Zero Trust Implementation Around the Globe

Entrust, along with IDG, conducted a survey among cybersecurity decision-makers in the U.S., Europe, and Asia-Pacific to understand enterprise adoption of Zero Trust frameworks. Respondents included the C-suite, IT executives, and security directors for organizations with 1,000+ employees.

What did they tell us? Here are some highlights.

Zero Trust has become an important cybersecurity issue

Top three cybersecurity priorities

1. Protecting an expanding perimeter
2. Improving user security awareness
3. Adapting to a changing threat landscape

When asked what their organization's top cybersecurity priorities were for the next 12 months, at the top of the list was a big Zero Trust issue: protecting an expanding perimeter (due to cloud adoption, remote work, global workforce, etc.).

But implementing a Zero Trust framework is not quick . . .

Anticipated timeline for implementing a Zero Trust framework

53% Already Implemented
20% Will implement Within 12 Months
27% Will implement in 12+ Months

Just over half (53%) of respondents have already implemented Zero Trust in at least one security area. But for those organizations that haven’t, most anticipate a timeline of more than one year for implementation.

Top four obstacles to implementing a Zero Trust framework

1. Challenging integrations with existing technology
2. Lack of visibility/observability
3. Resistance to change from users and/or customers
4. Managing access for remote/hybrid workers

Nearly half (49%) of enterprises say challenging integrations with existing technology is an obstacle to implementing a Zero Trust framework. Only 4% of respondents said their organizations had no obstacles.

Where does your organization stand?

Where does your organization rank in maturity when evaluated against the Zero Trust framework outlined by the Cybersecurity & Infrastructure Security Agency (CISA)? Answer a few short questions to find out. Take the Zero Trust maturity assessment:

Start Assessment