Gartner Research

The CISO's Conversation Guide to Zero Trust

Wayne Hankins, Zachary Smith,
Aaron McQuaid, Nahim Fazal

21 March 2024

Gartner®

The CISO's Conversation Guide to Zero Trust

Published 21 March 2024 - ID G00799106 - 14 min read

By Analyst(s): Wayne Hankins, Zachary Smith, Aaron McQuaid, Nahim Fazal Initiatives:

Cybersecurity Leadership; Build and Optimize Cybersecurity Programs

Cybersecurity leaders face challenges in communicating the benefits of zero-trust architecture to various stakeholders. This document guides them on how to clearly define zero trust's benefits and handle potential objections, ensuring buy-in and support from the organization.

Overview

Key Findings

- Cybersecurity leaders struggle to effectively communicate the benefits of zero-trust architecture to different organizational stakeholders.
- Cybersecurity leaders fail to deliver on zero-trust initiatives due to miscommunications with the team supporting this approach to defending the business.
- Many vendors use zero trust as a generic marketing term, making it much more difficult for cybersecurity leaders to clearly define zero trust's benefits for the organization.

Recommendations

- Communicate the zero-trust plan seamlessly to executive audience members by using nontechnical language and including the business benefits.
- Outline the benefits, technical requirements and guidelines that promote a successful cybersecurity paradigm shift to communicate the zero-trust plan to technical leaders and gain their buy-in.
- Engage architects in zero-trust discussions by outlining the organization's roadmap to connect users to applications securely while shifting to an explicit trust mindset.
- Establish a plan for handling objections by considering potential stakeholder objections and providing clarity to them.

Strategic Planning Assumption

By 2028, 20% of cybersecurity leaders will overinvest in zero-trust initiatives due to marketing hype, miscommunication and unreasonable expectations.

Introduction

As the frequency of cyberattacks and breaches increases and end users can access corporate resources from virtually anywhere, organizations need to enhance traditional perimeter-based defenses with a strong identity-based cybersecurity approach. Zero-trust core principles should be used as a guide as organizations begin this journey.

Zero trust is a security paradigm that replaces implicit trust with continuously assessed explicit risk and trust levels based on identity and context, supported by security infrastructure that adapts to risk-optimize the organization's security posture.

Unfortunately, many organizations are still confused about what zero trust is and what its benefits are. Data from the 2023 Gartner State of Zero-Trust Strategy Adoption Survey shows that more than half of respondents incorrectly believe they are implementing zero trust through security information and event management and endpoint detection and response technology deployments. [1]

We define zero trust as a mindset (or paradigm) that replaces implicit trust in existing IT architecture with explicitly calculated adaptive trust. Although zero trust may enable more secure use of cloud computing via identity-based adaptive controls, it's not a product or a set of products that organizations can purchase. Zero-trust principles can be applied across multiple company systems.

Cybersecurity leaders must ensure buy-in and support from crucial organization stakeholders by clearly explaining the benefits and answering objections for technical and nontechnical audiences.

This guide provides advice on:

- Communicating zero trust's benefits to nontechnical leaders, such as executives
- Communicating and gaining buy-in from technical leaders
- Engaging architects in discussions about zero trust

