IDC ANALYST BRIEF
Sponsored by: Zscaler

A successful migration to a zero trust architecture will require a smart combination of updated security practices and modernized security solutions.

Implementing Zero Trust as a Foundation for Secure Business Enablement

April 2022

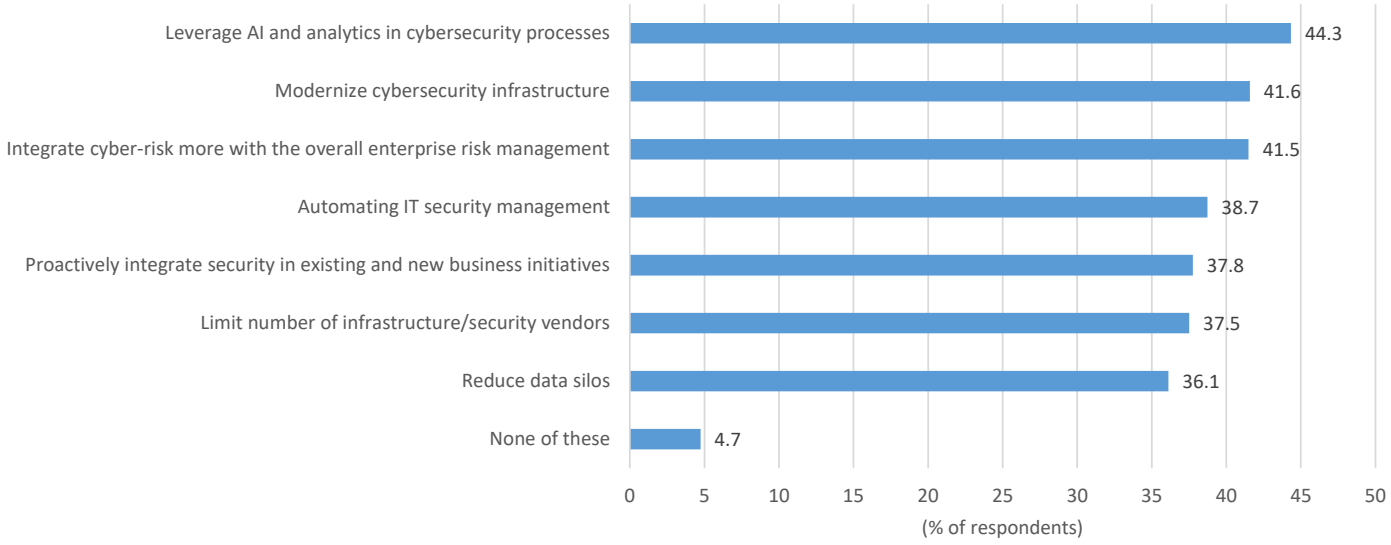
Written by: Christopher Rodriguez, Research Director, Network Security Products and Strategies

Executive Graphic

FIGURE 1: ***Digital Trust Investments Span Infrastructure Modernization and Advanced Analytics***

IT Buyers Cite Digital Trust as a Priority Investment Area for the Next 2 Years

Q ***Specific to security in 2020 and 2021, in which of the following areas has your organization invested or is your organization planning to invest to improve organizational (zero) trust?***



n = 507

Source: IDC's Future of Trust Survey, February 2021

Introduction

The cybersecurity industry has been locked in an ongoing game of evolving attack and defense strategies since the telecommunications era began. In 2020, the threat landscape accelerated with a sharp rise in ransomware and supply chain attacks that exploited gaps in legacy defenses, leading to several high-profile breaches in government agencies, critical infrastructure, large enterprises, and even security companies. For example, the highly publicized SolarWinds supply chain attack led to breaches at multiple U.S. federal agencies including the Department of Energy, Department of the Treasury, and Department of Justice, as well as state and local governments.

Traditional security architecture was designed for a time when employees primarily worked in an office setting, using corporate-issued devices to access resources in a datacenter. The modern enterprise IT environment is a maze of complexity, with applications, services, data, and other resources spread across multiple cloud environments and datacenters. Users may work in the office, on the road, or at home. Devices may include managed/unmanaged devices, personal devices, and IoT and OT devices. Legacy defenses that are static, perimeter oriented, and coarse are incapable of addressing threats that are dynamic, evasive, and persistent.

