White Paper

Maturing Your Zero Trust Approach

Sponsored by: Kyndryl

Philip Bues
May 2023

EXECUTIVE SUMMARY

Cybercriminals, inflationary pressures, geopolitical tensions, remote work, and the talent gap have pushed organizations into a new risk landscape. The COVID-19 pandemic accelerated digital transformation (DX) to the public cloud for many organizations with the promise of reduced costs and stronger security. This new adventure revealed weaknesses for which most organizations were ill-prepared.

Cloud environments are not static and require modern internal granular access control strategies and approaches, as part of a program many refer to as zero trust. The U.S. government has embraced the zero trust model in a series of communications from the federal branch requiring federal agencies and some contractors to meet specific zero trust architecture (ZTA) cybersecurity standards by the end of fiscal year (FY) 2024. There's been a lot of confusion in the market when it comes to zero trust, but the work being done by the U.S. Cybersecurity and Infrastructure Security Agency (CISA) and the federal government mandates provide the Zero Trust Maturity Model that organizations can rally behind. Now that we have a baseline model, the next step is putting this into practice. That's the really tricky part.

This white paper explores zero trust with Kyndryl Services under the guise of the CISA maturity model's five pillars: identity, device, network/environment, application workload, and data. Understanding the key first steps to establishing a zero trust program and assessing an organizational risk and security posture readiness must include preparing a case for stakeholders that recognizes "security risk is business risk."

SITUATION OVERVIEW

Evolution of Digital Transformation

While most organizations tend to prioritize go-to-market activities in their cloud migrations, business outcomes will be negatively affected if cloud security posture and hygiene are afterthoughts. Digital transformation accelerated cloud migration by turning to a lift-and-shift model, leading to implementation complexities and leaving gaps in defenses. Bad actors including cybercriminals and malicious insiders took advantage, launching ransomware and cryptojacking attacks both in the cloud and on premises. As participating organizations came to find out, on-premises legacy security does not translate well to the cloud.

Cloud complexities exponentially grew again in a new hybrid multicloud reality. Organizations became victims of their own success, often adding on point product solutions and additional public cloud

service providers to avoid vendor lock-in concerns. The use of on-premises private clouds remained among heavily regulated industries such as finance and healthcare. Unresolved complexities led to ransomware as a service, supply chain disruptions, zero-day vulnerabilities, and insider attacks, and the talent gap took center stage as identity became the new perimeter.

IDC believes while making changes may be disruptive in the short term, "disruptive" technologies and frameworks can also be a competitive advantage. Enter the zero trust framework.

IDC defines zero trust technologies as the use of micro-segmentation, identity-aware proxies (IAP, aka zero trust network access), and advanced authentication and encryption (aka software-defined perimeters) to minimize your blast radius in the event of a compromise. Zero trust is a holistic security framework that matures over time. Security practices such as developing a security-first mindset, least privileged access (LPA), and continuous monitoring/assessment are part of its DNA. As a guiding principle, zero trust treats all content as potentially malicious — whether or not it's from a trusted source — and treats all employees and contractors as potential insider threats, regardless of authentication.

Zero trust is now considered table stakes by many cloud-native organizations. What began as an initial response to traditional security practices including external perimeterization efforts being insufficient now just scratches the surface. While most organizations agree that for many applications, the benefits of public cloud outweigh those of on-premises deployments, understanding the shared responsibility model (SRM) requires a certain level of sophistication as organizations are responsible for security in the cloud, and depending on your cloud service provider (SP), the proverbial line in the sand can be difficult to see, creating gaps. Zero trust seeks to remove some of the complexities introduced by adhering to the principle of "never trust, always verify." Security becomes built in.

The intelligence gathered using a zero trust approach is almost infinite as the users, identities, and devices are continuously being authenticated and then authorized and all traffic is logged and inspected, which feeds and supports the real-time monitoring and analytics. Each customer challenge is unique and may require customized configurations. For example, if a security team member is addressing device security, they would add compliance to the base principle of least privilege (POLP) policies, while with applications and workloads, the approach may be to take advantage of DevSecOps, software supply chain security, and backup and recovery services. These layered security approaches with zero trust requires balancing friction to optimally mitigate risks.