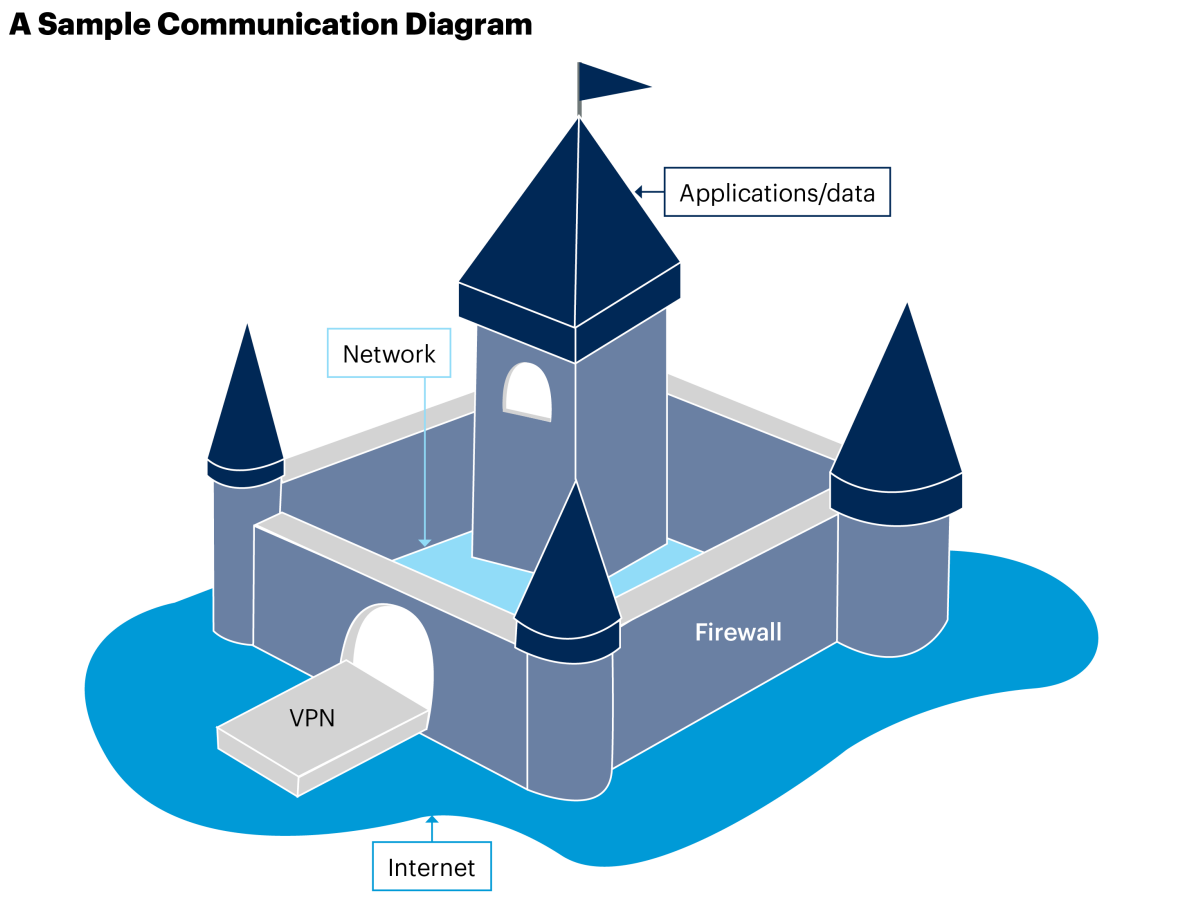
- Handling objections

Analysis

Develop a Zero-Trust Communications Story for Executives

Explaining your zero-trust strategy to nontechnical peers can be challenging. A great way to start the conversation is with an analogy familiar to the audience. For example, you can explain zero-trust principles with castles and moats (see Figure 1). Explain that moats, walls, towers and drawbridges were an in-depth defense strategy to protect the people and resources inside the castle.

Figure 1: A Sample Communication Diagram



Source: Gartner
799106_C

Gartner

Zero trust is a similar approach to how perimeter defenses have been established to protect resources today. We fortify our existing security controls like adding sentries and gating to walls and drawbridges around a castle and guards within the castle to ensure limited access to restricted buildings, areas and rooms. Zero trust allows us to enhance traditional security controls by limiting users to access only their approved applications and data.

If a strategy has not yet been developed, our Tool: Cybersecurity Strategy Template for CISOs can help cybersecurity leaders develop both a cybersecurity strategy and roadmap.

Most organizations had a high level of implied trust once users crossed the corporate firewall. Unfortunately, bad actors have learned how to bypass standard perimeter security. Therefore, additional controls must be deployed to secure valuable corporate resources.

Thus, zero-trust architecture was introduced. Since bad actors continue to find ways around perimeters, organizations must assume the bad actors have gained access to their network. Therefore, they must implement explicit trust for access to their resources. Simply said, never implicitly trust but always verify.

Business Benefits

While telling the story, include zero trust's business benefits as well as how it supports the business's core goals. The organization's zero-trust strategy should include these benefits and cybersecurity leaders should reference them during the discussion. Figure 2 can be used to help frame the business benefits for the executives.

Figure 2: Zero Trust Benefits

Ensure you link the generic benefits (e.g., reduce business impacts of error and attacks) to scenarios relevant to your organization. For example, zero trust can:

- Reduce the business impact of the login credentials of our sales agents being stolen.
- Support the digitization strategy of our client engagement system.

