Zero Trust: Beyond the Buzzword

Evan Pelecky
Product Manager, Cryptographic Key Management
Thales Trusted Cyber Technologies

Zero Trust is not just another buzzword in a never-ending list of tech trends. The principles of zero trust eliminates the binary trust/don't trust approach applied to users and assets in yesterday's on-premises, perimeter-centric environments.

According to a recent survey, 100% of U.S. Federal Government agencies are storing sensitive data in third-party cloud, mobile, social, big data and IoT platforms, which inherently makes data vulnerable. Traditional perimeter protection does not protect off-premise data, which speaks to the need to take a zero trust approach to data security.

In fact, the White House has even issued guidance including the Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems and Executive Order 14028 which require agencies to develop a plan to implement a Zero Trust Architecture. Attend this session discussion to learn about the best practices for implementing a zero trust architecture to protect your most sensitive data.

The speaker will discuss the top 5 things you need to know about zero trust:

- The basics. What is zero trust and how does it apply to data security?
- Setting the stage. How digital transformation can make data vulnerable but also more secure.
- Getting to work. Tips for putting zero trust architecture into action.
- What about the cloud? How does cloud make implementing zero trust faster but more complicated?
- Pulling it all together. How to develop a long-term strategy to protect data throughout its lifecycle that maps to guidance such as CISA Zero Trust Maturity Model, OMB Zero Trust Strategy, DoD Zero Trust Reference Architecture, and NIST Zero Trust Architecture.