IDC PlanScape

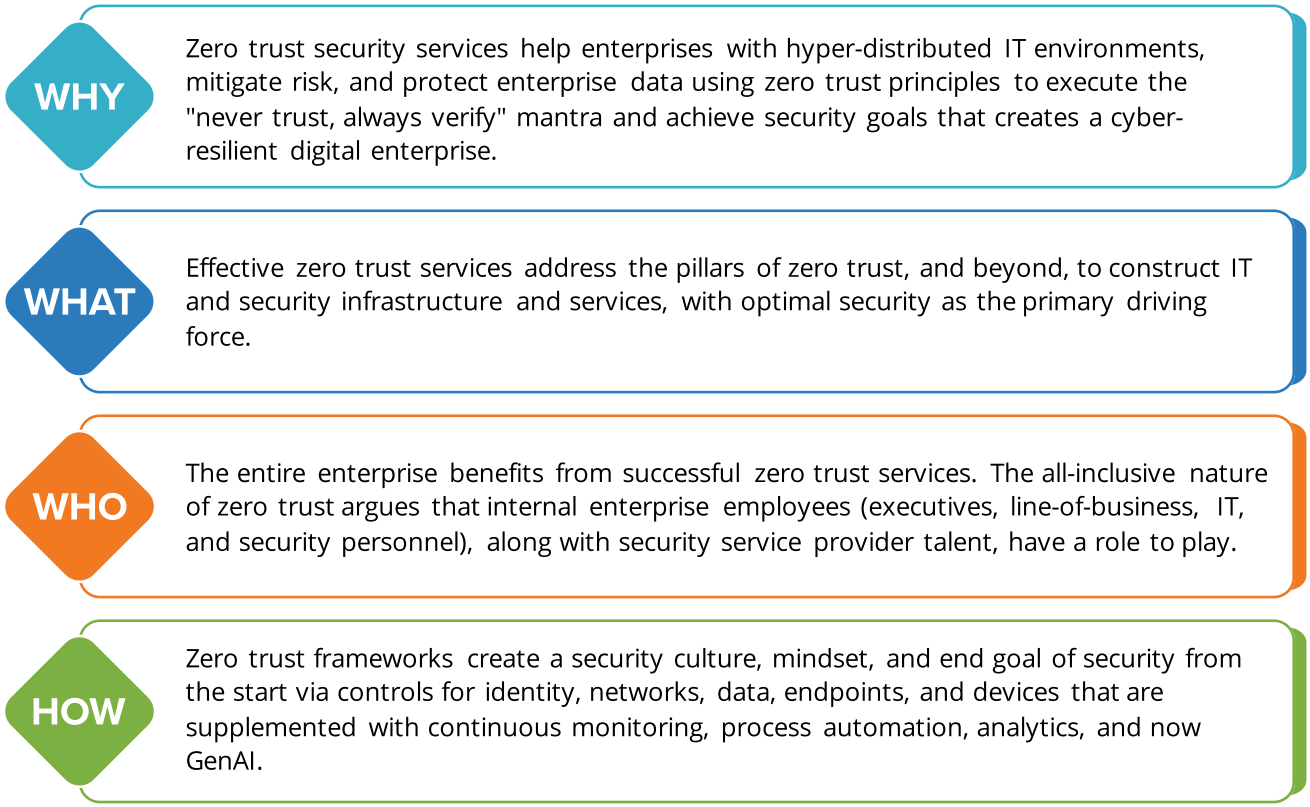
IDC PlanScape: Zero Trust Security Services

Scott Tiazkun

IDC PLANSCAPE FIGURE

FIGURE 1

IDC PlanScape: Executive Summary of Zero Trust Security Services



Source: IDC, 2024

December 2024, IDC #US52742324

EXECUTIVE SUMMARY

Zero trust: a strategy, a concept, a paradigm, an environment? If you will, it may be easier to grasp zero trust as one of these nouns in the context of preventative medicine for the IT environment. Albeit the idea of zero trust as a concept or paradigm does not sit well with those looking to address practical cybersecurity issues because the concept sounds more aspirational and not tangible. However, zero trust can be a tangible pursuit, and security services can greatly help achieve zero trust for an organization.