Ignition Guide to Creating Cybersecurity Value Stories provides advice on how to craft cybersecurity value stories that resonate with nontechnical audiences. For supporting templates and resources to help you execute these conversations, see the accompanying slides in Tool: Zero-Trust Conversation Guide for CISOs.

Gain Technical Leader Buy-In on Zero Trust

Confusion regarding zero trust permeates the market, and many vendors claim they can provide it out of the box. However, this is more marketing than reality. Cybersecurity leaders should clarify that zero trust is not a product or a tool that can be simply purchased and installed. Rather, it is a comprehensive security framework (composed of multiple vendor point solutions and nontechnical controls) that requires careful planning and implementation by the technical leaders.

At its highest level, cybersecurity leaders can tell technical leaders that zero trust is enhancing the organization's ability to "security connect users to applications."

In a zero-trust environment:

- Devices and users must be authenticated and authorized.
- Their behavior must be monitored, understood, and explicitly allowed.
- Trust needs to be established and/or verified every time a subject requests access to an object.

Zero trust is a paradigm or a continuum of capabilities that replaces implicit trust access with an access control model based on explicit trust, continuous monitoring, and verification of identity and context. Emerging capabilities that provide the "continuous monitoring and verification component" often take the form of a user-based risk score, which is dynamically updated in real time and used as input for automatic remediation or alerting.

Technical leaders may be tempted to jump straight to implementation. Cybersecurity leaders must temper these impulses and work with enterprise architecture and the PMO to prioritize zero-trust projects based on a formal risk and cost-benefit analysis.

Common Guidelines

Table 1: Common Guidelines for Zero-Trust Architecture

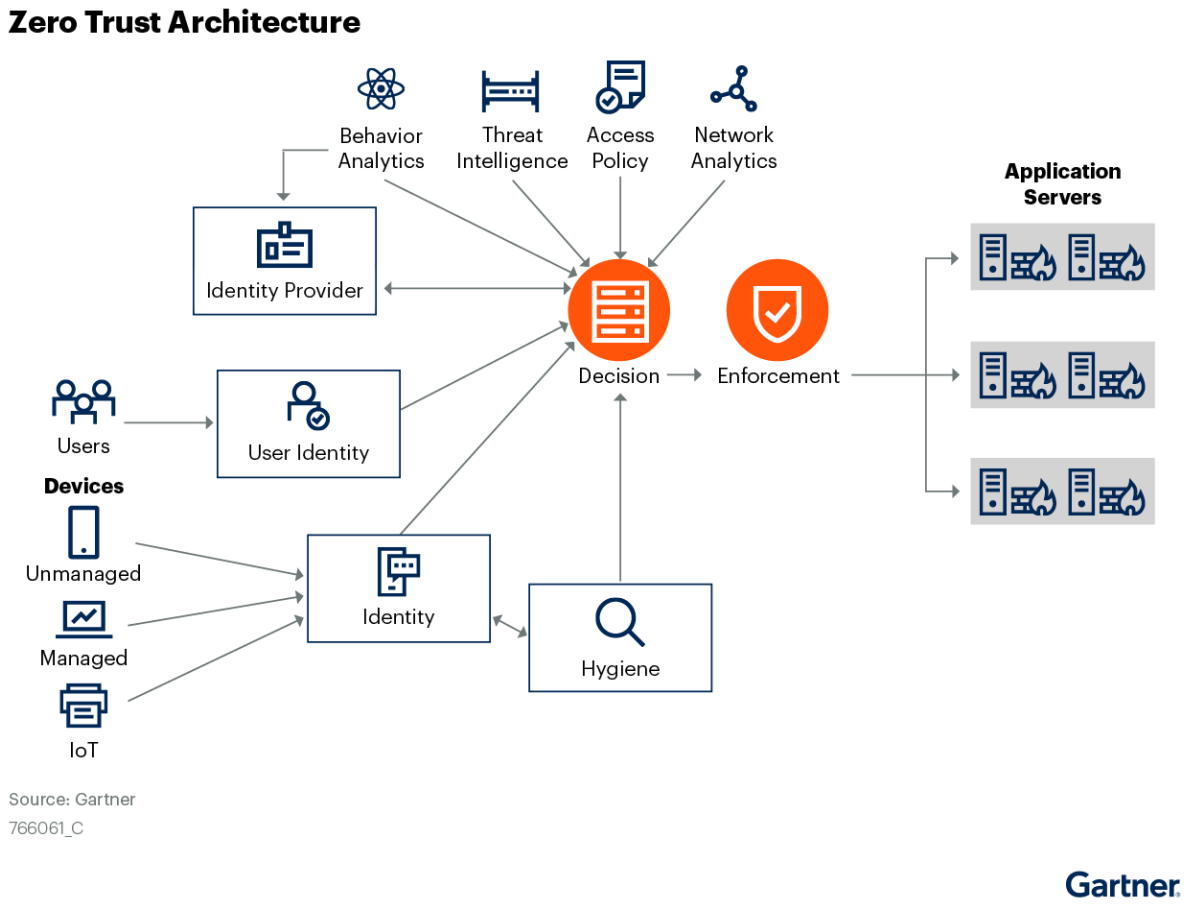
(Enlarged table in Appendix)