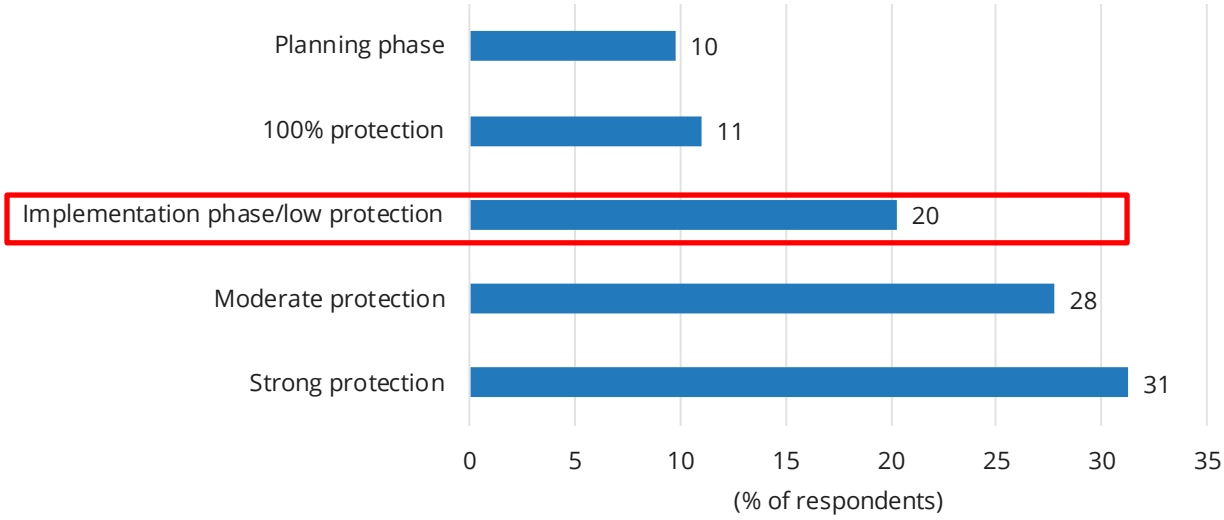
Zero trust also helps reduce pressures felt by the CISO and CIO to regularly present to the board and meet increasing compliance and cyberinsurance audit mandates, as cyberinsurance rates rise. The talent gap, insufficient cloud security skills, and difficult tools are still considered the biggest challenges to cloud adoption. Zero trust is now a "digital first" mandate. Security is now being viewed as a long-term investment, and just as a cloud journey happens in phases, so does zero trust. Owing to these dynamics, many organizations engage with a professional or managed services provider for consultation, implementation, and/or management.

IDC studies show organizations assert that public cloud is more secure, and positive business outcomes include cost savings, faster time to market, and improved user loyalty. Yet 20% of organizations rate their security posture readiness as "implementation phase/low protection" (see Figure 1). Security is provisioned differently in the cloud. Organizations know this, yet even mature security programs have their doubts.

FIGURE 1

Security Posture Readiness

Q. *Bad actors, some led by nation-states, are now targeting even those organizations with mature cloud security programs. In light of this, how would you rate your organization's security posture readiness?*



n = 400

Source: IDC's *U.S. Cloud Security Survey,* December 2022

Evolution of Zero Trust

Traditional perimeter security models of firewalls and organizational zones assumed that everything inside the network could be trusted. But compromised resources, devices, or users exposed the network to malicious actors and threats – many of which were free to move laterally to servers and data expanding the attack surface. Security is provisioned differently in the cloud and the ever-changing threat landscape required a radical shift in philosophy. By assuming that any device or user attempting to access a network, application, or resource is already compromised, organizations can take proactive steps to protect their networks and resources. This is zero trust. Zero trust evolves the security model to address varying risk levels, the difficulty in maintaining zones of trust, and the lack of "inside" or "outside."