Zero trust translates to continuous verification and assumption of the constant presence of hostile actors hoping to breach the enterprise in any number of ways. For that reason, zero trust and, by extension, zero trust services are never ending. As onerous as that sounds, having zero trust services in place removes much of the burden from the enterprise and alleviates the workload from IT and security teams via services that achieve a workable zero trust framework.

A workable zero trust framework and architecture addresses the problem of disparate technology silos and creates a security goal that all IT and security teams can work toward. Accordingly, this requires all parties to act as a team (e.g., CTO, CISO, CIO, security teams, IT teams) because this will require not only buy-in from all these parties but many resources to execute any zero trust project. This is where security services, both managed and professional, can play a key part in this pursuit, supporting the enterprise, and ensure that enterprise devices, data, applications, networks, and identities have the correct security posture that supports the zero trust project.

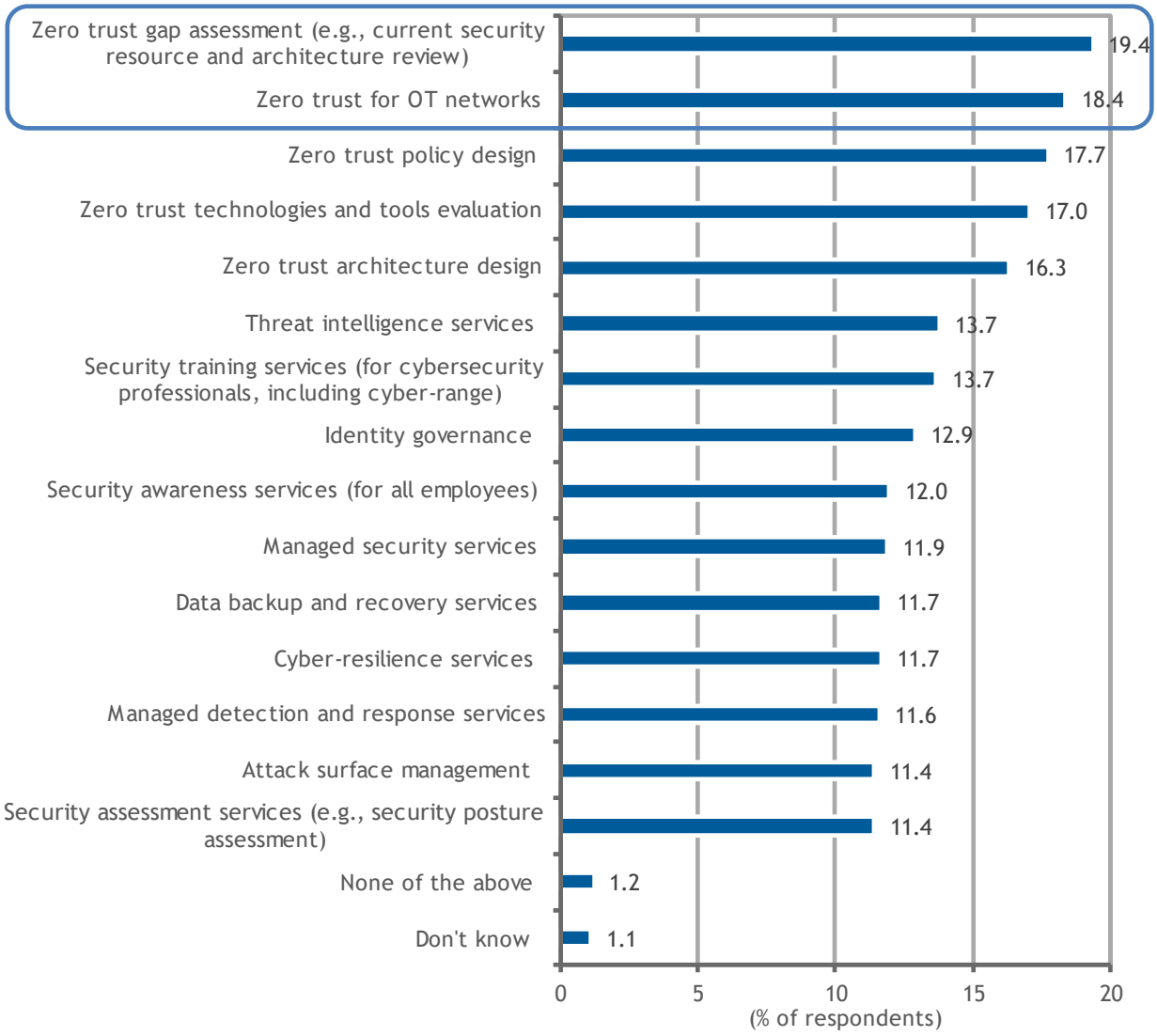
Enterprises do realize that a zero trust project will encompass many security areas. An IDC survey was conducted to determine what security services enterprises would need in 2024 for zero trust efforts. The results spotlight the disparate resources that enterprises will apply as part of their zero trust efforts.

