PRESIDIO FEDERAL vmware

Federal Cloud Transformation: Navigating Challenges With a Zero-Trust Approach

Digital transformation is a driving force for government agencies, with cloud technology playing a pivotal role. However, the focus isn't solely on adopting modern IT; it's equally about safeguarding it.

The expansive security perimeter of a cloud network poses a significant challenge, considering that every connected device becomes a potential entry point for cyberattacks. Addressing this concern, Zero Trust emerges as a key element in enhancing cybersecurity, particularly in modern IT environments. It extends beyond a singular component, impacting all facets, and operates holistically.

Recognizing its significance, the highest levels of government are actively embracing Zero Trust. In September 2021, the Office of Management and Budget unveiled a draft federal strategy, emphasizing the need for a zero-trust architecture to meet evolving cybersecurity demands. Former National Cyber Director Chris Inglis highlighted the adaptability required to counter adversaries.

Further reinforcing this approach, the Cybersecurity and Infrastructure Security Agency released the Cloud Security Technical Reference Architecture in the subsequent year, followed by the Zero Trust Maturity Model in 2023, providing guidance for implementation planning.

However, embracing new approaches introduces challenges. Ensuring cloud security involves understanding the security footprint at an uncompromised scale, navigating cybersecurity in a hybrid environment, and addressing skills shortages in emerging technologies like cloud and zero trust.

3 WAYS TO LEVERAGE ZERO TRUST

Evolve Hybrid Cloud Strategy: Update strategies for delivering services via both cloud and on-premises technologies. This adaptation is crucial as government employees transition back to office work, ensuring the continuity of zero-trust principles.

Utilize a Common Cloud Abstraction Layer: Enhance zero-trust capabilities by implementing a common cloud abstraction layer. This layer optimizes resource efficiency and fosters consistency in multi-cloud environments, accelerating cloud adoption.

Invest in Training and Recruitment: Address skills gaps by training existing staff and recruiting new talent. The government should evolve job roles and training programs to accommodate next-generation workers in fields such as cybersecurity and cloud technology.

STRATEGIC PARTNERS TO ENSURE MISSION SUCCESS

Elevate your agency's performance with mission-critical solutions. Redefining e-governance, VMware and Presidio Federal customize offerings to address cybersecurity challenges and fortify digital government operations, allowing agencies to seamlessly manage the cloud, proactively prevent threats, and enable a mobile workforce. Discover unparalleled excellence with VMware and Presidio Federal. Get started today at presidiofederal.com/partners/vmware.

Presidio Federal | 12100 Sunset Hills Rd #300A | Reston, VA 20190 | T: 571-789-0390
www.presidiofederal.com