Guideline	Steps	Details
Explicit Verification	1. Authenticate and Authorize 2. Single Sign-On (SSO) 3. Least Privilege Access	1. Every device, user, and network flow must be authenticated and explicitly authorized. Two-factor authentication is becoming a core function for critical assets. 2. SSO is also a critical part of any verification strategy as it can help drive adoption among the user community and decrease operational friction. 3. Grant users the minimum amount of access to accomplish the business function.
Efficient Access Control Logic	1. Role-Based Access Control 2. Adopt Continuous Adaptive Trust	1. Assign permissions based on roles or group membership rather than an individual user or host basis. 2. Use user-based risk scoring. If an authenticated user invokes a bad act, their risk score will be increased, and a policy enforcement or logging action may be taken against them based on an elevated risk score.
Assume Breach	1. Threat Hunting 2. Microsegmentation	1. Some attacks dwell in your environment for months or years. Establish a threat-hunting program to look for evidence of these events. 2. During segmentation projects, you often start by mapping the existing application flows. Don't assume all of these flows are authorized or benign. Validate your baseline with application owners and experts.
Segmentation	1. Application Segmentation 2. Network Segmentation	1. Apply segmentation at the application layer to isolate critical application environments. Application criticality is typically enumerated with a risk-based analysis. 2. This is often referred to as macrosegmentation. Divide the network into secure zones and enforce security policy to traffic as it moves between zones.
Monitoring and Validation	1. Continuous Monitoring 2. Behavioral Analytics	1. Monitor user behavior and network activity for indications of compromise. 2. Utilize user and entity behavior analytics to identify anomalies that could be security incidents.
Data Security	1. Encrypt Data 2. Protect Sensitive Data	1. Encrypt data at rest and in transit. 2. Classify data based on its criticality and then limit access to that data based on its classification.
API Security Security Automation	1. API Access Control 2. API Schema Security	1. Control and validate which services and applications can access each API. 2. Verify that APIs have a secure schema that only exposes required functionality.
Security Automation	1. Automated Policy Enforcement 2. Automated Response and Configuration Management	1. Use automation to enforce security policies in a consistent and repeatable manner. 2. Automate response functions to detect incidents faster and enforce minimum security baselines automatically for configuration errors.
Endpoint Identity and Posture	1. Posture Validation 2. Network Access Control	3. Ensure minimum security posture is met before granting access to resources. 4. Ensure an endpoint is valid and authorized for network access before you grant access. Typically a certificate is validated against an identity provider (IdP), such as Microsoft Active Directory or Okta, for this function.
Zero-Trust Security Culture	1. Continuous Improvement 2. Training and Awareness	1. Constantly reevaluate your zero-trust program based on lessons learned and evolving threats. 2. Educate every employee about zero-trust principles via an ongoing security awareness program.

Source: Gartner

Cybersecurity leaders must build a basic understanding of the above guidelines, which will be part of the conversation with technical leaders. The zero-trust architecture graphic in Figure 3 can be used as a reference to identify where these components are located within the model.

Figure 3: Zero Trust Architecture



Engage Architects in Zero-Trust Discussions

Cybersecurity leaders will depend heavily on architects to deliver on the organization zero trust strategy. Therefore, cybersecurity leaders must establish an understanding of what zero trust is and is not. It's extremely important to emphasize zero trust cannot be bought by a single vendor and is more about changing the way we think about cybersecurity.

Many cybersecurity leaders look for a simple way to discuss zero-trust architecture with their architects. For that, we suggest this simple phrase: "Securely connect users to applications." Zero does not literally mean zero in zero-trust architecture. To provide access, explicit trust must be established. More technically accurate terms would be "no blind trust," "zero assumptions" or even "zero implicit trust." So, let's recast the term as zero implicit trust.

