EINPRESSWIRE

Organizations Slow to Transition to Zero Trust Framework

Only 25% of organizations have fully implemented zero trust; lack of knowledge, technical execution and expense are barriers to adoption

NEW YORK, NY, UNITED STATES, October 18, 2022 /EINPresswire.com/ -- Zero trust is widely accepted as a powerful tool to secure complex IT environments and reduce attack surface. Yet adoption levels remain relatively low due to the challenges companies face with implementation, according to a recent survey conducted by CRA Business Intelligence, the research and content arm of the cybersecurity data and insights company CyberRisk Alliance.

Executives recognize the advantages of zero trust – including continuous protection for users, data and assets, the ability to proactively manage identities and threats, consistently enforce security policies, and detect and respond to threats faster. However, the report, based upon the responses of 216 security and IT leaders and executives, security administrators, and compliance professionals in the United States, reveals executives see many difficulties in implementing a zero-trust security model.

“Zero trust is a response to enterprise network trends that include remote users, bring your own device (BYOD), and cloud-based assets that are not located within an enterprise owned network boundary,” according to the National Institute of Standards and Technology. Zero trust focuses on protecting resources (assets, services, workflows, network accounts, etc.)” by transitioning the focus of security on the identity layer rather than the network layer to protect organizations from the theft of critical information.

Implementation is, however, oftentimes complex. In fact, survey respondents described a host of challenges related to the integration of their existing systems into an overall zero trust framework and in shifting from a legacy "all access" model to one that’s limited to just what is needed. According to one respondent, zero trust “is a massive undertaking due to the hybrid workforce that we employ and the sheer number of devices on our network. There is no quick fix; we need to proceed with implementation in a deliberate and careful manner.” Others said budget limitations and inadequate staff to provide oversight or support for a zero-trust model prevents adoption.

For those that haven't yet made the leap, many perceive the transition to zero trust is just too difficult or that it won't be effective. The most prevalent obstacles in adopting zero trust, however, are the lack of knowledge and buy-in from senior management – two key barriers that threaten the widespread adoption of this organizational imperative.

Key takeaways from the survey:

- Zero trust is yet to be widely embraced by organizations as a standard framework for cybersecurity. At the time of this study, only one out of four respondents reported implementation of zero trust by their organizations, although 30% are in the planning/evaluation stage and another 35% said they are considering it.

- Remote workforces and data protection are driving current and future zero trust adoption for most respondents. The largest proportions of current and future zero trust adopters reported top primary drivers to be improved security for their remote workforces (60%) and data protection (59%). Also, roughly half of all respondents said increasingly higher security risks (45%) and the increase in ransomware threats and attacks (50%) compelled their organizations to implement a zero-trust architecture.

- The largest share of zero trust adopters (83%) indicated they implement zero trust for verifying identity. Zero trust is also commonly used for securing devices and endpoints (70%) and internal, wireless, or internet network/environments (64%). This differs slightly for those considering or planning zero trust: nearly three of four (71%) said they are considering or planning to implement a zero trust architecture to help safeguard devices and endpoints, followed by network/environment (61%) and identity (60%).

- Based on respondents' comments overall, implementing zero trust is perceived as a significant undertaking by zero-trust adopters and non-adopters alike. Technical execution was frequently identified as a struggle for organizations implementing zero trust, as is the impact of zero trust on end-user friction and productivity. Among those who said their organization is not using, planning, or considering a zero-trust model, nearly one in four (23%) believed it would be too difficult to transition to a full zero-trust security model, while the same proportion said they didn't have the budget to support it.

- Zero trust champions are organizations who are either currently implementing (45%), planning to implement, or are evaluating zero trust (47%). Champions tend to be large organizations with large IT teams. They believe a zero-trust model is either a very important (54%) or extremely important (43%) component of their organization's overall cybersecurity strategy. Most of them (65%) are driven by data protection as their top motivator for zero trust, and a large majority of them currently implement zero trust to verify identity (83%) or are planning to implement zero trust to verify identity (71%).

The full research report is available for download here.

About CyberRisk Alliance
CyberRisk Alliance (CRA) is a business intelligence company serving the high growth, rapidly evolving cybersecurity community with a diversified portfolio of services that inform, educate, build community, and inspire an efficient marketplace. Our trusted information leverages a unique network of journalists, analysts and influencers, policymakers, and practitioners. CRA's brands include SC Media, Security Weekly, ChannelE2E, MSSP Alert, InfoSec World, Identiverse, Cybersecurity Collaboration Forum, its research unit CRA Business Intelligence, and the peer-to-peer CISO membership network, Cybersecurity Collaborative. Click here to learn more.

Jenn Jones
CyberRisk Alliance
+1 857-328-0173
email us here