Even with zero trust gap assessments and zero trust for OT networks leading the way in importance, other areas like policy design, architecture design, and threat intelligence are also seen as being important (see Figure 2). At the very least, this shows that enterprises know that a successful zero trust project requires many resources — professional services, managed services, solutions, assessments, and dedicated and part-time personnel — to implement zero trust. This is where security services can do the heavy lifting on a zero trust project.

FIGURE 2

Security Services Currently Used with Regard to Zero Trust Initiative

Q. Which of the following security services are currently used at your organization, and which do you expect will be used in the next 12 months with regard to your zero trust initiative?



n = 1,062

Base = respondents that indicated organizations researching/engaging/solution piloting/implementing zero trust initiative

Source: *IDC's Worldwide Security Services Primary Research 2022–2023 Survey,* February 2023

This IDC PlanScape focuses specifically on zero trust services. It discusses the why, the what, and the how of assessing and instituting managed and professional zero trust supporting services for the enterprise.

"The value and expertise that a service provider can bring to define and enact a zero trust framework cannot be overstated," said Scott Tiazkun, research manager, Worldwide Security Services at IDC. "Service providers are equipped to work with clients to determine where they are in a zero trust journey and position this type of project as part of a larger cyber-resilience effort that benefits the entire enterprise."

WHY ARE ZERO TRUST SECURITY SERVICES IMPORTANT?

Zero trust services can be seen as service providers' attempts to address the complexity of today's enterprises. If you look at security for today's enterprise, you can roughly divide it into three elements: systems (e.g., workplace applications, access control systems, enterprise applications, IoT devices), the enterprise network, and people/devices (e.g., employees, customers, vendors, third parties, corporate devices, personal devices). In this scenario, historically, the network was the security perimeter, with devices, workers, and systems all behind the network. Today's enterprise is more expansive and blurred with cloud-based applications, people dispersed, and devices outside the traditional enterprise network security perimeter. This has allowed for flexibility in access and extended reach for stakeholders but has increased security, risk, and governance issues for all companies. If you don't have a zero trust framework and associated services and solutions, you are at greater risk for security breaches.

Utilizing zero trust services can address problems and challenges that directly impact cybersecurity. These problems can include:

- Lack of clarity on zero trust processes, being unsure of where and how to commence a zero trust engagement
- Internal limitations or lack of understanding of existing security posture and road map
- Inadequate knowledge of security gaps in the operational, management, and technical controls
- Unwieldy number of applications, external and internal users, and identities
- Lack of a future state of security for the enterprise (e.g., heterogenous environments, multiple identities, cloud applications, and workloads)

The security service provider for zero trust will address these issues and assess and construct security and IT infrastructure using the tenets of zero trust guidelines (e.g., NIST 800-207, Cybersecurity and Infrastructure Security Agency (CISA) Zero Trust Maturity Model v2.0, DoD Zero Trust Reference Architecture Version 2.0) as well as adding their own services that can cut across the basic five pillars of zero trust. The objective is a comprehensive and self-correcting security and IT architecture to reduce redundancy, continuously monitor security areas, and automate routing tasks.

WHAT ARE ZERO TRUST SECURITY SERVICES?

Zero trust services are all professional and consulting services that will assess and design a zero trust framework and the managed services to execute on a zero trust framework. A zero trust framework will follow widely accepted guidelines (e.g., NIST, CISA, DoD) and, in many cases, a combination of these guidelines that service providers adhere to for their clients.

A zero trust project will provide value in several ways including enhanced cybersecurity capabilities to support future needs, minimize risk, support key security controls, enhance user experience, and reduce operations costs.