As a request for access comes into the zero-trust architecture, the risk to grant that access must be calculated. The risk calculation considers various signals such as device location, the believability of user assertion, device hygiene, threat intelligence, time of day, day of the week and the data sensitivity of the application being requested. Access is granted when the calculated risk is less than the value of extending the access.

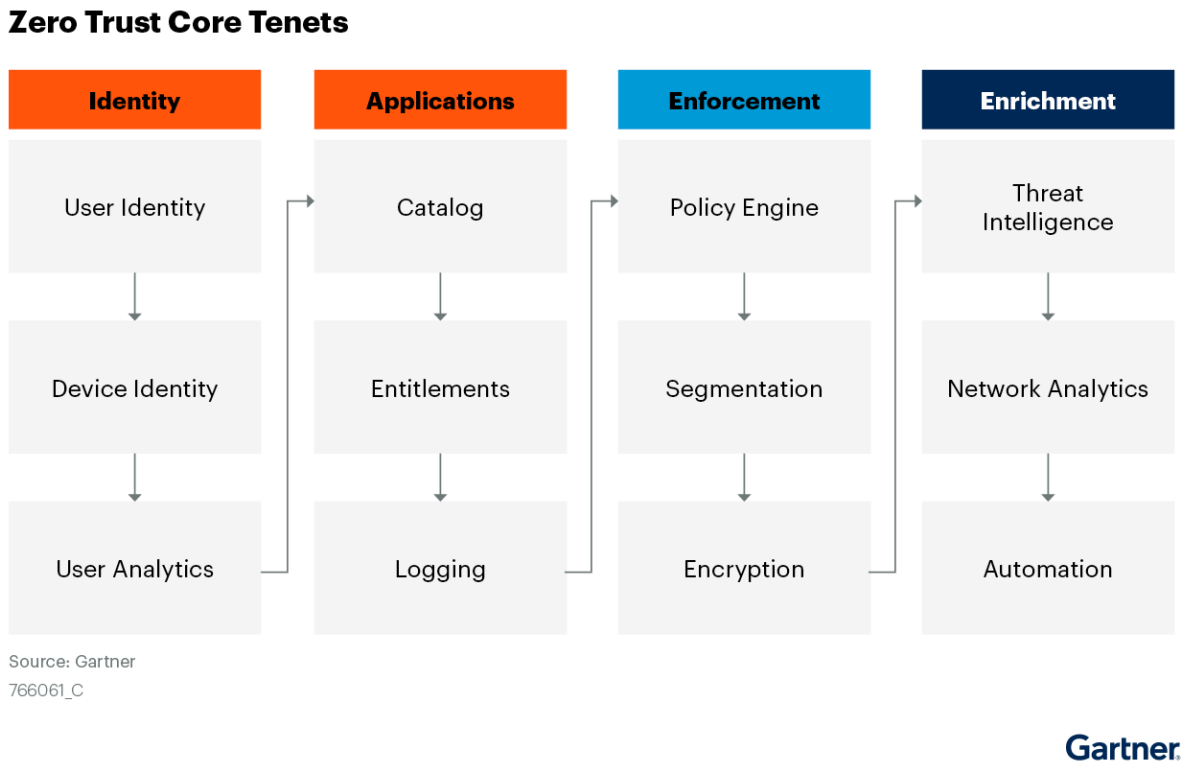
Attribute-based access control with continual assessment is one way to think about zero-trust architecture. Numerous entities, including national governments, industry trade groups and commercial entities, have set forth their requirements for what constitutes a zero-trust architecture. One example is the Cybersecurity and Infrastructure Security Agency (CISA), part of the U.S. federal government. According to CISA, the pillars for zero trust are:

- Identity
- Device
- Network/environment
- Applications and Workloads
- Data

We find this overly complex for many organizations. Focusing on the business, application and technical architecture of an organization enables you to mitigate risk more effectively while minimizing the complexity of deployment. With this in mind, we recommend architecting zero trust using the following four pillars (see Figure 4):

- Identity of users and devices
- Application governance and logging
- Enforcement via technical controls and encryption
- Enrichment with monitoring and automation

Figure 4: Core Tenets of Zero Trust



Establish a Plan for Handling Objections

Handling Objections With Executives

As with any conversation with nontechnical executives, cybersecurity leaders should be prepared to handle objections. Here is an example of a nontechnical leader's objection that often comes up.

