SPONSORED CONTENT | WHITE PAPER

Inside the **transition to Zero Trust**: What are the challenges and how can they be overcome?

Market Pulse

Savvy security leaders are increasingly turning to the Zero Trust framework to combat cyberattacks – but for many, there are multiple roadblocks and challenges.

In a new era of hybrid work where cyberattacks are on the rise in both sophistication and number, organizations are rethinking the way they address security. Traditional perimeter-based methods are no longer effective. Such methods take a "trust but verify" approach that assumes everything behind the corporate firewall is inherently safe

SPONSORED BY

CIO ENTRUST

Market Pulse

and secure. But this falls short with the acceleration of cloud adoption and digital transformation, as users access resources and data from anywhere at any time.

The Zero Trust approach is driven by the principle of 'never trust, always verify,' to ensure that only authorized users, devices, and entities can access resources on the network or in the cloud. Organizations are able to mitigate the damage a bad actor can accomplish.

Businesses are increasingly adopting Zero Trust frameworks, but they are being hampered by obstacles such as integrations with existing technology, lack of visibility, and resistance to change, according to a survey by Foundry and Entrust.

Successfully implementing Zero Trust will likely require substantial time and resources, and involve a wide array of policies and procedures, as well as technology investments. Once achieved, maintaining a mature and effective Zero Trust framework requires ongoing effort.

No business landscape is the same, and few if any organizations can address the entirety of their environments all at once. But they can identify the most critical data and resources as well as where they have gaps in their defenses, and then build a roadmap to implement a mature Zero Trust framework that addresses high-risk areas first.

How Zero Trust meets top security goals

Today, identity is the first line of defense for businesses. as bad actors access accounts through targeted phishing campaigns, social engineering attacks, and password exploitation – gaining access to data, applications, and infrastructure.

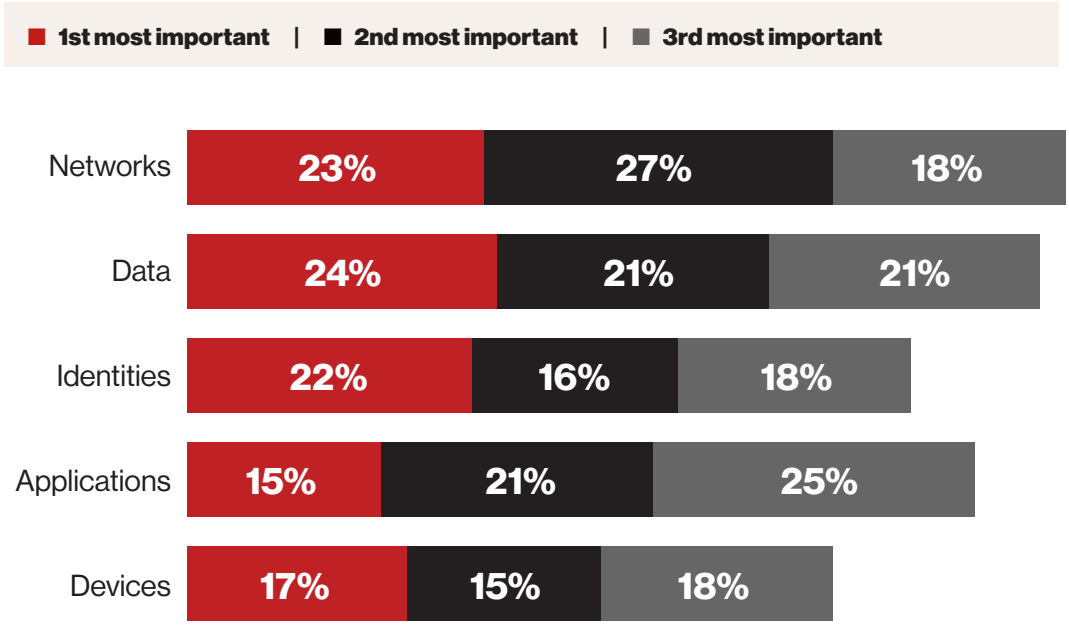
Market Pulse

Many attacks are not 'one off' and instead are intended to harvest data over an extended period by establishing persistence within an organization's networks. The Zero Trust security model requires organizations to continuously verify and authenticate users and devices.

Foundry and Entrust surveyed more than 300 cybersecurity decision-makers in North America, Europe, and Asia-Pacific, on their adoption of Zero Trust strategies. The survey examined obstacles to implementation, current and planned technology investments, and partner selection criteria.