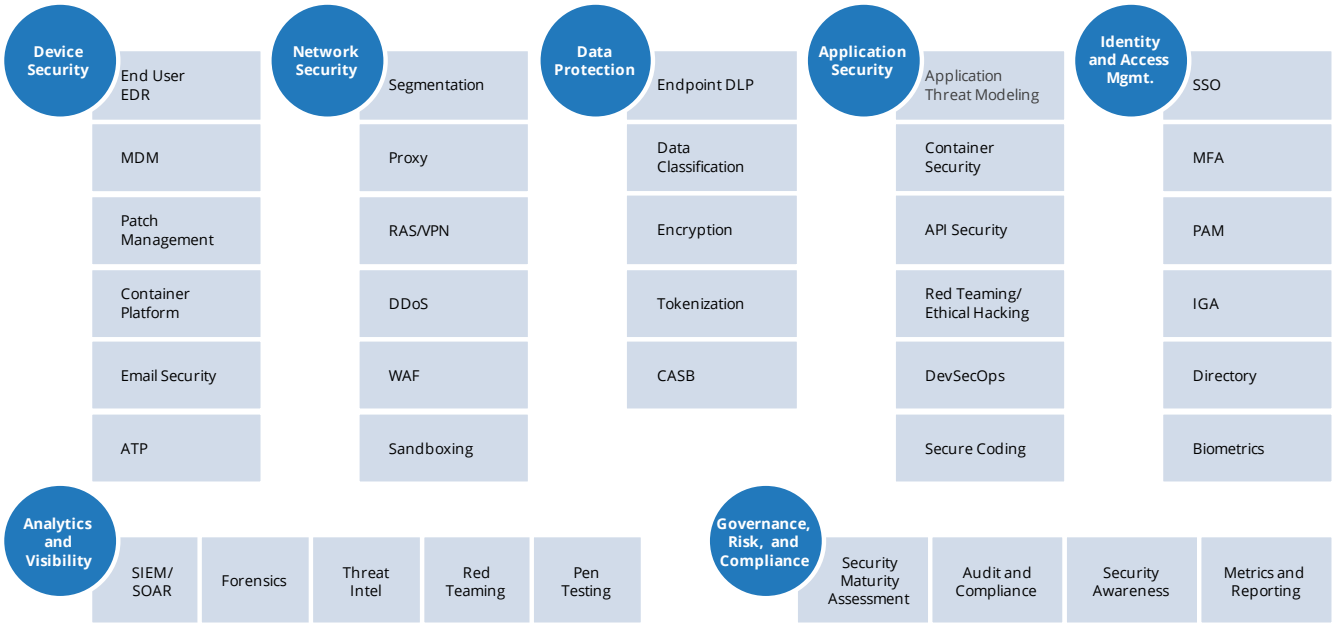
Holistically, a service provider will help clients:

- Create a zero trust definition statement for the enterprise.
- Assess and build a zero trust foundation framework based on enterprise needs and goals.
- Perform an assessment and determine the current state maturity score based on NIST CSF 2.0, CISA's Zero Trust Maturity Model, and zero trust architecture maturity models.
- Make recommendations across all zero trust pillars (device, identity, data, applications, and networks) specific for a customer.
- Align the assessment and future road map for solutions and services needed for the ongoing zero trust journey.

Today, continuous monitoring and analytics have become an important element of zero trust services. This is because monitoring and analytics are essential for identifying and responding to security incidents in a zero trust environment. These tools and services for monitoring and tracking activity across networks will detect signs of suspicious behavior. Analytics are used to identify patterns in network traffic as well as user behavior, which can also help identify potential threats before they become a security incident. Figure 3 provides an illustration of the enterprise security pillars for zero trust projects.

FIGURE 3

Enterprise Security Pillars for Zero Trust Projects



Source: IDC, 2024

While the elements in Figure 3 are not exhaustive, they are illustrative of the processes and services that must be addressed to meet the requirements of zero trust, pillar by pillar. A service provider will assess a zero trust client line item by line item and determine if a service or solution is in place to address the line item or if a road map needs to be created to address missing capabilities. As part of the zero trust project, consulting and assessment create coordination across all five pillars and cross-cutting capabilities (e.g., analytics and visibility, governance) to devise a road map that is priority tiered and reaches the zero trust goals. Also included in this process is tool and process rationalization.