Objection: Zero Trust Will Increase the Security Budget

Explain how your organization is already practicing some of the zero-trust architecture principles and how this investment currently supports the business. According to the 2023 Gartner State of Zero-Trust Strategy Adoption Survey, nearly half of the organizations investing in zero-trust do so via a mix of existing products and new products. Almost one-third invest in zero trust solely by exploiting the features and capabilities of existing products. As organizations push to achieve their digital transformation goals, they should include zero-trust principles earlier in the decision processes to help minimize the cost later in the project's life cycle.

Before meeting with nontechnical leaders, conduct a gap analysis against current capabilities as well as where the business needs to be to protect itself better. Our research, How to Decipher Zero Trust for Your Business, addresses additional areas of concern that may come up when meeting with executives.

Handling Objections With Technical Leaders

Technical leaders may have the following objections:

Objection: Why Do We Need to Allocate More FTEs to Support Another Security Projects?

Explain that zero-trust architecture is not a specific product but a paradigm that will take multiple years to achieve. Therefore, zero trust should be considered when increasing the organization's digital transformation and levering the FTEs supporting this effort.

Objection: Where Do I Start With Such a Complex Undertaking, and How Do I Ensure Zero-Trust Policy Is Scalable and Manageable?

Communicate to technical leaders that culture leads to adoption, and they need to have realistic expectations of the zero-trust policy. Advise them to set a cultural outlook where perfect is not the enemy of good. Specifically, they should encourage a culture where policy creation is group-based instead of host-to-host based. Group-based policies will scale better than host-to-host-based policies. You can have an exception for host-to-host policies based on risk assessment for the underlying application.

Some stakeholders may believe that maximum granularity must be used in every area of the network to achieve true zero trust. Cybersecurity Leaders must address these concerns and advocate for a more moderate stance so human and technical resources can handle millions of individual policy entries. Since the grouping of identities inside your IdP is critical for most zero-trust controls, you must ensure the current IdP membership is accurate and reflects the reality of the organization today.

Handling Objections With Architects

Objection: We Do Not Have an Asset Inventory, or We Have Too Many Applications to Use Zero Trust

An initial discovery of people, applications and devices will be part of the journey. Figure 4 provides the simplest flow to reduce friction. With respect to the question of too many applications, business-critical applications can be prioritized, which will help to steer architects on what to focus on. This too will help with ensuring that priority is given to identifying those users who are accessing these critical applications.

Objection: We Do Not Have the Technical Resources to Implement This.

As discussed, adopting zero-trust policies will be a journey and require some level of upskilling if the business requires a level of protection currently not being utilized. By focusing on business-critical applications and systems, organizations can reduce the requirement to leverage a significant amount of technical resources. The zero-trust project will leverage existing security toolsets that have already been deployed, alleviating the need to acquire new technical resources.

Objection: Are We Not Doing This Anyway? Is Zero Trust a Different Name for Defense in Depth?

A certain amount of crossover between defense in-depth and a zero-trust architecture exists. Zero trust is far more encompassing; it addresses security across a range of different domains including user, device, workload, data and network. The key difference is that previously with the defense-in-depth approach, there was not as much focus on identity and very little attention was given to concepts like secure by design. Zero trust is far more comprehensive; it provides mitigation at each point of an adversary's attack path, thereby allowing for the fact that the adversary may bypass a single control point.

Evidence

[1] **2023 Gartner State of Zero Trust Strategy Adoption Survey.** This survey was conducted to understand the current state of zero-trust strategy adoption across the industry and to reduce confusion about the scope and maturity of zero-trust strategies across industries and verticals worldwide. The survey was conducted online from 23 October through 24 November 2023 among 303 respondents from North America (n = 134 in the U.S. and Canada), EMEA (n = 98 in France, Germany and the U.K.) and Asia/Pacific (n = 71 in Australia, India, the Philippines and Singapore). Respondents' organizations had $500 million or more in 2022 enterprisewide annual revenue, and 2,500 or more employees. Respondents were qualified if their organization had already implemented (fully or partially) or was planning to implement a zero-trust strategy. Respondents were also required to have visibility into the strategies or investment decisions related to the zero-trust strategy. Disclaimer: Results of this survey do not represent global findings or the market as a whole, but reflect the sentiments of the respondents and companies surveyed.

This research is based on existing Gartner best practices on implementing a zero-trust strategy, which in itself is based on extensive interactions with Gartner clients and technology vendors.

