the same and not just talking about it. There is never going to be a state when businesses attain a stable cybersecurity model. As threats keep evolving, businesses need to keep evolving every day.

Technologies used for attacks

Certain technologies like bots, AI, and cognitive intelligence are being built into the attack vectors. Many times when organizations do not have an executable routine coming, these attacks sneak in and then start looking for power shells within the organizations to exploit them at the right time based on the information they collect. Companies have witnessed patterns in the past where certain ransomware have been sitting in environments, waiting for over 6 months to gather intel before they even declare themselves as ransomware.

The challenges for organizations today are multi-fold. Organizations are exponentially expanding their digital footprints. What that does mean is, organizations acquire a larger surface area and therefore a larger surface area needs to be protected and controlled. Thus the traditional castle moat security becomes inefficient, and zero trust security gains importance.

Cybercriminals are resorting to advanced tools to attack, which includes offensive artificial intelligence. This makes their attacks more productive, efficient, and successful across all the various stages of cyberattacks. Areas like automating the reconnaissance, crafting tailored impersonation attacks, or hiding identities by going under the radars have become a situation of a regular occurrence. When we talk about offensive artificial intelligence, what we are saying is that the machine learning algorithm is being utilized, supervised, and are incorporated with deep learning technologies.

The core solution to the problem is in the fundamental strategy that organizations adopt as a risk-management framework. Businesses should respond, detect, and identify both on a proactive and reactive basis. Organizations need to hold on to the opportunities that they get in terms of their ability to identify, interpret, and then respond to these attacks. Even the subtlest of the opportunities need to be seized to ensure that these attacks do not breach their systems. Unless organizations resort to the very same technology that is giving them a challenge, they won't be able to keep up with these attacks and will eventually fall prey to many more cyber attacks.

Why Zero Trust Security is Needed:

- Perimeter-Based Security is Ineffective in the Evolving Enterprise

Digital transformations are making traditional perimeter-based cybersecurity models ineffective and irrelevant because perimeters no longer define the scope of security enforcement. So Zero trust security that is also known as perimeter-less security comes into view. nobody gets unrestricted access to the entire system, each request needs to be continuously monitored and verified to gain access to different parts of the network. The zero trust model breaks down the single network perimeter into many tiny, granular microperimeters (a process called microsegmentation). This creates many secure zones that can each be secured individually, each one housing those data and applications that are relevant to a specific work process (or a small set of work processes). Under a zero trust model, only the particular users and devices that need access to a given microsegment are granted authorization to individual secure zones. The smaller the microsegments, the higher the level of security.

- Cloud Data Centres Require Shared Security Responsibility

  The new cloud environment requires a shared responsibility model, where certain security aspects are provided by the cloud vendor and others need to be taken care of by the enterprise. The assumption of trust in the infrastructure is no longer the same. A zero trust model assures this shared cybersecurity responsibility.

- Third-Party SaaS and PaaS Applications Can't Be Trusted Blindly

  Applications now are more likely to be offered as Software as a Service (SaaS) or even Platform as a Service (PaaS).Though they own the core logic and business logic, but they have little ownership of the software components used to build the applications as they use readily available services for authentication, logging, database, machine learning, etc. That means application developers can no longer blindly trust their "own" applications. In the zero trust approach, security controls are deployed with the assumption that the network is already compromised. No unauthorized processes or applications are allowed to execute and authentication is required for access to data.

- The Internet Network is an Unsecured Network

  Applications have moved to the cloud, and users access them remotely. This means that the network is no longer a secured enterprise network. The concept of implicit trust is no longer effective. Zero trust employs

least-privilege and "always-verify" principles, offering complete visibility within the network, whether in data centres or the cloud.

- Everyone in the Expanding Workforce Shouldn't Have All-Access

  Network users are no longer just employees and customers. Many users who access a business's applications and infrastructure could be vendors servicing a system, suppliers, or partners.
  None of these non-employees need, or should have, access to all applications, infrastructure, or business data. Even employees perform specialized functions and therefore do not need complete network access. So zero trust provides access controls and micro-segmentation, and least privilege access principles, which helps ensure no one gets more access than needed.

- You Cannot Verify the Security Status of All WFH Environments

  With a remote workforce, the possibility of unsecured Wi-Fi networks and devices increases security risks exponentially. Without an overarching system like a zero trust framework, whether or not employees are working in a secure environment can no longer be verified.

- BYOD is Not as Secure as Work Devices

  Under the WFH new normal, the devices that workers use are less likely to be ones assigned by the employer. Even if zero trust security can't force employees working at home to use work devices only for work, it can control the potential for a security breach because of the fundamental "trust nobody; verify everything" rule that enforces access controls at every point within the network.

- Cyberattacks Are Increasing

  Also with the increase in cyber attacks, it becomes important to keep in place a proper security model. With zero trust architecture in place we could build a better security posture and become cyber resilient. So it makes us less vulnerable to security breaches and would be better equipped to contain and mitigate financial or reputational damage.