Practically, what should clients expect from a zero trust service provider? Pretty much everything. Many service providers define multiple line items for each zero trust pillar.

Some initial services and elements cut across all five pillars (identity, devices, networks, data, and applications and workloads) of zero trust:

- Define the zero trust vision for the enterprise
- Establish a zero trust program management office (PMO)
- Perform a zero trust maturity assessment
- Promote a zero trust organizational culture at the enterprise

- Map and classify applications, assets, and traffic flows
- Design a zero trust policy and specific architecture for an enterprise

Things start to get more specific from that point on:

- For identity, service providers will:
  - Implement identity governance processes
  - Implement least privilege models/limit access
  - Consolidate identities (e.g., single sign-on [SSO])
  - Adopt multifactor authentication (MFA)
  - Implement a privileged access management (PAM) solution
  - Provide services to detect and remediate abnormal identity behaviors
- For networks, service providers will offer:
  - Macro-segmentation services
  - Implementation of SASE and NDR
  - Micro-segmentation
- For devices, service providers will offer:
  - Adoption of endpoint detection and response
  - Protection of mobile devices
  - Management of vulnerabilities based on risks
  - Secure access for “bring your own device” (BYOD)
  - Enforcement of device continuous compliance
  - Advanced automatic remediation
- For data, service providers will offer:
  - Data discovery and classification
  - Data tagging
  - Encryption key management
  - Tokenization and masking
  - Data backup
  - Implementation of data loss prevention (DLP)
  - Data security life-cycle management
- For applications and workloads, service providers will:
  - Shift security left (DevSecOps)
  - Enable app SSO and MFA
  - Provide end-to-end encryption

- Set up application logging
- Secure and monitor legacy applications
- Protect APIs (application programming interfaces)
- Adopt CASB (cloud access security broker)
- Adopt WAF (web applications firewall)

It is this step-by-step approach by service providers that addresses the pillars and stages of a zero trust journey to help enterprise reach an optimal security state that can best be defined as having:

- Fully automated self-reporting
- Dynamic least privilege access
- Cross-pillar interoperability with continuous monitoring
- Centralized visibility

AI, GenAI, and Zero Trust

AI and GenAI have and will continue to have a place as important tools for zero trust. Service providers are already offering AI-powered security operations solutions, and GenAI tools are coming.

Some service providers are offering integrated network and security tools along with analysis of data, leveraging machine learning and AI, to detect security issues. This not only enables issue remediation but also addresses business priorities like smart reporting with interactive consoles that report IT environment details and recommendations. GenAI will take this a step further with autohealing that allows automated remediation of issues coupled with risks evaluations, policy rectifications and configuration, and endpoint compliance. GenAI will also help sustain smart operations leveraging automation platforms, root cause analysis, configurations compliance, and continuous reporting of issues and their prioritization.

These AI- and GenAI-enabled tools are having an increasingly positive role alleviating the issues around the complexity of security that is impacting cybersecurity operations overall as well as achieving a zero trust framework. Users should expect benefits like streamlined visibility and insights into security tools. In addition, expect a better user experience because of interactions using GenAI-based chatbots that will update users with a view of their security posture, operations risk, compliance, and recommendations rather than having to search reports. Users of GenAI tools and services should also expect increased operational efficiency by proactively identifying issues, analyzing trends to identify patterns that could impact their zero trust framework, and performing root cause issues analysis.

WHO ARE THE KEY STAKEHOLDERS?

Because zero trust impacts how a company does business and can be positioned as a cyber-resilience effort, stakeholders and advocates come from all parts of the enterprise. Personnel from IT, security, global managed services, and DevOps are very involved during the assessment portion of a zero trust effort. Measured security metrics are also reported up to the C-suite, legal departments, compliance officers, and risk managers that have a dependency on governance and risk reporting that can impact their roles as well as enterprise needs like cyberinsurance, again pointing to the importance of a zero trust project.

In many cases, IDC found that the CISO role, acknowledging the impact that this type of project has, initiated the zero trust efforts and was instrumental in working closely with the service provider along the assessment, strategy, and planning phase of the zero trust project.

HOW CAN MY ORGANIZATION TAKE ADVANTAGE OF ZERO TRUST SECURITY SERVICES?