Contributors

Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

Video: Why Zero Trust Can Help, and How to Get Started

Quick Answer: Explaining Zero Trust Security Approaches to Tech Executives

Quick Answer: What Is a Cybersecurity Outcome-Driven Metric?

Effective Metrics Practices for Cybersecurity Leaders

7 Effective Steps for Implementing Zero Trust Network Access

How to Build a Zero Trust Architecture

Table 1: Common Guidelines for Zero-Trust Architecture

Guideline	Steps	Details
Explicit Verification	1. Authenticate and Authorize 2. Single Sign-On (SSO) 3. Least Privilege Access	1. Every device, user, and network flow must be authenticated and explicitly authorized. Two-factor authentication is becoming a core function for critical assets. 2. SSO is also a critical part of any verification strategy as it can help drive adoption among the user community and decrease operational friction. 3. Grant users the minimum amount of access to accomplish the business function.
Efficient Access Control Logic	1. Role-Based Access Control 2. Adopt Continuous Adaptive Trust	1. Assign permissions based on roles or group membership rather than an individual user or host basis. 2. Use user-based risk scoring. If an authenticated user invokes a bad act, their risk score will be increased, and a policy enforcement or logging action may be taken against them based on an elevated risk score.
Assume Breach	1. Threat Hunting 2. Microsegmentation	1. Some attacks dwell in your environment for months or years. Establish a threat-hunting program to look for evidence of these events.

		2. During segmentation projects, you often start by mapping the existing application flows. Don't assume all of these flows are authorized or benign. Validate your baseline with application owners and experts.
Segmentation	1. Application Segmentation 2. Network Segmentation	1. Apply segmentation at the application layer to isolate critical application environments. Application criticality is typically enumerated with a risk-based analysis. 2. This is often referred to as macrosegmentation. Divide the network into secure zones and enforce security policy to traffic as it moves between zones.
Monitoring and Validation	1. Continuous Monitoring 2. Behavioral Analytics	1. Monitor user behavior and network activity for indications of compromise. 2. Utilize user and entity behavior analytics to identify anomalies that could be security incidents.
Data Security	1. Encrypt Data 2. Protect Sensitive Data	1. Encrypt data at rest and in transit. 2. Classify data based on its criticality and then limit access to that data based on its classification.
API Security **Security Automation**	1. API Access Control 2. API Schema Security	1. Control and validate which services and applications can access each API. 2. Verify that APIs have a secure schema that only exposes required functionality.

Security Automation	1. Automated Policy Enforcement 2. Automated Response and Configuration Management	1. Use automation to enforce security policies in a consistent and repeatable manner. 2. Automate response functions to detect incidents faster and enforce minimum security baselines automatically for configuration errors.
Endpoint Identity and Posture	1. Posture Validation 2. Network Access Control	3. Ensure minimum security posture is met before granting access to resources. 4. Ensure an endpoint is valid and authorized for network access before you grant access. Typically a certificate is validated against an identity provider (IdP), such as Microsoft Active Directory or Okta, for this function.
Zero-Trust Security Culture	1. Continuous Improvement 2. Training and Awareness	1. Constantly reevaluate your zero-trust program based on lessons learned and evolving threats. 2. Educate every employee about zero-trust principles via an ongoing security awareness program.

Source: Gartner

Actionable, objective insight

Position your organization for success. Explore these additional complimentary resources and tools for cybersecurity leaders:

Research

Cybersecurity Threats: How to Prioritize, Manage and Reduce Them

Explore the best practices to break down silos between risk teams and the business.

Download Now

Report

Cybersecurity Trends: Optimize for Resilience and Performance

Use this report to equip your cybersecurity function for greater resilience.

Download Now

Toolkit

Implementing Zero Trust Security in the Public Sector

Accelerate your move toward a modern zero trust security approach.

Learn More

Conference

Gartner Security & Risk Management Summit

Join your peers for the unveiling of the latest insights at Gartner conferences.

Reserve Your Spot

Already a client?
Get access to even more resources in your client portal. Log In

Connect With Us

Get actionable, objective insight that drives smarter decisions and stronger performance on your mission-critical priorities. Contact us to become a client:

U.S.: 1 866 263 8917

International: +44 (0) 03301 628 476

Become a Client

Learn more about Gartner for Cybersecurity Leaders
gartner.com/en/cybersecurity

Stay connected to the latest insight

Gartner®