Today, zero trust relies on advanced and step-up authentication challenges in concert with traditional technologies that include micro-segmentation, identity-aware proxies, and encryption (see Figure 2):

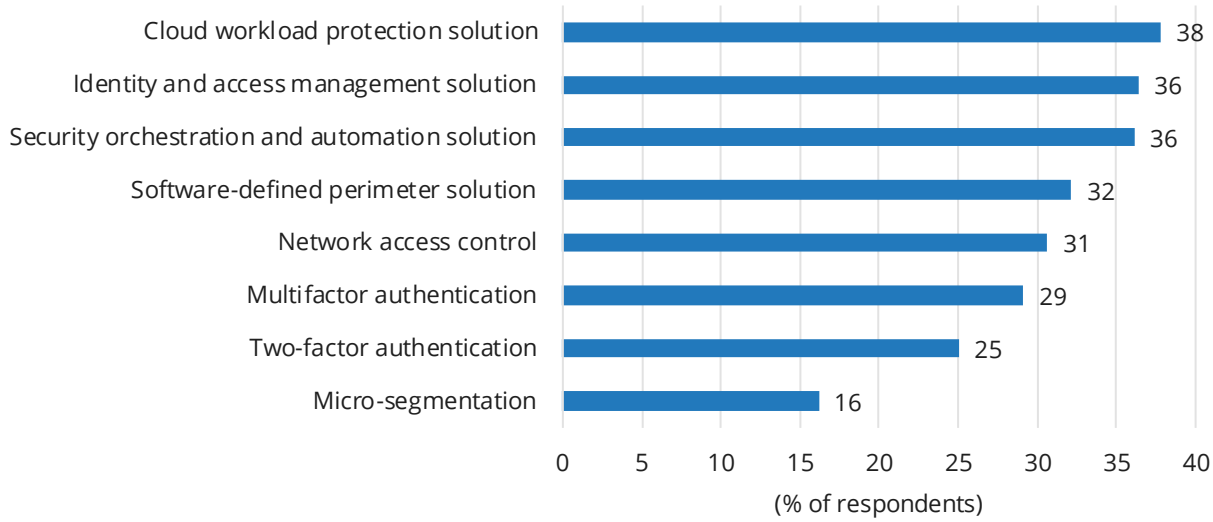
- Micro-segmentation evolved from firewalls and is a method to create secure zones that address lateral movement threats in datacenters and hybrid cloud environments.
- IAP is a modern approach to secure access of internal applications and systems for users outside of the network perimeter.
- Encryption (software-defined perimeters) allows users and devices to be authenticated for encrypted communications with granular access to applicable applications inside and outside the enterprise, thereby limiting the attack surface.

Organizations quickly realized that while shifting to a proactive security model such as zero trust, the new approach required additional solutions including workload protection, security orchestration automation, and data protection. These traditional and modern technologies align with the pillars of CISA's Zero Trust Maturity Model of implementation: identity, device, network/environment, application workload, and data.

FIGURE 2

Top Zero Trust Technologies Include Both Traditional and Modern Solutions

Q. What are the primary technologies you identified to achieve your zero trust strategy?



n = 1,445

Base = all respondents except those not planning to implement a zero trust strategy

Source: IDC's *Security Services Survey,* February 2022

However, as stated previously, this is a journey rather than an act. As organizations work to bring their security requirements up to date, ongoing cloud security assessments are a logical first step. Depending upon the security maturity of the organization, this may begin at different times during its cloud journey at planning, migration, or optimization. It's never too late, but earlier is better. To achieve zero trust, define your environment, identify and investigate your asset and resource inventory, and understand the technologies and how they interconnect. The key is to perform continuous monitoring and assessment. In this age of resource-constrained security teams, this may seem disruptive, and rightfully so; however, there is another way. Managed service providers, infrastructure providers, and consulting partners can help facilitate zero trust implementations. The improved visibility, automation, and governance controls help organizations make better security decisions by defining and enforcing security policies and compliance requirements.

