We surveyed IT leaders around the world to determine how they’re implementing Zero Trust authentication, enabling secure access to apps and services, and reducing stress on legacy IT systems. A Zero Trust approach helps alleviate these challenges by strengthening user authentication and policy-based adaptive access. IT leaders are now turning to a Zero Trust security model to meet their new requirements.

Organizations have been digitally transforming at warp speed in response to their employees working remotely and evolving global business operations. As a result, digital identities have become the single most exposed resource as employees access corporate resources from new devices in new locations.

Securing identities with Zero Trust

Most organizations have also implemented risk analysis to add a layer of real-time threat detection and alert automation. However, while the majority of organizations have implemented Zero Trust security controls—such as strong authentication and policy-based adaptive access—implementation of AI-based threat detection and alert automation is lagging behind.

Zero Trust is still in its infancy for many organizations

We asked IT executives at different company sizes how confident they are in their Zero Trust identity management roadmap. 79% of respondents said they are confident in their Zero Trust identity management roadmap, while 16% said they are somewhat confident and 5% said they are not confident. This suggests that while many organizations are making progress with their Zero Trust implementation, there is still a lot of work to be done to fully realize the benefits of this approach.

Pillars of a Zero Trust framework

In the following survey, we asked IT executives to rate the importance of different pillars of the Zero Trust framework within their organizations. 82% of respondents said that securing devices and identities are the most vital pillars of their Zero Trust framework, while 18% said that data security is the most important pillar. This highlights the importance of strong authentication and policy-based adaptive access in securing user access and protecting sensitive data.

To learn more about how Microsoft Azure Active Directory can help streamline and strengthen your Zero Trust implementation, visit microsoft.com/security/business/identity.