studio 2G + Red Hat | TD SYNNEX Public Sector | DLT

Redefining Security:

Bringing Zero Trust Architecture to the Public Sector

What exactly does it mean to implement zero trust architecture? At a recent session at Nextgov's CyberDefenders summit, industry experts discussed how agencies can get started on their ZTA journey. Here's what they had to say.

Introduction

After a year of prolific cyberattacks — from the SolarWinds breach to the Colonial Pipeline Hack — it has never been more important for government agencies to prioritize their security posture. Increasingly, they're turning to zero trust architecture to keep their networks safe from attack.

But what, exactly, does it mean to implement zero trust? And why are more organizations taking this approach? At a recent session titled, "Zero Trust Is a Team Sport," sponsored by Red Hat and part of Nextgov's CyberDefenders summit, industry experts discussed how agencies can get started on their ZTA journey.

Here's what they had to say.

1. Define Zero Trust for Your Organization

Step 1

According to Michael Epley, chief architect and security strategist at Red Hat, agencies need to understand what ZTA is before knowing when and how to implement it.

"Zero trust [is] the future of security," he said. "It's built around the concept of assuming breaches in your enterprise, and building your appropriate zero trust security boundaries throughout that enterprise and allowing access controls only where appropriate."

The cybersecurity executive order, released in May 2021, refers to zero trust as "a security model, a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgment that threats exist both inside and outside traditional network boundaries."

In essence, ZTA assumes no user or application attempting to access a network should be automatically trusted.

Zero trust [is] the future of security. It's built around the concept of assuming breaches in your enterprise, and building your appropriate zero trust security boundaries throughout that enterprise and allowing access controls only where appropriate."

MICHAEL EPLEY
Chief architect and security strategist at Red Hat

2. Successful Zero Trust Implementation

Step 2

John Dvorak, a Chief Architect and zero trust evangelist at Red Hat, added there are a number of capability models that help illustrate the ZTA implementation process. He pointed to a chart shared via the ATARC Zero Trust Lab that allows companies to map product capabilities against ZTA core pillars including data, device and endpoint, network and environment, application and workload, user, visibility and analytics, and automation and orchestration.

"This visualization shows you how complex the capabilities are compared to the different core pillars of zero trust security," he noted.

That level of complexity cannot be solved by a single vendor. Instead, Dvorak said solution providers and partners should play to each others' strengths.

"The takeaways here is that no one vendor, no one open-source project, is going to cover [all architecture requirements]," he explained. "We need a holistic approach and we need to work together as a community to come up with solutions to address zero trust."

Red Hat has built relationships with trusted partners to help organizations implement this security framework. For instance, it partners with companies that focus on microsegmentation, encryption, identity management and workload security.

"We believe the best way to address our customers' zero trust journey is through a trusted ecosystem that brings together the best of the open-source community and our diverse industry partners," Dvorak said in another statement. "We like to say 'Better Together' when it comes to great technology and business solutions, and this has never been more true than it is today when tackling zero trust."

"The takeaways here is that no one vendor, no one open-source project, is going to cover [all architecture requirements]. We need a holistic approach and we need to work together as a community to come up with solutions to address zero trust."

JOHN DVORAK
Chief Architect and zero trust evangelist at Red Hat

3. Open-Source Technology Is a Key Component of ZTA Success

Step 3

An open-source approach, which grants users the right to modify, study or distribute the software's source code, helps enable this type of collaboration without compromising security, Dvorak said.

According to a recent Red Hat survey of more than 1,200 users, 87% of polled IT leaders identified open source as either more secure or as secure as proprietary software.

"We see this uptick [in open source] every year," Dvorak said. "To address zero trust, we feel very strongly that the open-source community and the open-source projects, as well as the vendor communities out there working together, will provide a better, holistic approach to securing enterprises in the future."

The same survey asked users what they believed to be the top benefits of using enterprise open source. The responses? Higher-quality software (35%), access to the latest innovations (33%), better security (30%) and the ability to safely leverage open source technology (30%).

"Open-source software has become pervasive, and it has become an engine for innovation as well as security," Epley said.

Red Hat helps fuel that engine by curating open-source projects. The organization participates in open-source community discussions and events, sponsors and works alongside developers and customers, and then applies rigorous software development processes to turn open-source projects into enterprise-ready platforms.

"[We are] applying security best practices, hardening and testing validation of those products and technologies, thus providing the stable platforms that we can build zero trust and enterprise architectures around," Epley added.

Ultimately, Red Hat's goal is to bring open-source innovation to an enterprise — but without the risk. Indeed, its entire supply chain is built around reducing risk and making open source more consumable for an enterprise. Due diligence, like testing, security scanning and validation are key to open source and ZTA success.

Red Hat has also embarked on a new project called Signature Store. The goal? Improve open-source software supply chain security. Sponsored by the Linux Foundation, Signature Store is a collaboration between Google and Red Hat bringing DevSecOps to the ZTA implementation process.

Step 3

"We're trying to build [a] community and raise awareness in this space," Epley said. "That is the mission of everything we do, to be that catalyst between communities and customers, contributors and partners to help . . . facilitate technological innovation."