As 72% of organizations plan to implement Zero Trust capabilities in 2020 to mitigate growing cyber risk, nearly half (47%) of cyber security professionals lack confidence applying a Zero Trust model to their Secure Access architecture, according to the 2020 Zero Trust Progress Report released by Cybersecurity Insiders and Pulse Secure, globally renowned provider of software-defined Secure Access solutions.

2020 Zero Trust Progress report
The 2020 Zero Trust Progress report surveyed more than 400 cyber security decision makers to share how enterprises are implementing Zero Trust security in their organization and reveal key drivers, adoption, technologies, investments and benefits. The report found that Zero Trust access is moving beyond concept to implementation in 2020, but there is a striking confidence divide among cybersecurity professionals in applying Zero Trust principles.

“Cyberattacks and enormity of data breaches in 2019 has challenged the veracity of secure access defenses”

“The sheer volume of cyberattacks and enormity of data breaches in 2019 has challenged the veracity of secure access defenses, even in well-funded organizations,” said Scott Gordon, chief marketing officer at Pulse Secure. “Zero Trust holds the promise of vastly enhanced usability, data protection and governance. However, there is a healthy degree of confusion among cyber security professionals about where and how to implement Zero Trust controls in hybrid IT environment – which is clearly reflected in respondents’ split confidence levels.”

**Data protection**

Of the organizations building out Zero Trust capabilities in 2020, data protection, trust earned through entity verification, and continuous authentication and authorization were cited as the most compelling tenets of Zero Trust.

The report also discovered nearly one-third of organizations (30%) are seeking to simplify secure access delivery, including enhancing user experience and optimizing administration and provisioning. Additionally, 53% of respondents plan to move Zero Trust access capabilities to a hybrid IT deployment.

**Vulnerable mobile and at-risk devices, BYOD and IoT trend**
More than 40% of survey respondents expressed that vulnerable mobile and at-risk device, insecure partner access, cyber-attacks, over privileged employees, and shadow IT risks are top challenges to secure access to applications and resources.

“Digital transformation is ushering in an increase in malware attacks, IoT exposures and data breaches, and this is because it’s easier to phish users on mobile devices and take advantage of poorly maintained Internet-connected devices. As a result, orchestrating endpoint visibility, authentication and security enforcement controls are paramount to achieve a Zero Trust posture,” said Gordon. While 45% are concerned with public cloud application access security and 43% of respondents expressed Bring Your Own Device (BYOD) enablement issues, more than 70% of organizations are looking to advance their identity and access management capabilities.

Secure Access for Hybrid IT models

“Secure Access starts with appropriate and well-maintained user provisioning but requires entity authentication and compliance checks to invoke conditional access – regardless if a user is remote or on a corporate network, if the device is personal or corporate-owned, or if the application is internal or in the cloud,” said Gordon.

Workforce mobility and hybrid IT models have placed most workloads beyond the shelter of corporate networks and traditional perimeter defense – which creates significant user access and data concerns. The 2020 Zero Trust Progress Report revealed nearly a third of cybersecurity professionals expressed value in applying Zero Trust to address hybrid IT security issues.

Re-evaluating secure access infrastructure

“Organizations at all stages of cloud adoption should re-evaluate their access security posture and data privacy requirements as they move applications and resources from on-premises to public and private cloud environments. Applying a Zero Trust model that aligns to hybrid IT migration will allow organizations to realize utility computing economies while maintaining security and data privacy.”
disruptive way to implement Zero Trust Network Access (ZTNA) functionality when, where and how they require,” said Gordon.

The report highlighted that a quarter of organizations seek to augment their current secure access infrastructure with Software Defined Perimeter (SDP) technology (aka Zero Trust Network Access - ZTNA). “Organizations interested in exploring ZTNA should seek a solution that works in parallel with a perimeter-based VPN to gain essential operational flexibility for enterprises and service providers supporting data center and multi-cloud environments,” said Gordon.

**Hybrid IT deployment**

Of the respondents considering SDP, a majority (53%) would require a hybrid IT deployment and quarter (25%) would adopt a SaaS (Software-as-a-Service) implementation.

“Some organizations are hesitant to implement Zero Trust as SaaS because they might have legacy applications that will either delay, or prevent, cloud deployment. Others might have greater data protection obligations, where they are averse to having controls and other sensitive information leaving their premises, or they have a material investment in their datacenter infrastructure that meets their needs,” said Holger Schulze, founder and CEO of Cybersecurity Insiders.
You may also be interested in...

Pulse Secure And Cloud Distribution Collaborate On Zero Trust Access S...

Pulse Secure, global provider of software-defined Secure Access solutions, has announced a new distribution partnership with Cloud Distribut...

Blending Physical Security With Convenience Is No Simple Task

Back in the 1960s a lead engineer working in conjunction with the United States Navy for Lockheed’s Skunk Works team coined the acrony...

Entrance Control Vs Access Control: Similarities And Differences

Entrance control and access control - of the physical kind - are common terms in the security industry which are often used interchangeably,...

Pulse Secure Appoints Alex Thurber As Chief Revenue Officer To Acceler...

Pulse Secure, globally renowned provider of software-defined Secure Access solutions, has announced that Alex Thurber is joining the executi...