CyberRisk
ALLIANCE

FOR IMMEDIATE RELEASE

Contact: Jenn Jones
Phone: (857) 328-0173
Email: press@cyberriskalliance.com

CRA Study: Zero Trust Interest Surges, But Adoption Lags as Organizations Struggle with Concepts

New York, NY, March 31, 2022 – Organizations are keen to implement zero trust architecture but have been held back by a continued lack of understanding about what that entails, according to new survey findings from CRA Business Intelligence, the research and content arm of cybersecurity information services company CyberRisk Alliance.

The survey, sponsored by Attivo Networks and HP Wolf Security, was conducted in January and February 2022 among 300 IT and cybersecurity decision-makers and influencers from the United States. Respondents represented organizations of all sizes and industries. Survey objectives were to gauge how well organizations understand zero trust and to document current deployment and usage trends.

With all the attention focused on zero trust, one could reasonably expect that organizations would be in the advanced stages of implementation, but for many, deployment has been slowed by a struggle to fully comprehend the pieces that embody a zero-trust architecture, as well as lack of budget and boardroom buy-in.

"Despite zero trust mandates within federal agencies, commercial organizations are less familiar with zero trust concepts," said Matt Alderman, EVP, CyberRisk Alliance. "Our current research reveals that management supports zero trust, but budgets are the largest obstacles to implementation, resulting in slow adoption. On a positive note, application security will be the primary benefactor of zero trust spending in the next year."

Among the findings:

- **Only 35% are very familiar with zero trust concepts.** The highest percentage — 40% — are only somewhat familiar, and 25% are "a little" familiar.

- **Only 36% have implemented zero trust,** but another 47% plan to adopt it in the next 12 months.
- **Nearly half of those who have not implemented zero trust are constrained by management/investment.** Twenty-six (26%) percent cite a lack of management support and an additional 23% cite lack of budget.
- **Ransomware attacks and remote worker risks are driving current and planned zero trust strategies.** Specifically, 55% said an increase in ransomware is a motivating factor, 53% point to the increased risks from remote workers, and 32% are driven to implement zero trust out of concern over potential supply-chain attacks.
- **Only 35% are “highly confident" in their zero trust capabilities.** Sixty percent (60%) are moderately confident, and 5% are slightly confident.

This report provides guidance to help security teams move forward - given the challenges outlined by respondents - including recommendations from the U.S. National Institute of Standards and Technology (NIST). The report also explores the practices of “champions” -- respondents who have experienced the most zero trust success.

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, InfoSec World, Cybersecurity Collaboration Forum, our research unit CRA Business Intelligence, the peer-to-peer CISO membership network, Cybersecurity Collaborative, and now Identiverse, ChannelE2E and MSSP Alert. Click here to learn more.

About Attivo Networks

Attivo Networks®, the leader in identity detection and response, delivers a superior defense for preventing privilege escalation and lateral movement threat activity. The ThreatDefend® Platform provides unprecedented visibility to risks, attack surface reduction, and attack detection across critical points of attack, including endpoints, in Active Directory, and cloud environments. www.attivonetworks.com.

About HP Wolf Security

From the maker of the world’s most secure PCs and printers, HP Wolf Security is a new breed of endpoint security. HP’s portfolio of hardware-enforced security and endpoint-focused security services is designed to help organizations safeguard PCs, printers, and people from circling cyberpredators. HP Wolf Security provides comprehensive endpoint protection and resilience that starts at the hardware level and extends across software and services. https://www.hp.com/us-en/security/endpoint-security-solutions.html

###