

# WHY ZERO TRUST MATTERS AT WORK

*(and how to foster it)*



# Practical Ways to Make Zero Trust a Reality and Add Value

*An interview with Michael Epley, Chief Architect and Security Strategist, Red Hat*

True zero trust is not a single tool or technology, and there is not an end state. But it does not mean you have to wait months or years to see the fruits of a zero-trust strategy.

**“Enterprises can get immediate value from zero-trust architectures, even as they face a long and maybe never-ending journey ahead,”** said Michael Epley, Chief Architect and Security Strategist at Red Hat, which specializes in enterprise open source software innovation. “Its fundamental concepts have been around a long time and are here to stay (even if the buzzwords change).”

Reactive security is not enough to tackle today’s challenges. It assumes access granted to the network implies trustworthiness. And that is not the case. Zero trust proactively combines people, processes and technology across a wide set of domains to constantly verify identity and allow necessary access.

As you map out your journey, here are some practical approaches to consider.

**Establish a zero-trust tiger team or center of excellence.** This specialized team should be fully familiar with core principles, White House guidance and any agency plans. This team will help to evaluate your agency’s zero-trust readiness against a maturity model.

**Ensure zero-trust pillars are represented** by team members actively working in those focus areas (identity, device, network, application and data). Coordination throughout the journey capitalizes on existing tools or automation and is needed for consistent access enforcement.

**Address siloes.** Strong, centralized and consistent user identity is foundational across all the zero-trust focus areas. It is critical your agency transforms any existing siloes of identity into a more agile and distributed architecture that’s integrated with enforcement platforms departmentwide.

**Perform comprehensive technology surveys** and asset accounting to prevent overlooked areas and map out necessary access criteria. Identifying and tagging data assets is also key for defining what needs protecting and how.

**Define zero-trust minimum viable products.** Determine realistic incremental stages for your agency, define each protection surface, and plan a solution to meet the requirements in the timeframe necessary.

**Perform user acceptance testing** with a well-defined rollout and rollback plan at each incremental stage to ensure daily work is not negatively impacted.

“The most visible change, if any, for employees will be how they interact with systems,” Epley said. Access will no longer be assumed. Although this change could alter normal workflows, context-driven solutions cannot be cumbersome to the workforce. Any burden increases risks of non-compliance and encourages shadow IT.

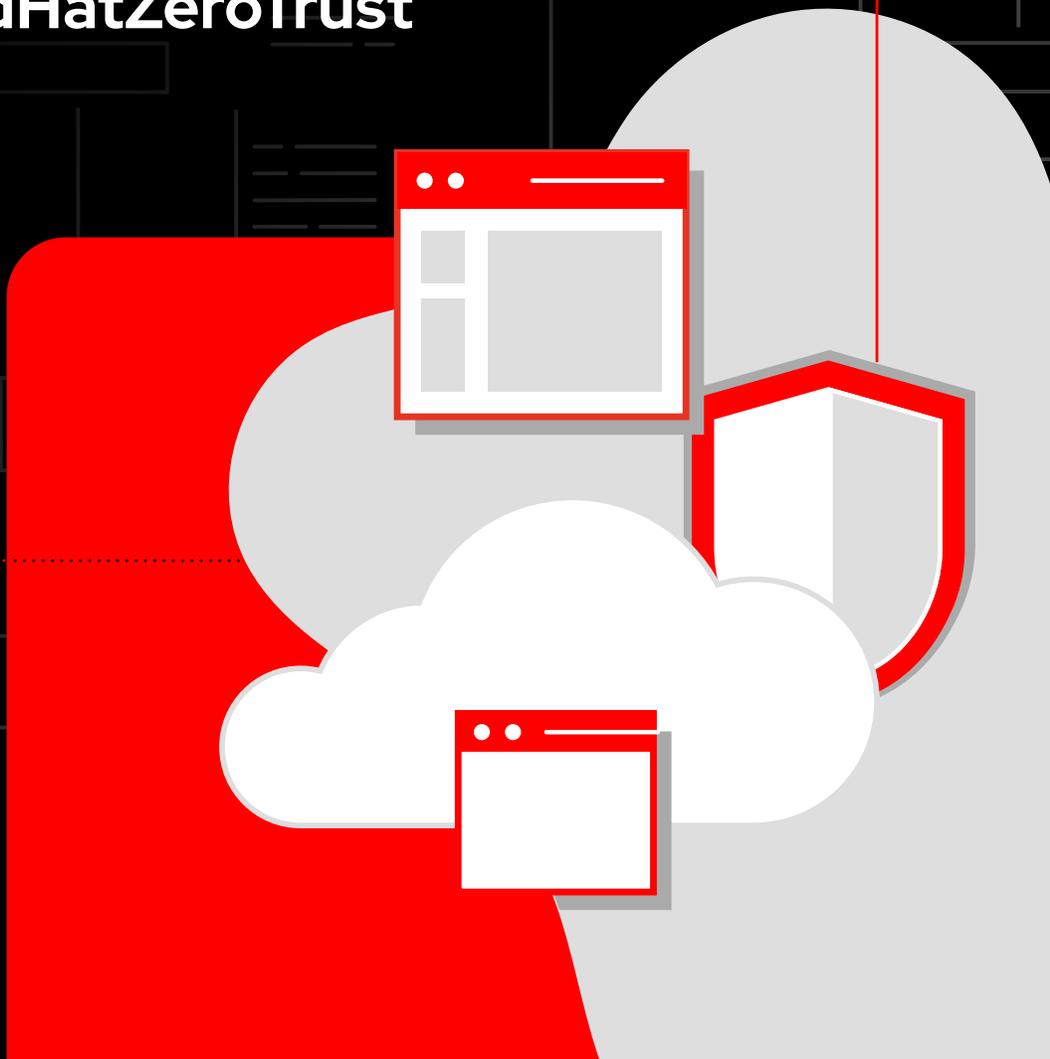
Ultimately, zero trust is not a one-and-done activity. “The most important reason is the ever-evolving set of business needs and functions, implemented by new people, roles and resources,” Epley said. “Cybersecurity is a constant arms race, and our systems must continue to evolve to address new threats, risks and vectors.”



# Zero Trust Identity Architectures

Discover best practices for integrating and managing user and system identities in a Zero Trust system.

**Watch Now:**  
[carah.io/RedHatZeroTrust](https://carah.io/RedHatZeroTrust)





---

Thank you for downloading this Zero Trust GovLoop Guide featuring Red Hat! Carahsoft is the Master GSA and SLSA Dealer and Distributor for Red Hat Enterprise Open Source solutions available via GSA, SLSA, ITES-SW2, The Quilt and other contract vehicles.

To learn how to take the next step toward acquiring Red Hat's solutions, please check out the following resources and information:



For additional resources:  
[carah.io/RedHatResources](https://carah.io/RedHatResources)



For upcoming events:  
[carah.io/RedHatEvents](https://carah.io/RedHatEvents)



For additional Red Hat solutions:  
[carah.io/RedHatPortfolio](https://carah.io/RedHatPortfolio)



For additional Open Source solutions:  
[carah.io/OpenSourceSolutions](https://carah.io/OpenSourceSolutions)



To set up a meeting:  
[redhat@carahsoft.com](mailto:redhat@carahsoft.com)  
877-RHAT-GOV



To purchase, check out the contract vehicles available for procurement:  
[carah.io/RedHatContracts](https://carah.io/RedHatContracts)