What is Zero Trust?

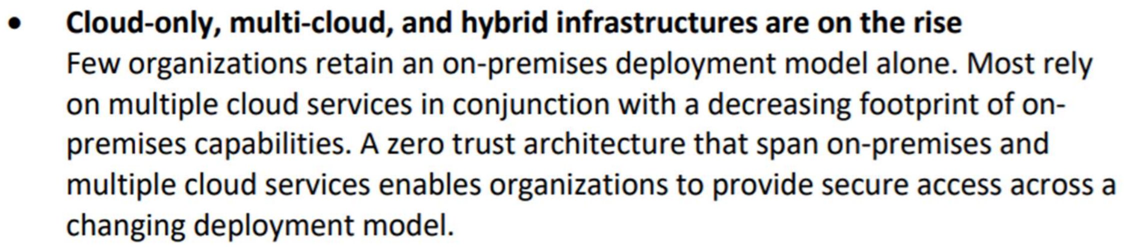
Zero trust architectures address a fundamental shortcoming in how many organizations have traditionally approached security: namely, that people and devices inside the network or a given security perimeter are assumed to be trustworthy. If an authenticated user wants access to data, they get it. If a corporate device is connected to the network, it is treated as a trusted entity. The cybersecurity approach in such situations is to build strong defenses that keep the bad out and let the good in. Over the past several decades, this model has proven to be flawed due to emerging cybersecurity threats, the desire for more convenient ways of digitally interacting with organizations, the recent rapid shift to remote work, and the rise of hybrid deployment models.

Threats, trends, and current issues elevating the need for zero trust include:

- **Insiders represent a significant threat to organizations**
  People inside the network accidentally expose data to unauthorized individuals by misdirecting an email message, falling for phishing campaigns, or using unsanctioned cloud services (e.g., a personal Dropbox account) to speed up a business process or get around IT security policies but failing to secure confidential corporate data when doing so. Other people inside the network act stealthily with malicious intent to steal corporate intellectual property, share confidential data with outsiders, or help cybercriminals to compromise the organization by acting as an accomplice.

- **Compromised devices threaten security posture**
  Corporate devices become compromised through malware, keyloggers, unpatched applications, early-stage ransomware infiltrations, viruses, and other pernicious activity. Left unchecked, such devices can spread infections and vulnerabilities within the corporate network or become a channel through which corporate data is surreptitiously exfiltrated. Device threats are amplified when IT does not control the environment, such as with bring-your-own-device strategies or the use of personal devices with the pivot to remote working.

- **Employees are using compromised networks to connect to corporate data**
  Even before the pandemic of 2020 forced a rapid rethink in work location and the devices used to access work resources for many people, remote access to support mobile workers, ad hoc telecommuting, and work-from-home arrangements had increased. Employees on the road leveraged free Wi-Fi networks in coffee shops and airports, and those working from home relied on consumer-grade Wi-Fi routers to establish connectivity with the corporate office, raising the specter of breached data through network sniffing, malicious hotspots, remote access vulnerabilities, and other forms of surveillance.



- **Cloud-only, multi-cloud, and hybrid infrastructures are on the rise**
  Few organizations retain an on-premises deployment model alone. Most rely on multiple cloud services in conjunction with a decreasing footprint of on-premises capabilities. A zero trust architecture that span on-premises and multiple cloud services enables organizations to provide secure access across a changing deployment model.

Some key takeaways include:

• **Zero trust offers a new approach to cybersecurity** - Instead of assuming users and devices in network were trustworthy, zero trust leverages ongoing verification of trustworthiness

• **Mitigating trends, increasing efficacy, and strengthening cybersecurity protections are the key drivers of zero trust** - Organizations are putting high emphasis on protecting key and confidential data sources from current threats

• **Organizations face a journey to implement zero trust architectures** - Looking ahead many orgs plan to fully deploy zero trust protections within two years or less

• **Technical and resourcing barriers to zero trust currently rate highly** - Transitioning towards zero trust presents a slew of challenges including technical limitations found in legacy systems, and obtaining the appropriate financial and staffing resources

• **Zero trust architectures leverage multiple types of cybersecurity solutions** - Orgs must deploy and integrate a combination of solutions to deliver zero trust architecture

The philosophy of ‘never trust and always verify' has become the foundation of defense against emerging cybersecurity threats. With the shift to remote working, compromised devices and networks as well as internal threats continue to elevate the need for zero trust infrastructure.