- Advanced Persistent Threats (APTs) Are Becoming More Sophisticated

Now a days cyberattacks could have national, societal, physical, and financial repercussions. Cybercrime is now highly organized and is perpetrated by nation-states, international crime rings, and ransomware groups. These bad actors are sophisticated enough to easily bypass traditional perimeter security. They deploy APTs(Advanced persistent threats) and stealthily move about until they accomplish their goal of stealing information or disrupting systems that have not implemented micro-segmentation or a zero trust model.

- The Security Stakes Are Higher

  Cyberattacks have evolved to target user data, customer data, financial data, and core business knowledge, basically anything that could be valuable. Core government systems, weapons, nuclear power plants, and even elections are at risk. Because the stakes are so high, at every level of society and government, we need robust and resilient cybersecurity strategies. Whether implemented by a multinational enterprise or a government agency, the zero trust framework will improve cybersecurity posture and increase cyber resilience.

Principles of Zero Trust Security:

- All network traffic is untrusted
  A core principle of zero trust security is that all network traffic is untrusted. The fact that some traffic may originate on the corporate network, or even in a highly secure segment of the network, does not entitle it to implicit trust. Because all network traffic is untrusted, all of it should be inspected and logged.
- Micro-segmentation should be applied
  All networks should be finely segmented and access control policies should be enforced between segments. This is known as micro-segmentation. Without this very granular segmentation, attackers who have acquired user credentials or compromised a system can roam freely across the entire infrastructure. So can malicious insiders. As we will discuss, micro-segmentation can be applied not just to networks, but also

to applications, and even individual servers, devices, endpoints, and workloads.

- All entities are low trust
  There should be no implicit trust between any entities in the IT environment. That includes users of all kinds, workloads (whether on physical servers or virtual machines or in containers, in corporate data centres, or on cloud platforms), network and security devices, and endpoints such as servers, laptops, mobile devices, kiosks, and ATMs. Connections between these entities should be allowed only after their identities have been verified and a level of trust has been established.

- Trust should be assessed dynamically
  The trustworthiness of each entity should be assessed and reassessed dynamically, based on all available information about the entity and the situation. For example:
  A user might be assessed initially based on credentials and information available at logon (such as the device used and it's location), then reassessed based on behaviours, such as requests to access applications and volume of content downloaded.
  A workload might be assessed initially based on its function (say, web front end of an ecommerce application) and location (Amazon Web Services), then reassessed based on activities such as connections to workloads in the corporate data centre.

- Trust should always be assessed in the same way
  A given entity should always be assessed using the same criteria. If using a personal mobile device represents a risk, that fact should carry the same weight whether the user is in the headquarters office or at an airport. The final result of the assessment may be different (the use of a public WiFi network at the airport increases risk), but the same tests are applied. To put it another way, if a personal device is risky, it should not be given a free pass just because it connects inside the headquarters office. This approach of providing a uniform, dynamic set of access criteria is behind the concept of "Zero Trust Network Access" (ZTNA).

- The principle of least privilege access should be applied
  The principle of least privilege says that entities should be given access only to those resources they need to perform their intended functions. In the context of zero trust security, that means once a level of trust has been

established for an entity, it should be granted an appropriate amount of access for that level, but no more.

The main benefits of a zero trust model are:

- Superior risk mitigation from closing security gaps and controlling lateral movement on the network
- Improved cybersecurity and support for mobile and remote employees
- Strong protection for applications and data, whether they're in the cloud or an on-premises datacentre
- Reliable defence against ransomware, malware, phishing attacks, and advanced threats

It provides you with full visibility into precisely who (or what) accesses your network — so you know the time, location, and applications involved in every access request. It prevents data breaches by micro-segmentation and isolating high value assets, so lateral movement is restricted, and data can be safe to some extent. Furthermore, limiting what a user can access and how long they can access it goes a long way in reducing the impact of a breach. If access is restricted to only a limited dataset — and is time-bound — attackers have a much lower chance of getting the data they're looking for when they're looking for it. Zero trust can help security staff to work smarter, as it utilizes centralized monitoring, and you can easily generate reliable data stored in a single location. So this facilitates robust analytics, and the team can gain insights they wouldn't have been able to otherwise. So, now the security team can maintain a more secure environment with fewer staff. Zero trust Security is also known as perimeter-less security. Here identity is the perimeter. Firewalls are no longer sufficient now that users are spread across the world, and data is spread across the cloud. Identity is attached to the users, devices, and applications seeking access, so Zero Trust offers robust protection for workers and data in any location.

Working of Zero Trust Architecture:

Implemented properly, a zero trust security model is closely attuned to behavioural patterns and data points associated with all requests made to a

company network. Zero trust security solutions may grant or deny access based on criteria such as:

- User identity
- Geographic location
- Time of day
- Operating system and firmware version
- Device posture
- Endpoint hardware type

Effective zero trust security will be highly automated, and its protections may be delivered via cloud and/or from an on-premises implementation. Identity providers and access management are key components of any zero trust framework, since they provide a variety of critical measures such as:

- **Adaptive authentication**: Authentication type and authorization access based on the results of the user identity, geolocation, and device posture assessment.
- **Multifactor authentication**: Second factors like additional devices and one-time codes may be required on top of a correct password.
- **Single sign-on**: A common set of credentials allows access to multiple applications, and can be granularly managed and revoked at any time.
- **Lifecycle management**: Workflows like employee onboarding and offboarding can be streamlined by assessing and correlating identity directories.