BREAKING DOWN SILOS AND EXECUTIVE ORDERS

The federal zero trust architecture strategy is a bold move by the U.S. government to defend its systems from cyberattacks in a manner that's consistent with what many leading organizations have, or are in the process of integrating, within the private sector. The high hurdle here is adjusting complex and expansive systems and applications to integrate with the available identity security technologies in order to address the new authentication, authorization, and session management requirements in the time frame allotted. This strategy, set forth by the Office of Management and Budget (OMB) Memorandum M-22-09, may result in a web-based renaissance for identity systems within the federal government that could easily spill into the private sector and whose effects can already be felt and seen.

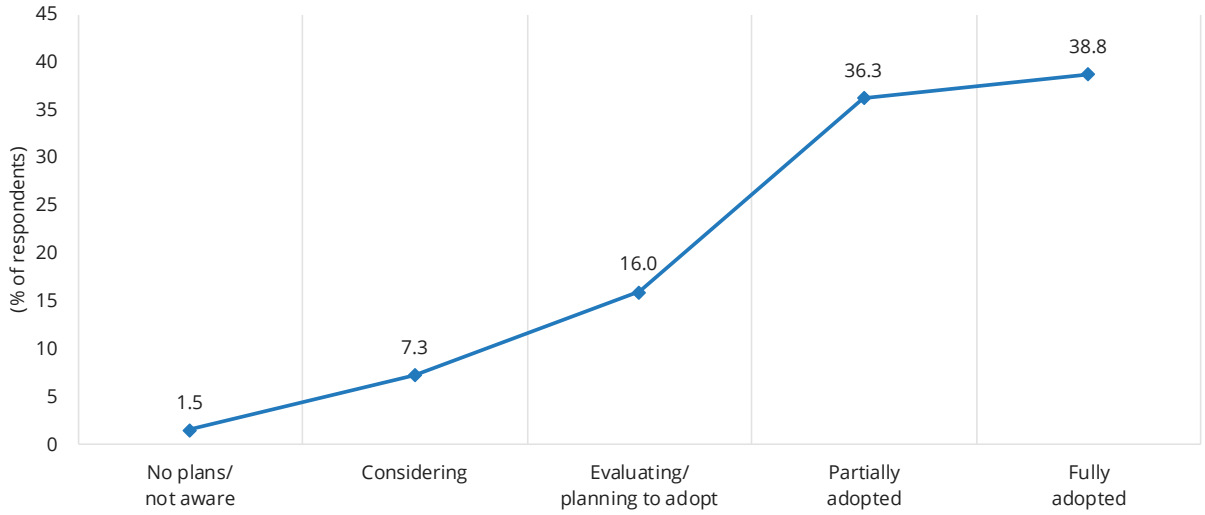
If integration is the high hurdle, then culture is the pole vault. The most obvious challenges are the cultural nuances of bringing together historically siloed teams of CloudOps, DevOps, NetOps, and SecOps. Outside of the regulatory and compliance mandates at the federal level, security teams must prove that their zero trust framework will not hold up development or increase time to market.

To help facilitate these conversations, organizations should consider establishing or using their cloud center of excellence (CCoE) to further collaborate with their managed security SPs to drive the sharing of information and zero trust implementation. The CCoE is more a neutral third-party voice with a centralized view and budget. In IDC's December 2022 *U.S. Cloud Security Survey,* over 75% of organizations responded that they have either partially adopted or fully adopted a CCoE (see Figure 3).

FIGURE 3

Adoption of Cloud Center of Excellence

Q. Does your organization currently have a cloud center of excellence?



n = 400

Source: IDC's *U.S. Cloud Security Survey,* December 2022

Remember, the best time to address a security breach or incident is before it occurs. Organizations thinking about defending rather than being proactive will suffer the consequences.