Once an enterprise decides that zero trust is an important cyberinitiative, it has to execute on a plan of action. Most importantly, if an enterprise knows that it does not have the resources needed nor the IT and security maturity to tackle the elements of zero trust, a service provider is the most obvious and knowledgeable partner to work with to marshal the resources needed.

Enterprises will need to talk to several service providers to determine their level of knowledge and experience addressing zero trust services. IDC talked to several service providers that offer zero trust services and has delineated how they address professional and managed services for their zero trust clients.

Avanade

Avanade is heavily focused on the Microsoft platform. Accordingly, it has had success as two-time winner of the Microsoft Zero Trust Champion award. The company also specializes in long-term zero trust projects. One example of this was helping a global consumer brand implement a zero trust environment while preparing for divesture from its parent company. This project centered around Microsoft 365 Security and Azure Security environments, and Avanade helped secure the new entities' infrastructure and assets.

While Avanade focuses on the basics (identity, devices, networks, applications, and data), it includes as part of its zero trust framework additional service layers and

controls for governance, analytics, and automation. Governance services include defining clear access policies and standards applicable to all personas in the enterprise. Avanade also has services to leverage automation processes to grant and approve access to IT services, data, and collaboration. Avanade also employs analytics to continuously assess zero trust posture and analyst behavioral attributes such as user, device, and network flows to measure deviations from zero trust baseline metrics. Avanade distinguishes itself by offering clients a zero trust program management dashboard that acts as a single point of information for the entire zero trust program, and the dashboard also charts progress of the project. Users can delve into specific data points for applications, locations, or products to track and assign a maturity-level grade associated with zero trust goals. This dashboard is updated by Avanade team members associated with the project and is informed by Power BI metrics from Avanade.

Avanade initiates zero trust projects by looking at and defining general security principles that a client needs. This is then rationalized against an assessment on where the client currently is on their zero trust journey. Avanade works with key stakeholders to develop a zero trust plan, determines what has worked well in the past, and conducts discovery workshops for future needs. From there, Avanade creates services road maps and heat maps to determine priorities and initial efforts first needed. Some clients are more security product focused to address the pillars of zero trust, while some clients prioritize compliance around regulatory issues. Avanade works with the clients that have these differences in priorities while addressing the basics of zero trust. Solutions that Avanade will bring to clients include identity and access management, device hardening, data loss prevention, and reporting for audits and Information Commissioner's Office (ICO).

Avanade claims over 1,700 security professionals globally in 26 countries and over 1,000 security clients globally.

Infosys

The zero trust service offering by Infosys for its clients is based on a foundation architecture framework in which Infosys assembles services and tools to institute policies, controls, and operations for the pillars of the zero trust framework (e.g., data, devices, network, identity/users, and applications and workloads). A typical Infosys zero trust engagement includes conducting workshops to understand customer's current policies and technology and security landscape, followed by creation of a custom zero trust definition and framework, addressing not only the zero trust pillars as previously mentioned but also the "horizontal" elements like analytics, visibility, automation, orchestrations, and governance.

Infosys also performs a zero trust maturity assessment based on NIST CSF, ZTA (Zero Trust Architecture) Maturity Models, and additional functions across zero trust pillars specifically designed for its customers. This assessment includes review of the enterprise security stack from both an architecture and tools perspective that designates if various elements (e.g., end-user EDR, segmentations, encryption, container security, conditional access, privilege access management) currently exist at acceptable levels, partially exist or are not properly implemented, or do not exist in the enterprise. Infosys' core guiding principles for zero trust include "cloud first," least privilege, and API first, with emphasis on ROI from existing toolsets.

For its clients, Infosys promises to align zero trust assessments with recommendations and future road map needs to reach an optimal zero trust maturity level. It draws on global best practices to jump-start a zero trust journey and aligns the client's current and in-pipeline projects with the determined zero trust model. Thus the zero trust journey and implementation road map is curated based on the current state of its customers' security posture and target desired state.

A typical zero trust initial assessment consists of two weeks of planning; eight weeks of assessment, analysis, and project definition that include requirement gathering and gap analysis and recommendations; and two weeks to deliver a final assessment report.

