What makes Zero Trust the right model for cybersecurity now?
Security incidents are trending in the wrong direction, and we need to change our collective approach. Many enterprises continue to rely on castle-and-moat security models which put the protection at the perimeter and are easily bypassed by modern attacks. Once hackers breach the firewall, they can easily move around the network.
Zero Trust removes this concept of network-based implicit trust. It retrains our security models to demand architectures that rely on explicit, context-based authentication and authorization. In other words, we take nothing for granted when it comes to any request for access, and we assume the worst until we can prove the best.

Who needs to be involved for Zero Trust to be successful?
Cybersecurity is a team sport, involving more than just the security and IT staff. While this has always been true, we have normalized a culture where security and IT often make access decisions in isolation and business leaders don’t always understand their role. To define what needs to be protected and how we will protect it, technical teams need the active participation of product owners, agency risk managers, application developers, data stewards and other interest groups.

How can open-source software contribute to a strong security solution?
Open source taps into a broad community of ideas and knowledge to bring new security solutions to market. Most major technology companies are contributing today to open source, reducing the time it takes to build new capabilities. The code itself is visible and inspectable by third parties, which provides opportunities to recognize and correct bugs. This contrasts with closed-source development, which typically relies on trust in a single vendor to inspect and correct their own code. No code process is without risk, and open source is no exception.

That’s where companies like Red Hat come in. We have the resources, expertise and incentive to deliberately perform code analysis on open-source components before we release code to customers, lowering risk. In true open-source community fashion, we report those findings back to the upstream communities, allowing everyone — including competing products — to benefit.

What are the key steps for getting started with Zero Trust?
Two steps are essential: First, define the data, applications and systems that need protection. Second, map the transaction and data flows among them. Ensure success on this long journey and begin by choosing one major, modern system to validate in a proof-of-concept project that will help everyone understand and gain confidence in Zero Trust.

Based on the outcomes of that project, next steps include defining centralized identity providers and developing standard policies for data access. Finally, recognize that some legacy systems may never be able to fully support the identity tenets of Zero Trust until we can upgrade or replace them. However, there are other pillars of Zero Trust that emphasize defense-in-depth concepts around network micro-segmentation, software run-time protection, isolation through one-way transfer devices, and other techniques.