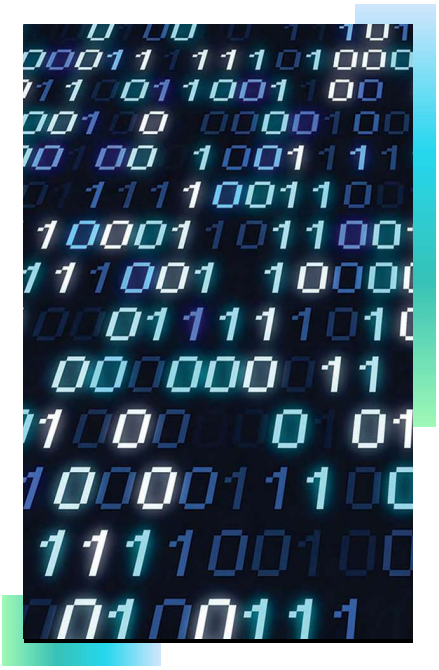
DELL TECHNOLOGIES

Embedding zero trust into modern systems

A comprehensive approach to cybersecurity that includes zero trust is integral to the success of IT modernization

Jeremy Browning
Dell Technologies



The threats facing federal IT systems and critical infrastructure are continually expanding, and the attacks are growing in complexity to keep pace with advancements in artificial intelligence. Although AI holds tremendous promise for helping agencies leverage data to drive better mission outcomes, it also provides bad actors with new and efficient ways to penetrate IT systems.

Given that data is the digital currency that unlocks value, securing data must be paramount to protect its quality and value. Therefore, cybersecurity must be a key consideration in any IT modernization effort. If an agency doesn't build a solid security foundation into its IT planning, its modernization efforts will be at risk.

A long-standing cybersecurity principle

Zero trust plays a crucial role in securing modern IT systems. It is not a new concept but rather a long-standing cybersecurity principle that focuses on continuously validating users and limiting access to only what an individual, system or application needs to complete its authorized tasks. The federal government's recognition of the increase in internal and external risks has led to stricter requirements that government and critical infrastructure systems adhere to zero trust controls.

The best way for agencies to achieve success is to incorporate zero trust early in their IT modernization planning. Historically, many IT companies and agencies prioritized the core functionality of a service, application or capability to drive mission or business outcomes, and considered security only afterward. This mindset can create significant challenges because funding might run out before zero trust goals are met. In addition, retrofitting security into established products or processes can unintentionally introduce costly risks.

However, when security is treated as a core requirement during design and planning, it becomes an integral part of the solution life cycle, driving savings while ensuring stronger integration into enterprise IT operations.

Legacy infrastructures and funding challenges

Although it would be easier to implement zero trust controls with a greenfield solution (by starting with a new IT infrastructure), most agencies are bound to legacy infrastructures that have been built up over decades. These infrastructures represent massive investments and include systems that are difficult to upgrade or migrate due to various technical and institutional limitations.

ADOBE STOCK// MYVECTOR

At Dell Technologies, we have developed the capability to consult with agencies to understand their IT modernization goals and zero trust mandates, and then we help them develop an approach that will drive zero trust maturity in areas of their enterprise infrastructure identified as deficient. We also work with agencies to leverage our ready infrastructures, developed with our extensive partner community, to take a greenfield approach where it makes financial and operational sense.

One of the biggest obstacles to IT modernization is funding. Some agencies approach these challenges with a capital expenditures model, which involves significant upfront costs for purchasing and upgrading hardware and software. For agencies with limited budgets, this approach can make it difficult to invest in a modern IT infrastructure. Furthermore, capital expenditures are often rigid in terms of budgets and timelines.

"GIVEN THAT DATA IS THE DIGITAL CURRENCY THAT UNLOCKS VALUE, SECURING DATA MUST BE PARAMOUNT TO PROTECT ITS QUALITY AND VALUE."

However, many agencies have worked with Dell Federal and Dell Financial Services to develop a strategy that leverages a mix of capital expenditures, operational expenditures and discretionary funds available throughout the year. This well-planned modernization model allows for more flexibility and better alignment with financial and operational needs. ■

Jeremy Browning *is federal civilian sales director at Dell Technologies.*