Overall, the trend toward Zero Trust is clear: 53% of the respondents reported having implemented a Zero Trust framework in at least one security risk area. Meanwhile, 10% are building a plan, or updating their current architecture to integrate Zero Trust, and 28% are interested but have not yet started to develop a Zero Trust strategy. North American organiza-

Figure 1 | **First areas of focus when implementing Zero Trust**



SOURCE: FOUNDRY, AN IDG, INC. COMPANY

Market Pulse

tions are somewhat further along, with 74% having at least started the effort, compared to 68% in Europe and 67% in Asia-Pacific.

While the move to embrace this security methodology is clear, implementation timelines vary. A majority (58%) of those who are planning to implement Zero Trust say it will take more than a year to do so in at least one security area. Nearly a fifth (19%) put their timeline at within 6 months, and 23% within 7-12 months.

Implementing Zero Trust architecture is a complex undertaking, requiring organizations to decide what areas to prioritize and when. Data security is the top priority of both large (54%) and midsize (48%) enterprises. Larger organizations are more likely (45%) to prioritize identities than midsize (33%) ones. More midsize (48%) than large companies (40%) prioritize networks.

Larger organizations are also more likely to project a shorter timeline for implementation, with 47% estimating it can be done within 12 months, compared to 40% of midsize organizations.

The research also sought to understand more about the implementations themselves: 44% say they are adopting Devsecops as part of Zero Trust implementations, the most frequently cited action. Other top-ranked activities include conducting security assessments (37%), implementing security training for users (36%), encrypting data (35%), and adopting managed security services (35%).

Overcoming challenges

Zero Trust strategies are inherently complex. Organizations must further their capabilities in many areas:

- **Enable phishing-resistant identities**
- **Defend against remote account takeover attacks**
- **Secure hybrid and remote work**
- **Reduce the attack surface**
- **Deliver strong identity, encryption, and access control**
- **Access a broad and integrated ecosystem**
- **Future-proof Zero Trust investments**

Market Pulse

Not every organization has identical needs, so each must adopt the strategies and frameworks best suited to its unique requirements. Getting started can seem overwhelming.

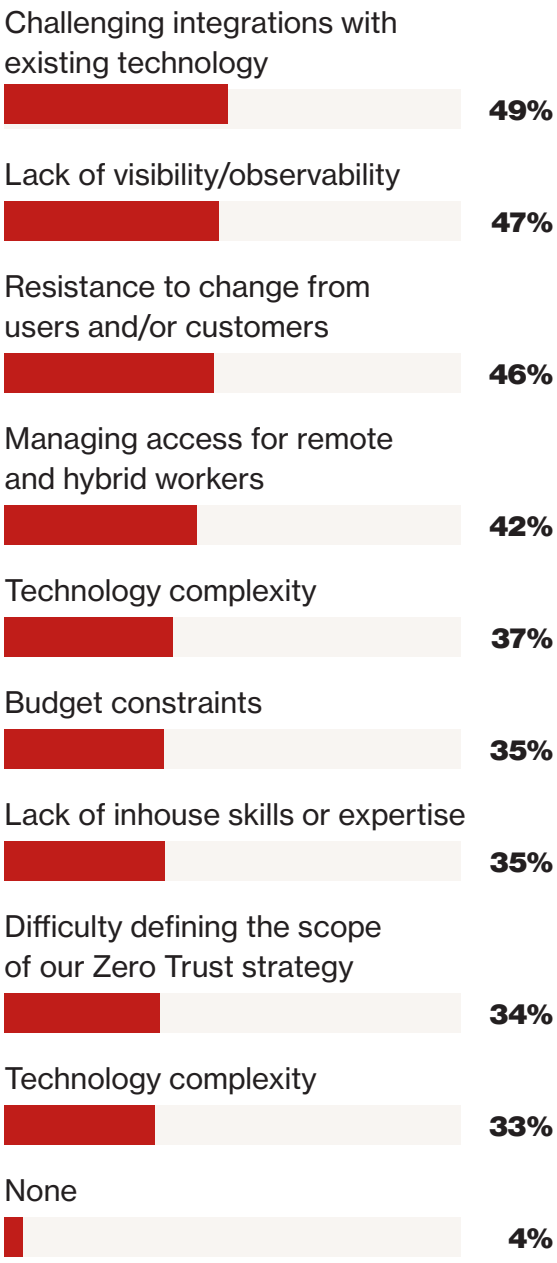
More than half (55%) rate governance and security policy enforcement as extremely or very challenging when implementing Zero Trust. Other acute challenges cited were automation and orchestration of tools and workflows as well as gaining visibility into assets and analytics (both 49%).

Nearly half (49%) cited challenging integrations with existing technology as an obstacle to implementation. Managing access for remote workers was also cited (42%).

Interestingly, resistance to change from both users and customers was frequently cited (46%), showing that Zero Trust is more than a technology project. Balancing the needs of user experience with security while adapting to a new way of working requires a cultural shift.