Beyond these fundamental capabilities, specific zero trust security tools can also deliver advanced protection through:

- Network segmentation and traffic isolation
  Cybersecurity solutions such as next-generation firewalls and secure browsers help isolate traffic from the main corporate network. This segmentation curbs lateral movement, reduces risk, and minimizes the damage of a breach even if it does occur. Because risky users are confined to a relatively small subnet of the network, they cannot move laterally without authorization. Under normal circumstances, microsegmentation security policies also help limit access by user group and location.
- VPN-less proxies
  Classic VPNs do not align with zero trust principles, since one-time access gives a user the metaphorical keys to the kingdom. Instead of this castle-and-moat security approach, the zero trust model uses a dedicated VPN-less proxy that sits between user devices and the full spectrum of applications they need, from web and SaaS apps to client/server (TCP and

UDP) based apps, and even unsanctioned web apps. This proxy can enforce granular cybersecurity measures, such as adding a watermark and disabling printing, copying, and pasting on an endpoint if the contextual evidence supports doing so.

- Adaptive authentication and adaptive access
  Adaptive access and authentication allow organizations to understand the state of end user devices without having to enroll them with a mobile device management (MDM) solution. Based on a detailed device analysis, the system intelligently offers the user with a suitable authentication mechanism based on their role, geo-location, and device posture.

- Unified endpoint management
  From one interface, administrators can manage all applications and resources across the enterprise. Unified endpoint management helps keep up with the rapid pace of updates to different applications and operating systems, plus it simplifies any complexity created by mergers and acquisitions.

- Remote browser isolation
  Remote browser isolation redirects the user session from a local browser to a hosted secure browser service when the access occurs on an unmanaged device. This ensures users can access their apps in a sandbox environment and allows them to stay productive. At the same time, this protects endpoints and networks from malicious content from the internet with browser isolation capabilities, creating an airgap from corporate resources.

- Security analytics
  Security analytics solutions amass the valuable data needed for determining what counts as anomalous activity on a network. Networks can intelligently evaluate in real time whether a request is risky and help automate security enforcements based on user behaviour and anomalies detected in the system. This helps reduce manual work for IT, provides timely enforcement, and reduces the risk of breaches.

- SD-WANs
  Software-defined wide area networks (SD-WANs) provide cloud security, including secure direct access to SaaS and traffic encryption,

along with scalable bandwidth and intelligent traffic control for applications of all kinds.

Building a Zero Trust Network Architecture:

Zero trust security is not a single product, but an overarching security framework for continuously evaluating risk and controlling secure access across an environment. Accordingly, multiple solutions, including but not limited to those described above, may be deployed in tandem to support a zero trust model.
The exact process for designing and building zero trust security will vary by organization and solution set, but a common progression will involve:

- Assessing existing cybersecurity controls and determining the key network flows and vulnerabilities.
- Determining a protected surface that will be shielded from harm through zero trust security measures.
- Implementing specific technologies such as adaptive and multifactor authentication, VPN-less proxies, and secure embedded browsers.
- Continuously monitoring the network to keep tabs on suspicious activity and fine-tune the solution mix and overall cybersecurity approach as needed.

Disadvantages of Zero Trust Framework:

Although a zero trust model showcases a comprehensive security strategy, it does make security policies complex. Though the maqin disadvantage is the efforts and time needed to set up the framework and complexity of the Zero trust framework, other disadvantages revolve mainly around this one major drawback, and are listed as follows:

- Needs efforts to set up: Introducing new policies on an existing network is challenging, especially during the transition phase. Sometimes, building a new network from scratch is easier than switching over to the same network. Additionally, if legacy systems are not compatible with the zero trust model, starting a new network would be feasible.

- Needs user-specific policies: Managing company employees for access grants is inevitable. However, the user pool extends to

clients and third-party vendors as they also use company portals or websites. This implies that, with these add-on access points, a zero trust model needs policies in place specific to each group of users.

- More devices to handle: Today, different users tend to use different devices. Each device has a different set of properties and communication protocols. This means that organizations need to implement and update policies to manage the growing number of devices on the network.
- Complex application management: Likewise, applications are of various types. They are generally used across multiple platforms via a cloud environment. Sometimes, they are also shared with third parties. Hence, a zero trust approach requires better application planning, monitoring, and management depending on users' needs.

Conclusion:

Everything has its own advantages and disadvantages, so it depends on how many solutions it provides for our problems, without creating many other problems for us. Zero trust security is seen to solve most of our problems in the security aspect, while creating just one main problem regarding complex set up needed for its architecture and implementation. So we can conclude that Zero trust model is a great security measure that can be implemented by industries to keep themselves safe from cyber-attacks and to avoid security breaches.