What Do Agencies Need to Implement Zero-Trust?

Apr 22, 2019 https://www.meritalk.com/articles/what-do-agencies-need-to-implement-zero-trust/

A new report from ACT-IAC (American Council for Technology-Industry Advisory Council) finds that zero-trust technologies are available and lend themselves to incremental installation, but need support from the mission side of the agency for effective implementation.

The report, released April 18, was requested by the Federal CIO Council to explore the maturity, readiness, and suitability of zero-trust technologies for the Federal government. In its findings, ACT-IAC noted that zero-trust technologies are available and have been successfully implemented in the private sector, but require buy-in from the whole agency to avoid perceived failure.

"Zero-trust can be thought of as a strategic initiative that, together with an organizing framework, enables decision makers and security leaders to achieve pragmatic and effective security implementations," the report states.

On the availability side, the report emphasizes that no one company has a holistic solution for sale.

"[Zero-trust] is not a thing you buy, it is a security concept, strategy, and architectural design approach," the report states.

The report also notes that agencies must account for the cost avoidance of prevented breaches in assessing return on investment. Benefits outside of a stronger security posture can include the ability to address compliance audits for policies like FedRAMP, FISMA, and National Institute of Standards and Technology (NIST) publications, re-use of common templates, and the ability to use low-cost commodity circuits.

"As agencies pursue digital transformation goals and deploy more cloud-based applications they need to ensure they leverage a zero-trust model built around the idea that an agency should not inherently trust any user or model," Stephen Kovac, vice president, global government and compliance, Zscaler, told MeriTalk. "To make zero-trust possible, agencies should look to a FedRAMP authorized remote access service that creates dual inside out connections between an authorized user and specific applications using TLS encrypted micro-tunnels, with no inbound listeners."

Agencies also don't have to swallow the entire zero-trust whale in one go.

"If you are planning to include zero-trust in your security strategy, your current environment may already include zero-trust tools and components that can be leveraged," the report notes. Agencies can leverage investments such as strong identity credential and access management and mobile device management. ACT-IAC offers a maturity model for agencies to follow to track their deployment.

Challenges to implementing zero-trust in the Federal government include the wide variety of agencies and different security maturity levels, interdependencies with other Federal agencies and private sector partners, and compliance requirements that don't take the full picture of zero-trust into account.

"It's unlikely to see widespread adoption of zero-trust unless it is designated as a governmentwide priority – All relevant activities associated with zero-trust need to be a key focus for agencies to achieve the desired outcomes," the report states.

For IT departments looking at zero-trust, the report also emphasizes the need to get agency leadership on-board.

"Because zero-trust can affect mission program systems' security, risks, and performance, it is imperative for agency heads and affected program leaders to work together with IT staff on the design and implementation of zero-trust," the report notes.