An example of an assessment, for the network pillar of zero trust, would include Infosys identifying elevated risk situations such as legacy VPN–based access, limited segmentation, multiple firewall types, or inconsistent rules management. Infosys would recommend actions like consolidating employee access or a move to a ZTNA (zero trust network access) for employees and third parties for internet-based as well as for in-house applications. It may also accelerate data protection and risk identification to secure sensitive data across channels. The goal as defined by Infosys would be to gain actionable insight and accelerate measurable risk reduction in the network pillar of zero trust.

The execution is often run in a hybrid model with a combination of greenfield zero trust capabilities (introducing new ones, if required, to accelerate zero trust journey) and brownfield implementation, where customers are already having partially deployed solutions, but capabilities can be extended and improved further based on zero trust principles. Prioritization of these zero trust initiatives is determined based on factors such as quick ROI, risk reduction in iterative manner starting with high-risk assets and/or applications, business priorities, increased compliance, and visibility. Infosys will address the multiple pillars of zero trust for clients in this methodical fashion and emphasize the gained intelligence each pillar can generate for its clients as part of the zero trust project.

Infosys claims 13,768 dedicated security professionals based in 15 countries worldwide and 526 security clients globally.

Kyndryl

Kyndryl embeds zero trust projects front and center as part of its security services for IT modernization for clients. These services include security assurance, security operations and response, cyberincident recovery, and zero trust. This larger portfolio includes 96 offerings of which 60 are advisory and consulting and 36 are managed services as of November 2024.

Specifically, the Kyndryl Zero Trust Adoption Framework, positioned as part of Kyndryl Security & Resiliency Services, was launched in 2021 and includes a wide range of services addressing zero trust principles that are built on Kyndryl's 60+ alliances with solutions and service providers. With this range of partners that are both market leaders and niche players, Kyndryl has a vendor-agnostic approach to zero trust. Kyndryl says that many initial assessments of clients that are pursuing a zero trust strategy suffer from fragmented security architectures, the absence of a unified architecture, and services compounded with tool-heavy environments that lend itself to vendor rationalization.

As one element of the Kyndryl Security & Resilience capabilities, Kyndryl zero trust services are divided into four main domains: identity and access management, endpoint security, network security, and data privacy and protection. In total, there are 27 zero trust offerings of which 15 are advisory and consulting and 12 managed services. Because this is part of the larger framework of security assurance and incident recovery, Kyndryl is able to deliver organizationwide zero trust principles for holistic business outcomes and not just focus on service or solutions silos.

The Kyndryl Zero Trust Adoption Framework is employed to give clients a direction and vision of what zero trust will look like for that specific enterprise. Kyndryl works with clients' IT and security teams to define goals (for the business and internal cultural adoption) and objectives (whether in terms of technology, architecture, or governance and reporting) that need to be executed with new or existing IT and business processes for zero trust enablement. Kyndryl says that cultural adoption, or change management, is key to a successful zero trust project.

Kyndryl offers very detailed road maps and process steps for identity, devices, networks, apps and workloads, and data during the initial zero trust definitions and vision phase all the way through provisioning, refining, and scaling the zero trust effort across the enterprise. The Kyndryl Zero Trust Maturity Assessment (ZTMA) helps customers measure progress in their zero trust journey. During this, Kyndryl evaluates clients against a set of industry-standard zero trust principles to align business and IT

priorities with customers' individual security risks and compliance requirements. This includes:

- Identifying security gaps against Kyndryl's governance model
- Developing a zero trust security road map conforming to a client's specific security, industry compliance, and investment strategy requirements
- Following a use case–driven approach to help strengthen zero trust capabilities across multiple security disciplines for faster zero trust model adoption

Kyndryl claims over 2,000 security professionals specifically dedicated to zero trust services, with another 4,400+ FTEs that support security assurance services, security operations and response services, and incident recovery services.

Optiv/Optiv + ClearShark

Optiv and Optiv + ClearShark have one of the more detailed and far-reaching approaches to zero trust security services. Optiv and Optiv + ClearShark (Optiv acquired ClearShark in March 2023 to double its presence in the federal sector) see zero trust as a means to achieve the goal of risk reduction and reduce the attack surface. The difficulty many enterprises have with a zero trust project, from Optiv and Optiv + ClearShark's perspective, is that one size does not fit all, and therefore you must look at risk assessments to determine the criticality of services and controls that will be utilized in a zero trust project. As part of this perspective, the two organizations help clients understand that zero trust is not a technological problem but an enterprise mindset around controls and access.