Meanwhile, flexible working is having different impacts regionally. While 44% in North America say managing

Figure 2 | Obstacles to implementing a Zero Trust framework



SOURCE: FOUNDRY, AN IDG, INC. COMPANY

Market Pulse

access for flexible working is a top obstacle, the figure drops to 27% in Europe. When it comes to technology complexity that dynamic flips: 46% in Europe see it as a challenge compared to just 27% in North America.

With many organizations stretched by limited budgets and persistent cybersecurity staff shortages, managing and monitoring identities for every user, device, and system can appear daunting.

"You can't fix what you can't see or what you can't understand," James LaPalme, vice president of Identity Solutions with Entrust says. "You need to know where you are today, in order to then roadmap how to get where you want to be. Issues arise when there isn't centralized visibility and control."

Organizations must be prepared for the time and effort it takes to integrate new security solutions in their current technology ecosystem. Resource and expertise shortages can slow progress.

Dealing with these challenges requires focus and prioritization. There is no one-size-fits-all solution. Businesses can only implement what their budgets allow for, so it is important to determine where the organization is most vulnerable.

Market Pulse

Embedding Zero Trust throughout the business

Implementing Zero Trust starts with selection of a framework, or model, that enables IT teams to create a roadmap for implementing security controls and policies.

The National Institute of Standards and Technology (NIST), the U.S. Department of Defense, and the Cybersecurity & Infrastructure Security Agency (CISA), as well as the UK's National Cyber Security Council (NCSC) offer frameworks or guidance applicable to Zero Trust.

Most models offer similar core pillars, with slight variations. The CISA model version 2.0[1], updated in 2023, describes how organizations can best apply Zero Trust principles across five pillars:

- **Identity**
- **Devices**
- **Networks**
- **Applications & Workloads**
- **Data**

CISA's model implements the 7 tenets of Zero Trust outlined in NIST guidance:

- **All data sources and computing services are considered resources.**
- **All communication is secured regardless of network location.**
- **Access to individual enterprise resources is granted on a per-session basis.**
- **Access to resources is determined by dynamic policy.**
- **The enterprise monitors and measures the integrity and security posture of all owned and associated assets.**
- **All resource authentication and authorization are dynamic and strictly enforced before access is allowed.**
- **The enterprise collects as much information as possible about the current state of assets, network infrastructure, and communications, and uses it to improve its security posture.**

[1] CISA, CISA releases zero trust maturity model version 2, April 2023, https://www.cisa.gov/news-events/alerts/2023/04/11/cisa-releases-zero-trust-maturity-model-version-2

Market Pulse

"What we've seen in the market is that the one published by CISA is one of the more widely adopted frameworks by both government entities and private enterprises," LaPalme says. "The CISA model has a comprehensive coverage across several risk areas that offers controls and defenses across a large attack surface."

Zero Trust frameworks should be employed across different risk areas that an organization may be exposed to.

Enterprises are dealing with multiple threat vectors because of digital interactions with customers, contractors, and employees. Information is being accessed from a variety of different places. In addition, many organizations today are utilizing a variety of environments, including on-premises applications, software as a service, and varied cloud services.

The diversity of business computing resources and services results in myriad roles and responsibilities across different functional areas that all require different types of permissions. Zero Trust provides the guidance and models to implement a strong comprehensive defense across a perimeter-less enterprise.

Decision-makers surveyed by Foundry and Entrust indicate they are spending 10% of IT budgets, on average, for their Zero Trust requirements. The solutions they are deploying include: anti-virus/malware (85%); endpoint protection (79%); authentication (78%); encryption (77%); data loss prevention (76%); biometrics (74%); and access controls (72%).

When it comes to technology investment, businesses appear to see the merits of different approaches. Nearly two-thirds of respondents prefer best-of-breed solutions when making technology purchases to support Zero Trust.

Market Pulse

Meanwhile, 28% prefer a single vendor offering the most comprehensive solution set across multiple segments and risk areas.

When selecting technology partners to support their Zero Trust journey, 75% say that leading providers for specific products are the most important consideration; close behind, with 74% of respondents, are turnkey solutions that can be easily integrated across applications and enterprise systems; followed by 72% citing solutions that align to their preferred Zero Trust framework. Businesses in the planning stage of their Zero Trust journeys favored a single vendor approach (39%).

When selecting solutions and providers, it's important to consider how easily they integrate with your existing technology stack and align with local and industrywide processes and policies. No one vendor can provide complete coverage but Entrust offers a portfolio of solutions that starts with a strong core identity and extends across the Zero Trust landscape. Entrust integrates with key technology partners to ensure organizations can implement a comprehensive approach that is affordable and easy to configure and manage.

For more insight on implementing your near- and long-term Zero Trust strategy, visit Entrust's website.