Zero Trust Is Critical for Managing Your Organization's Network Security

Zero Trust security models hold the promise of vastly enhanced data protection and governance for those organizations willing to adopt a few key principles.

William J. Bender
Chief Information Officer, U.S. Air Force (retired)
Senior Vice President
Leidos

An overarching premise of this viewpoint is that your network is under attack at this very moment and that adoption of a Zero Trust framework can harden your environment against such attacks while minimizing the impacts to your network once compromised.

Digital Transformation is ushering in an increase in malware attacks, IoT exposures and data breaches, because it has become both easier to phish users on mobile devices and to take advantage of poorly maintained Internet-connected devices. Workforce mobility and hybrid IT models have placed most workloads beyond the shelter of on premise networks and traditional perimeter defenses, leading to significant user access and data concerns.

With an ever-increasing number of sophisticated cybersecurity attacks on federal agencies, IT leaders and decision makers are prioritizing Zero Trust Security Architecture to protect their data. While Zero Trust implementations are moving beyond mere concepts, however, there remains a significant divergence of thought among cybersecurity professionals in applying Zero Trust principles. On one hand, the sheer volume of cyberattacks and enormity of data breaches challenge confidence levels in any organization's ability to defend themselves, while on the other confusion reigns as to how and where to implement Zero Trust controls in every organization's uniquely-hybrid IT environment.

Still, Zero Trust security models hold the promise of vastly enhanced data protection and governance for those organizations willing to adopt a few key principles:

- A shift in cybersecurity mindset accepting that a network is already breached (or will be soon)
- A reduction in implicit trust of authenticated users
- An architecture designed to specifically reduce damage caused by attacks
- A prescribed set of incremental steps to improve defenses against advanced cyber threats

Some organizations hesitate to implement Zero Trust because they have legacy applications that could delay or prevent cloud deployment. Others

> Applying a Zero Trust model that aligns to hybrid IT migration can allow organizations to reap the benefits of compute and store economies, while also experiencing a non-disruptive implementation toward Zero Trust functionality.

see themselves having greater data protection obligations, and are averse to having controls and other sensitive information leaving their premises, or may have already made significant investments in data center infrastructure.

Having acknowledged threats exist both inside and outside traditional network boundaries, however, Zero Trust architectures serve to keep the focus on desired business outcomes centered on maintaining user productivity while defending the network from those threats. Applying a Zero Trust model that aligns to hybrid IT migration can allow organizations to reap the benefits of compute and store economies, while also experiencing a non-disruptive implementation toward Zero Trust functionality.

Conceptually, Zero Trust architectures eliminate implicit trust in any one element, node or service by requiring continuous verification of the operational environment via real-time information from multiple sources to determine access and other system responses, while also focusing on protecting data in real-time within a dynamic threat environment. To achieve this requires comprehensive security monitoring, granular, risk-based access controls and overall security system automation.

Again, committing your organization to a Zero Trust strategy requires a cultural mindset shift from multi-layered perimeter network defenses to an acknowledgement your network has already been breached. Hence, the primary objective changes to minimizing the impact. Zero Trust, done right, implements a comprehensive set of mitigation protocols including software-defined perimeters, micro-segmentation for more granular identity and access management controls and a series of identity aware proxy controls via continuous authentication and user-based access.

In the end, Zero Trust requires commitment to an adaptive defense strategy and sustainable threat protection as the best way to secure and protect the data that matters most to your organization. ■

About The Author

Lt. General Bender (retired) most recently served as CIO for the Air Force, where he was responsible for 50,000 cyber operations and support personnel across the globe with oversight for the USAF's IT investment strategy and a portfolio valued at $17 billion. After retiring from the Air Force following a 34-year career there, Lt. General Bender joined Leidos in September 2017. Now tasked with overseeing and managing the Strategic Account Executives, a group of customer-facing senior-level former government officials, Lt. General Bender aims to bolster customer relationships and advance strategic initiatives to foster organic growth.