Along these lines, Optiv and Optiv + ClearShark approach zero trust based on four overarching themes that will guide the zero trust project and act as desired outcomes for their clients:

- Adopt a context-based security model, which actively consumes risk-based information to secure business assets
- Default to "trust nothing" so that any entity (i.e., user or device) is a potential threat actor
- Secure the IT and security environments with architectures that create risk-based perimeters around business resources
- Maintain comprehensive visibility across the enterprise with response activities that respond to any breaches/changes

The Optiv zero trust maturity journey includes 9 pillars and 63 capabilities. During the initial assessment phase, a client's current capabilities are measured against the Optiv and Optiv + ClearShark model. This includes gathering information from clients via a 300–400 question assessment process. This approach is based on CISA and DoD zero

trust maturity criteria along with Optiv and Optiv + ClearShark experience and best practices. This hybrid approach is a differentiator for both and creates clearer maturity goals while including the DoD and CISA criteria and ensures a more accurate representation of maturity. Assessments are then generated based on a 1–4 scale, from basic to optimized, and these scores help prioritize processes and services toward zero trust goals.

Optiv and Optiv + ClearShark's zero trust blueprint includes the standard zero trust categories (identity, network, devices, data, and applications and workloads), but the organizations also assess and create road maps for other important areas including, security program management, security risk management, automation and orchestrations, and analytics/visibility. Security risk management includes services for third-party risk management, security metrics, and security controls management. Automation and orchestration include services for policy orchestration, SOAR (security orchestration, automation, and response), and incident response.

The experience of Optiv and Optiv + ClearShark has been that many clients already have services or solutions that can serve as foundational aspects of the zero trust project. However, many times there are internal culture issues in that personnel at executive levels may not understand what modernization associated with a zero trust project can and will drive from an operations, security, and business process efficiency perspective.

Optiv has 400 full-time security professionals based in North America (the United States and Canada) and in India. Optiv has over 6,000 clients.

Note: All numbers in this document may not be exact due to rounding.

ADVICE FOR TECHNOLOGY BUYERS

Achieving zero trust strategy and the "never trust, always verify" model is an ideal that will be a hard-earned but not necessarily an elusive objective. With the right services, solutions, stakeholder buy-in, and expectations, zero trust can be realized, especially with professional and managed services from dedicated and experienced security service providers. Because zero trust addresses so many security pillars and associated solutions, it is best to look at zero trust services that address the concepts of zero trust. These factors, in fact mindsets, to consider are:

- **Zero trust and associated services are not a one-click deployment.** It is too broad and all-encompassing to hit the "easy button."
- **Approaching zero trust is a holistic endeavor.** It includes program assessment and design and change management that has to be supported by managed services, consulting services, and security tools.

- **It will not be possible to have 100% zero trust.** Being pragmatic and methodical will be key to achieving the goals of a zero trust assessment and lowering risk (when balanced against the cost of zero trust projects to get to the zero trust goal).
- **Zero trust will be a continual journey.** Since a zero trust "end of project" is not realistic, having professional and managed services in place to continually verify the pillars of zero trust helps make zero trust part of the IT and security culture. At that point, zero trust, and the elevated security it creates, is able to address enterprise business risk and governance challenges as they arise.

RELATED RESEARCH

- *Market Analysis Perspective: Worldwide Security Services, 2024* (IDC #US50635824, October 2024)
- *Ransomware: Mid-2024 Update — Attacker Methods Are Improving* (IDC #US52611724, October 2024)
- *Ransomware: Mid 2024 Status — Healthcare in the Crosshairs* (IDC #US52608424, October 2024)
- *IDC PlanScape: Cyber-Range Security Services* (IDC #US52544324, September 2024)
- *IDC Market Glance: Managed Security Services, 3Q24* (IDC #US52593324, September 2024)
- *IDC Market Glance: Professional Security Services, 3Q24* (IDC #US47972522, September 2024)
- *IDC's Worldwide Security Services Taxonomy, 2024* (IDC #US50636024, June 2024)

ABOUT IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology, IT benchmarking and sourcing, and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives. Founded in 1964, IDC is a wholly owned subsidiary of International Data Group (IDG, Inc.).

Global Headquarters

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com