LogicFinder
Consulting, Development and Training

Zero Trust Implementation

Introduction:

Zero Trust security, known as zero-trust architecture, zero-trust network architecture, or zero-trust network access is parameterless security. It is an approach to the design and implementation of IT systems. It is an IT security model that requires identity verification for every person and device trying to access resources on a private network from wherever they are.

Background:

Our customer's business deals with the data of both customers and employees and were at risk of losing sensitive information. A data breach happened inside the perimeter. The hackers got inside the firewalls and moved around virtually unchecked with little to no resistance.

The enterprise was at constant risk of cyberattacks as well as vulnerabilities. There was a need for a one-stop solution to cater to the needs of both its cyber environment and network. We deployed Zero Trusted security measures for our customers to be more secure over the network. Our service allowed our customers to be able to access management checked at devices and applications leveled regardless of the device and its networks.

Customer Challenges:

- To ensure that devices are managed and validated as healthy.
- To ensure the identities are validated and secure with multi-factor authentication everywhere.
- To ensure the least privileged access.
- Ensuring the protection of IoT devices, networks, and the platform used.
- To eliminate the risk of data breaches.
- To eliminate the backdoor insertion.
- To prevent and detect computer attacks, malware, attacks on user privacy, and network threats.

Solutions Provided to the Customer:

1. Identity Verification

To enhance the security of the environment, we introduced MFA for administrators who had access to the servers. We then extended this multifactor authentication protocol to cover any user that connected to our resources from outside of the corporate network. This heightened demand for mobile devices to connect to our corporate resources motivated us to modify and update our multifactor authentication system, leading to an improved user experience.

2. Device & Access Verification

We launched device verification by enrolling all devices into a device-management system and finished the roll-out process for Windows, Mac, iOS, and android. We also achieved major progress in segmenting the network, by constructing a number of new user and device segments, which

included the new internet-default wireless network in all buildings. Policy updates were sent out to all users, thus making the new internet-based network their primary option.

3. Implemented New Security Measure

With our cloud services, we added new parameters that existed at the access point itself, which made older security measures virtually obsolete. Data breaches on our customer networks were prevented as a result.

We restricted all employees from accessing the company's sensitive information with Active Directory services and also segmented the networks based on specific needs and positions using multi-factor authentication. This helped prevent the spread of malware on their network.

4. Real-time Monitoring

We ensured the deployment of a Security Information and Event Management Solution (SIEM) and Intrusion Detection Systems (IDS) throughout the network, including OT monitoring capacity.

5. Better Protection

All in all, our service of Zero Trust security offered our clients better protection for users and data. By authenticating and monitoring every user, device, and application in every location, we were able to minimize the risk of a security breach.

Security Flaws Detected:

- An efficient mechanism to defend against computer attacks did not exist.
- There was an old security model that needed to be updated.
- Every user, device, and application was in need to be authenticated and authorized.
- Due to improper testing and configuration, software vulnerabilities existed.
- Real-time monitoring was required.

Company Info

LogicFinder

Website: https://www.logicfinder.net
E-mail: info@logicfinder.net