VIEW POINT

SECURE DIGITAL TRANSFORMATION WITH ZERO TRUST ARCHITECTURE

Abstract

Cyber-attacks are an ever-present threat for enterprises, particularly as IT ecosystems become increasingly elaborate. Ensuring trust across all third parties is complex, yet its absence can severely affect business operations. Therefore, business leaders looking to enhance their security protocols ought to consider operating from a position of zero trust. This paper examines the vulnerabilities that cause IT risk in enterprises. It also explains how zero trust architecture helps deepen security across five key enterprise pillars.

Infosys®
Navigate your next

Introduction

Most organizations are on an ambitious quest to drive digital transformation through cloud and SaaS models for enhanced productivity and operational efficiency. But with the advancement of technologies, there has also been a rise in advanced cyber-attacks. Therefore, securing the IT infrastructure of enterprises and having a robust cyber security program in place has become a business imperative.

Gartner's 2021 CIO Agenda Survey finds that enterprises are spending more on cyber security initiatives than ever before. Out of over 2000 CIOs, 61% reported increasing investments in cyber/information security [1]. In addition, by 2024, 30% of enterprises aim to adopt cloud-driven security technologies such as Secure Web Gateway (SWG), Cloud Access Security Brokers (CASB), Firewall-as-a-Service (FWaaS) capabilities, and zero trust networks from the same vendor[2].

Zero trust networks follow the assumption that one's business is continuously compromised. It is a framework that helps organizations better define their access control strategies and ramp up authentication. It strengthens the security posture of enterprises using the 'secure by design' approach. It leverages the 'Zero Trust Security Architecture Strategy' that allows organizations to integrate security controls into the core of the IT landscape.

Enterprise IT Risks

The current climate of escalating cyber security hazards is due to several factors. More than competition, businesses seek collaboration. They are expanding their relationships with other partners, contractors, and vendors. Information needs to flow seamlessly among these players and within the enterprise, which creates numerous nodes that are vulnerable to security breaches.

There is also a proliferation of personal devices used at work. This trend particularly caught on during the COVID-19 pandemic. Unsecure endpoints added to the enterprise network act as a gateway to threats. A survey by Deloitte found that fraudulent emails, phishing attempts, and spam emails have increased by 25% ever since employees began working from home [3].

Virtualization of enterprise networks is a prominent trend. While physical networks have some form of physical safeguards, virtualized networks need consistent security patches to protect from vulnerabilities. These vulnerabilities include malware, outdated software, misconfigured firewalls, and social engineering attacks [4]. In the same vein, the overall enterprise infrastructure and application landscape need requisite safeguards. Previously, the most significant threats were natural disasters or vandalism. Today, with businesses moving to the cloud, data and application security are more prone to risk arising from improper risk planning and risk design [5].

Data is the most critical asset for enterprises. With the emergence of 5G and IoT devices, siloed data is being pumped into data lakes, making it an attractive target for hackers. It is estimated that an average of $15 Mn is lost every year due to poor data management [6].

Five-tiered Zero Trust Architecture

Zero trust architecture is considered an apt alternative to traditional security architectures.

Most security systems typically aim to thwart cyber-attacks coming from the outside while ignoring internal threats. In zero trust architectures, nothing is trusted without verification and, hence, threats are blocked from traveling through enterprise networks. Enforcing this includes enabling strict data permissions and user authentication, thereby establishing reliable security systems that prevent data breaches or theft.

Zero trust applies in-depth defense across five key pillars of an enterprise's IT landscape.

Users

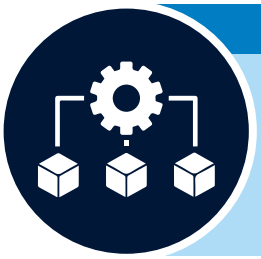
It defines who are trusted users and their access rights through robust policies and procedures aligned to the business. Solutions such as identity and access management as well as identity governance enforce controls, thereby establishing trust between the user and enterprise resources. Some of the leading security controls used are Active Directory (AD), Lightweight Directory Access Protocol (LDAP), single sign-on, multi-factor authentication, biometric, password-less, and consumer access security.

Devices

Zero trust security for devices includes asset discovery, applying security controls to the device's core, and real-time compliance to security posture. Device security controls also involve deploying endpoint detection and response, antivirus, device encryption, device vulnerability management, and mobile device management.

Networks

Implementing zero trust security for networks is possible in two ways. On one level, enterprises should define trust levels, deploy segmentation and micro-segmentation, and enforce policies. At the higher level, they should adopt cloud-first and Internet-first solution strategies based on Secure Access Service Edge (SASE) solutions.



Infrastructure and applications

Zero trust security is mandatory across the enterprise core of infrastructure and applications. Security controls include host AV/EDR, vulnerability management, web application firewall, Cloud Access Security Broker (CASB), container security, APIs, app security, and DevSecOps in the software development lifecycle.

Data

Zero trust security for data begins with identifying, classifying, and encrypting data. Then, enterprises must prevent data loss and leakage, secure storage mechanisms, and institute data recovery techniques. It is important to implement zero trust data security no matter where the data resides, be it real-time, on the cloud, in motion, at rest, or as messages.

Enterprise-wide threat monitoring, detection, automated response, and advanced threat intelligence will always help defend against ever-evolving cyber threats. However, the zero trust architecture strategy takes security to deeper levels by ensuring technical security and enterprise-wide security policies, procedures and standards across all key pillars of business IT.

Conclusion

Cyber security attacks are looming threats for enterprise IT ecosystems due to the rise in user communities, devices and endpoints, network virtualization, cloud-based applications, and poor data management. Hence, organizations must reimagine their defensive strategies and become proactive about enterprise security as they embark on digital. A zero trust framework pervades the five key pillars of enterprise IT and secures users, devices, networks, data, and infrastructure. It enforces additional layers of security to block external and internal threats from flowing undeterred through enterprise networks.

References

1. https://www.gartner.com/en/newsroom/press-releases/2021-05-17-gartner-forecasts-worldwide-security-and-risk-managem
2. https://www.gartner.com/en/articles/the-top-8-cybersecurity-predictions-for-2021-2022
3. https://www2.deloitte.com/ch/en/pages/risk/articles/covid-19-cyber-crime-working-from-home.html
4. https://purplesec.us/common-network-vulnerabilities/
5. https://www.riskmanagementstudio.com/infrastructure-security-vs-evolving-threats/
6. https://www.gartner.com/smarterwithgartner/how-to-create-a-business-case-for-data-quality-improvement

Author

Shambhulingayya Aralelemath
AVP - Senior Principal Technology Architect | shambhulingayya.a@infosys.com

For more information, contact askus@infosys.com

Infosys®
Navigate your next