Securing identities with Zero Trust

Organizations have been digitally transforming at warp speed in response to their employees working remotely and evolving global business operations. As a result, digital security teams have been under immense pressure to ensure their environments are resilient and secure. Many IT leaders are finding that their traditional security controls aren't scalable enough to support this transformation and their organization is being exposed to unnecessary risk.

IT leaders are now turning to a Zero Trust security model to meet their new requirements. A Zero Trust approach helps alleviate these challenges by strengthening user authentication, enabling secure access to apps and services, and reducing stress on legacy remote work solutions—all while providing a seamless and productive user experience.

We surveyed IT leaders around the world to determine how they're implementing Zero Trust practices to provide secure remote access to corporate resources without impacting productivity.

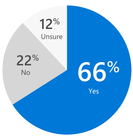
1 MOST IT LEADERS ARE USING ZERO TRUST IDENTITY MANAGEMENT AND MOMENTUM IS PICKING UP

76% of companies currently say Zero Trust is the backbone of their access strategy, indicating its widespread adoption. The shift to remote work has accelerated adoption, as IT leaders are tasked with keeping data secure as employees access corporate resources from new devices in new locations.

66%
of IT leaders have invested in Zero Trust in the past 3 months.

WITHIN THE PAST 3 MONTHS...

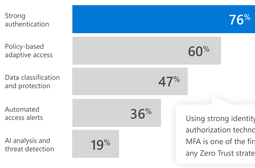
HAVE YOU MADE INVESTMENTS INTO ZERO TRUST PRACTICES?



HOW MANY COMPANIES IN EACH INDUSTRY HAVE IMPLEMENTED ZERO TRUST?

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.

WHAT IDENTITY-RELATED ZERO TRUST SECURITY CONTROLS HAVE YOU ALREADY IMPLEMENTED?

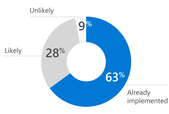


Using strong identity authorization technologies like MFA is one of the first steps in any Zero Trust strategy.

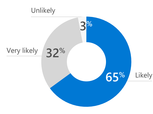
2 MOST ORGANIZATIONS PRIORITIZE MFA AND SSO

The majority of organizations (**63%**) have already implemented multi-factor authentication (MFA) to secure identities, which is the first step in any company's Zero Trust journey. **97%** of respondents say they'll implement single sign-on (SSO) in the near future.

HOW LIKELY ARE YOU TO IMPLEMENT MFA TO SECURE IDENTITIES IN THE NEAR FUTURE?



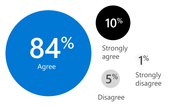
HOW LIKELY ARE YOU TO IMPLEMENT SINGLE SIGN-ON (SSO) IN THE NEAR FUTURE?



Most organizations have also implemented risk analysis to add a layer of real-time protection during authentications and sessions.

DO YOU AGREE WITH THE FOLLOWING STATEMENT:

> "My organization **analyzes risk prior to granting access and during sessions** to deliver real-time protection."



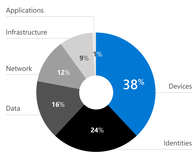
3 SECURING DEVICES AND IDENTITIES ARE THE MOST VITAL PILLARS OF A ZERO TRUST FRAMEWORK

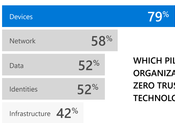
With corporate data being stored and access outside the corporate network, IT leaders prioritizing security at the points of access.

Devices and identities are seen as the two most important pillars of any company's Zero Trust security model.

WHAT'S THE MOST IMPORTANT PILLAR IN YOUR ZERO TRUST SECURITY MODEL?

The most mature aspect of most IT leaders' Zero Trust model is device security (79%)—other pillars are still in progress.





WHICH PILLAR DOES YOUR ORGANIZATION HAVE THE BEST ZERO TRUST CONTROLS AND TECHNOLOGIES FOR?

4 ZERO TRUST IS STILL IN ITS INFANCY FOR MOST ORGANIZATIONS

Only **12%** of IT executives are very confident in their company's current Zero Trust identity management roadmap.

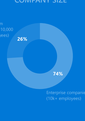
To learn more about how Microsoft Azure Active Directory can help streamline and strengthen your Zero Trust implementation, visit **microsoft.com/security/business/identity**

RESPONDENT BREAKDOWN | DATA COLLECTED FROM APRIL 15-30, 2020

IT EXECS

LOCATION

COMPANY SIZE



Insights powered by PULSE

Microsoft