ESSENTIAL GUIDANCE

Organizations realize that to take advantage of all that cloud has to offer, they must secure their environments. The benefits of zero trust include increased security, improved compliance, and reduced costs. By assuming that any device or user attempting to access a network, application, or resource is already compromised, organizations can take proactive steps to protect their networks and resources. This can help prevent data breaches, reduce the risk of malware or other malicious activity, and improve compliance with regulations such as HIPAA, PCI-DSS, and the GDPR. In addition, by reducing the attack surface of an organization's network, zero trust can help lower costs associated with security and compliance. Zero trust strategy checklist considerations are:

- Zero trust table stakes should include:
  - Understanding your security health and hygiene
  - Identifying any organizational friction or lack of buy-in from stakeholders and developing use cases that align to business objectives
  - Recognition that there is a talent shortage
- Conduct a risk and readiness assessment.
- Establish a risk matrix of positive/negative risk-based outcomes and strategies.
- Partner with your cloud vendor/managed security SP and ask:
  - How are assets and data managed?
  - Will enabling zero trust affect current development processes?
  - Is it clear which identities, both human and nonhuman, have network access, device access, and read/write privileges to specific data sets — in real time? Detailed data is needed to make risk-based decisions.
- Tie readiness assessments and results to control frameworks.
- Align strategic investment decisions with technologies that will support the security improvements delivered with zero trust.

Moving to the cloud gives you better access to trained and specially certified practitioners with expertise including integrating existing and new cloud-native security solutions and frameworks, especially around building automation in the workflow, identity and access management solutions, multifactor authentication, SSO and least privileged access, and cloud workload protection.

SOLUTION

Consistent with current industry thinking, Kyndryl's zero trust services model assumes that any device or user attempting to access a network, application, or resource is already compromised and should be treated as untrusted. This approach is designed to protect against both internal and external threats and to minimize the attack surface of an organization's network. It's a modern cybersecurity strategy that understands security risk is business risk and is proactive in securing a cloud environment by interconnecting multiple visibility points, automating detection and response, and performing risk-aware access decisions.

Kyndryl does this by:

- Leveraging your existing security investments for quicker results and better returns on investment (ROI)

- Driving prevention by identifying risks and recommending solutions across complex multicloud environments
- Providing multidisciplinary security expertise
- Applying zero trust principles to secure business outcomes

Kyndryl's zero trust services also include being able to consult and build consensus with multiple audiences, from the C-suite to the security practitioner. As a trusted partner, it can bring together previously siloed teams and break down the cognitive dissonance that may exist in the C-suite.

Today, organizations are faced with a myriad of security challenges. Whether it is ransomware, shadow IT exposures, zero-day vulnerabilities, user authentication bypasses, or alert fatigue — they all deplete what little energy the cybersecurity team has left. Kyndryl recognizes that it takes a holistic, unified security-first approach to secure modern cloud environments.

CHALLENGES: OVERCOMING ZERO TRUST IMPLEMENTATION

It's a cloud *journey,* so you need to be thinking long term. Despite the benefits of zero trust, there are also challenges that organizations may face when implementing this security model. One of the main challenges is that zero trust can be complex to implement, especially for organizations that have large and distributed networks. In addition, zero trust can be difficult to manage, as it requires constant monitoring and updating to ensure that it remains effective. Another challenge is that zero trust can be costly, as it requires significant investments in new technologies and processes. A "trusted" third party such as a managed security SP can help organizations sort through the complexities and help create a plan to develop internal support and to budget accordingly.

CONCLUSION

Overall, zero trust is a framework and security philosophy that can be used to protect an organization's networks, applications, and resources from both internal and external threats. It is a proactive approach to security that can be used to reduce the attack surface, improve compliance, and reduce costs over time. Realizing that zero trust frameworks should be adaptive as one size does not fit all will lead to collaboration between previously siloed teams, improving your chances of success. Every cloud journey is unique, but there are proven best practices that lead to an elevated security posture:

- Develop use cases to create a cultural shift to a security-first mindset and remove organizational friction by aligning to business outcomes.
- Ask the right questions and engage your cloud center of excellence.
- Understand your environment.
- Assess your risk and security posture readiness.
- Consult with a cloud service provider or managed security SP before choosing your zero trust framework and strategy.

These are the key steps to maturing your zero trust approach.

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. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

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