The 7 pillars of a **zero trust architecture**

Dell's model helps agencies assess their current cybersecurity framework and achieve a highly secure digital transformation

Daniel Carroll
Dell

Last year's Executive Order on Improving the Nation's Cybersecurity mandates a zero trust approach, and though the order has a particular focus on federal agencies, it is also aimed at protecting critical infrastructure. That broad view reflects the realization that we need to come together as a community to protect all our interests. The bad actors outnumber us tremendously, and increasingly complex networks are difficult to protect.

Zero trust offers a way to secure today's IT networks and therefore must be at the center of the government's efforts to achieve an effective and safe digital transformation. Otherwise, bad players could disrupt all the progress agencies are making and render the transformation ineffective.

Security policies that are easily understood

Zero trust is based on the principle that all users, devices and applications should be validated before they are allowed to access the network. To ensure success, however, security policies must be easily understandable for everyone who's involved in the life cycle of technology. That includes the employees who work in procurement and contract management, for example, as well as the IT team.

Leveraging the tenets of the National Institute of Standards and Technology's guidance on zero trust architectures, Dell Technologies developed a seven-pillar model that helps IT leaders explain zero trust principles and their importance to agencies' cybersecurity efforts. The pillars are:

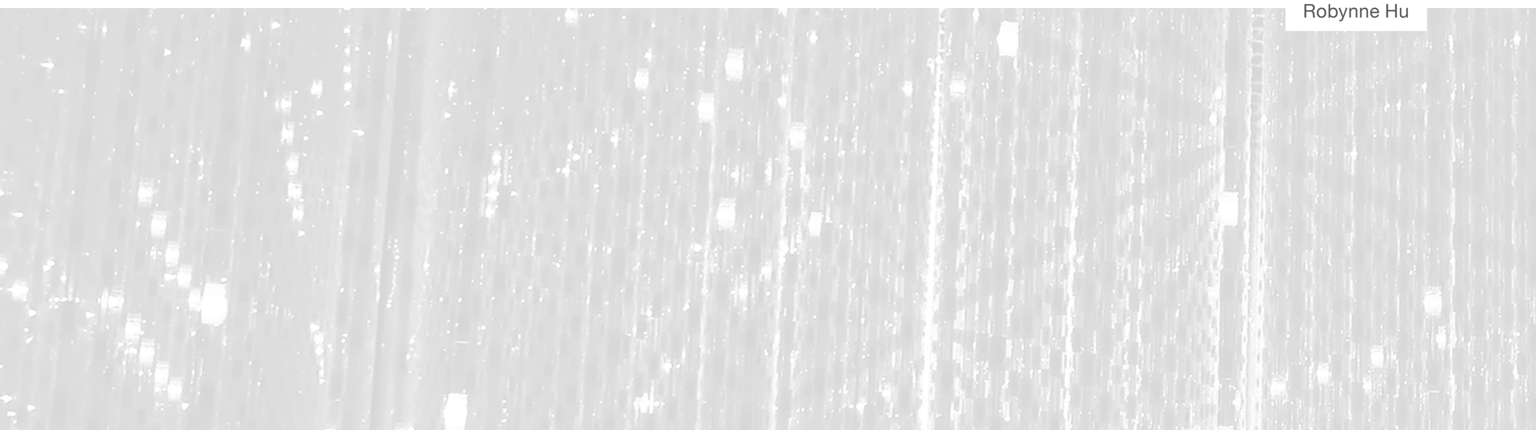
- Device trust
- User trust
- Transport and session trust
- Application trust
- Data trust
- Visibility and analytics
- Automation and orchestration

The first five are relatively self-explanatory, and the last two provide a basis for enforcing them. For example, if a device is acting in a way that's unusual, then the visibility and analytics component will highlight the activity so the automation and orchestration component can cut off the device's access and protect the infrastructure.

Taking stock of existing tools

Agencies already have substantial investments in cybersecurity tools they can leverage as they move to zero trust. They can start by taking stock of the applications, practices and services they are currently using that support zero trust principles. Which ones are missing? And which tools does an agency have that it's not using?

New products are often deployed without enabling their full security capabilities, so agencies should consider what untapped features in



Robynne Hu

> “Ultimately, **agencies must be able to identify everything within their networks** — not just users, but also devices and applications.”

their existing tools could help them enhance their cybersecurity posture. Then they can identify what they need to purchase to fill any gaps.

Ultimately, agencies must be able to identify everything within their networks — not just users, but also devices and applications. Zero trust involves validating that those objects are authorized to access agency resources and blocking any new objects that don’t come onto the network in the appropriate way.

Similarly, data governance is necessary to understand where data is, who owns it and who or what should have access to it. Some observers like to believe that Edward Snowden was a master hacker. But he simply walked into a data center, plugged in a USB drive and copied a massive amount of files to that drive. There was a failure in the cybersecurity framework and potentially in the background-check process, but the reality is that he was able to access massive amounts of data that he should not have been able to access.

It is a picture-perfect example of a situation that a zero trust architecture is designed to prevent. ■

Daniel Carroll is field CTO for cybersecurity at Dell Technologies.