DELL Technologies

Trust, But Verify

The federal community is ready for Zero Trust.

By Cameron Chehreh

Zero Trust doesn't actually mean "trust no one." It means, to quote former President Ronald Reagan, "Trust, but verify." Trust isn't given without validation. In the past, access may have been more open in a bid to simplify IT processes, but that came at the cost of security.

The U.S. Department of Defense has said its next-generation cybersecurity architecture will be based on Zero Trust principles. With the Center for Strategic and International Studies and McAfee reporting that estimated global loss from cybercrime would near $1 trillion, I think that's a sound approach. As we wrap up the 18th annual Cybersecurity Awareness Month, it's more important than ever that federal agencies follow the theme assigned to this last week of October: Cybersecurity First.

Zero Trust is a great place to start the discussion. Zero Trust doesn't actually mean "trust no one." It means, to quote former President Ronald Reagan, "Trust, but verify." Trust isn't given without validation. In the past, access may have been more open in a bid to simplify IT processes, but that came at the cost of security. We also know that threats often come from inside the enterprise, and many are a result of inadvertent actions by employees or a failure to adopt basic cybersecurity principles such as updating systems to close known exploits. Cyberattacks today are increasingly brazen and unfortunately, harder to detect. The technology we are using – AI, ML, the Internet of Things – to transform our government's digital future is being weaponized and used against us. So how do we use Zero Trust to combat this?

It's important to understand that Zero Trust is not "the thing." There is no silver bullet or a single product that is Zero Trust. It is a set of cybersecurity principles applied across everything you do within your architecture. Federal agencies need to determine what task or mission they're trying to solve for. The more specific the area of focus, the more effective the solution.

Dell Technologies has an emerging seven-pillar model for Zero Trust built from multiple sources such as standards from NIST and the U.S. Department of Commerce Bureau of Industry and Security, and requirements from executive orders. For now, I'm going to focus on three of the most critical: data trust, device trust, and transport and session trust. In each zone of an architecture built with Zero Trust principles, access is granted by exception. Just because you've made it through the front door, doesn't mean you're invited to visit every room in the house. If at any point there's a failure to validate your identification, your access is terminated. Immediately. This prevents a malicious actor from "sitting" on your network undetected. Agencies are discovering cyberattacks too long after they occur, which leaves them open to a far wider invasion of their networks or data centers.

The application of a Zero Trust principles is similar to the structure of a Navy ship. You want to be able to seal off, from inside, the part of the boat that's been breached to limit the chances of the entire ship flooding and sinking.

The application of a Zero Trust principles is similar to the structure of a Navy ship. You want to be able to seal off, from inside, the part of the boat that's been breached to limit the chances of the entire ship flooding and sinking. How will you section off your data center so you can move quickly to seal off a leak and prevent it from getting to other areas?

With the proliferation of the bring-your-own-device approach to connect remotely with work, the need to secure hardware is essential. Our next pillar, device trust, also covers larger "devices," like data center infrastructure, client endpoints and switching architecture. At Dell Technologies, we focus heavily on this area. Many of our solutions include features that support the current Zero Trust model. For example, our supply chain risk framework mirrors that of the comprehensive risk management framework of the National Infrastructure Protection Plan, which outlines how government and the private sector can work together to mitigate risks and meet security objectives. Our framework incorporates an open feedback loop that allows for continuous improvement. Risk mitigation plans are prioritized and implemented as appropriate throughout the entire solution life cycle.

Establishing transport/session trust means you have enacted micro-segmentation to better control who and what is utilizing which protocols to access devices and data. Network segmentation has been around for some time, but it was difficult to make it truly operational, and equally challenging to maintain at enterprise scale. By leveraging software-defined networking, and applying Zero Trust architectural principles, we can now scale the enterprise. This means an agency can accomplish complex tasks more simply through automation. Automation makes user-profile verification and user behavior heuristics more easily accessible as methods of identifying and isolating anomalies that could signal intrusion into your network.

Our commitment to our government customer is shared by industry-leading solution providers with whom we partner to deliver fully realized solutions that can support Zero Trust at the endpoint, data center, edge and in cloud environments. We also bring partners together to solve complex security challenges to meet the highest federal security requirements.

The federal government has made great strides already in implementing the pillars I mentioned earlier, like device and application security. They are moving toward Zero Trust principles as well, and I'm certain that evolution will proceed apace. What we've learned from the pandemic is that civil employees can rise to the challenge and accomplish their missions from almost anywhere. We've got a lot of work to do, and I'm eager to see us succeed.

About the Author: Cameron Chehreh

Cameron Chehreh is the Chief Technology Officer and Vice President of Presales Engineering at Dell Technologies Federal. In this role, Cameron is responsible for strategy execution, leadership, and innovation management for Dell Technologies' technology portfolio for the Civilian Government, Department of Defense and Intelligence Community markets.

DELL Technologies