The True Meaning of Zero Trust and How to Implement It Correctly: Context is the New Perimeter

Colby Proffitt
Cyber Strategist
Netskope

Zero Trust is the hot new buzz word - but what does it mean and how can you actually implement it across your federal organization effectively?

Being completely cut off is the only way to achieve 100% trust, but such a "Cone of Silence" approach didn't work for Agent Smart and it won't work for your federal agency if you need to collaborate with others. In reality, every action does not require the same level of scrutiny or protection. Browsing LinkedIn, for example, should not carry the same level of protection as uploading a file.

At Netskope, we believe that context is the new perimeter and Zero Trust (ZT) is an architectural principle with two main purposes:

- Replacing implicit trust with explicit trust, continually assessed and adapted as necessary by evaluating not just identity but all of the context surrounding an interaction to determine what level of access is appropriate
- Concealing resources from the public internet so that they remain undiscoverable (not just inaccessible) to anyone not specifically granted approval

Most security architectures in place across federal agencies today were engineered for a technology ecosystem that has significantly changed over the last two decades. And while the pandemic served as a forcing function, causing many federal organizations to come to terms with the shortcomings of their tooling, practices, and approach to security, the limitations of legacy (i.e., vulnerable) technology solutions were just as debilitating over the last 20+ years as the pandemic was disruptive over the last 18+ months. Traditional security practices and tools are ill-equipped to protect the onslaught of cloud applications and legacy tooling simply cannot meet the requirements of an effective ZT approach.

In this session, you'll learn:

- What Zero Trust really means
- How to implement it quickly in the short-term and correctly over the long-term
- Why context-aware security is critical to a successful Zero Trust implementation

Better security is rooted in the ability to make better business and mission decisions for your federal organization and the ability to make better decisions relies on understanding the risk facing your organization, in real-time with telemetry-rich, data-driven context. Netskope’s approach to ZT empowers federal agencies with the ability to not just secure and protect agency data, but to confidently and continuously control access to, and interaction with, agency data as well.

Please join us to learn about the importance of a layered, context-centric approach, the core tenets to ZT, and how you can secure funding to implement ZT within your federal organization.

.