Enterprise Strategy Group | Getting to the bigger truth.™

The State of Zero-trust Security Strategies

Zero-trust approaches are arguably more relevant than ever due to the increasingly distributed nature of the modern enterprise, which has only been accelerated by the shift to work-from-home models. Yet for many organizations, confusion remains as to exactly what a zero-trust initiative should entail, where to begin, and how best to overcome the organizational obstacles that result from such a cross-functional undertaking.

Definitions of Zero Trust Vary...

43%
A security strategy which assumes the network is compromised and brokers resource-specific access through a least-privileged approach supported by continuous authentication, authorization, and risk evaluation for every request

30%
Security technologies that granularly segment the network, data centers, and cloud infrastructure to enforce east-west traffic policy in order to limit lateral movement and prevent untrusted entities from gaining broad access to the network

26%
Security technologies that create an identity- and context-based logical access boundary around an application or set of applications, hiding them from public view and restricting access to a set of named entities via a trust broker

...Leading to Divergent Zero-trust Practices

TOP FIVE APPROACHES

55% Identify and inventory all devices on our network

50% Multiple factors of authentication for all users

48% Analytics to identify anomalous behavior

48% Data classification and security controls

45% Conditional access model that weighs multiple factors

Zero-trust Organizations Report Smoother WFH Transitions

Zero-trust organizations reporting a smooth transition to WFH:
63%

vs.

NON Zero-trust organizations reporting a smooth transition to WFH:
43%

Formalized Strategies Are Important But Often Not the Starting Point

88%
of organizations have a formalized, **documented strategy for zero trust** that guides their cybersecurity program

GENESIS OF ZERO-TRUST INITIATIVES.

Users Expect a Broad Range of Capabilities, Paving the Way for a Platform Approach

TOP FIVE ZERO-TRUST ATTRIBUTES.

31% Coverage for cloud/ on-premises

29% Risk assessment capabilities

25% Automation of policy creation/management

25% Integrations with analytics platforms

24% Integrations with identity providers

We are currently using a platform approach to support our zero-trust strategy
37%

We will consider a platform approach to support our zero-trust strategy over the next 12-24 months
28%

Zero-trust Collaboration Issues Do Exist, Leading to Interest in Centers of Excellence

TOP FIVE ORGANIZATIONAL CHALLENGES RELATED TO ZERO TRUST.

32% Communication issues related to collaborative tasks

32% Security teams are slow to incorporate feedback from non-security teams

29% Lack of clarity about areas of responsibility

29% Non-security teams move too quickly without input from security teams

29% Different groups are measured and compensated on conflicting goals

Budget Models Differ but Zero-trust Funding is Typically Net-new

Discrete zero-trust budget within other security program budgets such as network security, identity and access management, or data security
48%

A dedicated zero-trust program budget
35%

76%
report net-new zero-trust funding

The Bigger Truth

At its essence, zero trust was designed with the idea that network location should not be a determining factor for establishing trust. In today's dynamic environment when users, applications, and resources could be in corporate offices, at home, in public clouds, or anywhere in between, zero trust has become not just an intriguing approach, but a required model to secure the modern enterprise.

LEARN MORE

Source: ESG, a division of TechTarget, Inc. Research Report, The State of Zero-trust Strategies, April 2021.