The situation has driven demand for modernized security strategies such as "zero trust" into broad mainstream adoption. The term is beginning to translate to a set core of technology solutions as well, such as zero trust network access (ZTNA). However, a degree of confusion about zero trust remains as IT buyers are inundated with marketing messages that define the issue too narrowly or too broadly. This IDC Analyst Brief will review the future of zero trust and the implications for enterprise security architecture.

Definition of Zero Trust

"Zero trust" is a strategy to realign security practices and tooling into a modern security architecture that ensures least-privileged access to data and resources. Access decisions are based on strong identity validation, context-aware policies (e.g., location, time, device type/status, user behavior), and authorization that is as granular as possible. A guiding principle of zero trust is to assume that the network has already been compromised, thus reinforcing the need to move away from implicit trust based on user location and an overreliance on perimeter-based protections.

Zero trust architecture is the blueprint by which enterprises can implement these zero trust concepts. Accordingly, zero trust architecture features the following foundational elements:

- **Granular authorization:** Ideally, only one entity is connected to another, specifically and purposefully. Full network access is not provided—instead, users are provided with controlled, conditional access to only the specific application required.
- **Strong identity and authentication practices:** These practices include MFA and continual monitoring. User identity is validated for each session and during sessions.
- **Dynamic context-based policies:** Geographic location, application type and risk level, time of day, and device type/status are useful contextual factors for determining risk thresholds.

- **Universal application of zero trust:** Zero trust must be extended to all entities, subjects, and resources. Note that "subjects" typically refers to human users but should also account for devices, applications, and workloads that communicate with each other.
- **Continuous threat detection/protection:** Threat intelligence and security analytics are key to identifying zero-day threats and threats that abuse their "trust" status, including insider threats and compromised accounts.
- **"Need to know" access only:** Data and resources are protected entirely behind policy enforcement points, are accessible to only authorized users under specific controlled conditions, and are invisible to all other users.

Benefits of Zero Trust Adoption

Zero trust architecture is an encompassing strategy spanning systems for identity, authentication, endpoints, devices, users, and infrastructure. Realigning these systems in accordance with zero trust principles yields an optimal security posture. Furthermore, technology solutions are being introduced into the market to aid enterprises in the evolution to a zero trust architecture, such as zero trust network access:

- **Reduced business risk of advanced threats, data theft, ransomware, and lateral movement of threats:** In IDC's *Future Enterprise Resiliency and Spending Survey*, 54% of organizations reported one or more attacks that blocked access to systems or data; one in five victims paid a six-figure ransom. Detection or disruption early in the kill chain prevents costly breaches or ransoms down the line.
- **Zero attack surface:** Applications are hidden completely behind policy enforcement points and only connect out to authorized users. Therefore, applications are invisible to users that block scanning, brute force attacks, DDoS attacks, exploits, and other unwanted activities.
- **Reduced lateral movement:** Zero trust isolates the applications from the network. As a result, malicious entities that gain network access cannot discover or connect to resources and data. This capability is key to mitigating damages— that are common in flat networks — from ransomware, insider threats, and other threat actors by preventing lateral movement.
- **Session-specific risk threshold:** Enterprises can determine and manage the risk based on session-specific factors (e.g., user, device type and posture, application risk, and data type).
- **Improved user experience:** Traditional security architecture requires IT organizations to backhaul traffic to the perimeter for inspection. Zero trust solutions are typically cloud services at the edge, closer to the user, that can avoid this unnecessary detour. Policy enforcement and protections are applied inline, rather than redirecting traffic to a specialized cloud service, which avoids the related latency and potential disruption posed by each additional hop.
- **Reduced cost and complexity:** Perimeter-based security remains in use but is difficult to scale up, whereas cloud services offer advantages of flexibility and elastic scalability.

- **Regulatory compliance:** In IDC's *Future of Trust Survey*, IT leaders were most concerned about "complex regulatory requirements" (28%), second only to "increasingly sophisticated cybersecurity attacks" (31%). Executive Order 14028, Improving the Nation's Cybersecurity, indicates that zero trust strategies will soon be the expectation rather than the exception.

Considerations for the Future Zero Trust Adopter

Zero trust is poised to play a foundational role in the evolutionary process toward zero trust adoption. However, there remains a high degree of confusion regarding zero trust.

Zero Trust Myths and Misperceptions

- **Duality of zero trust:** Zero trust is a strategy — a set of principles that ensure security in the modern digital transformation era. Whereas, implementations, such as ZTNA, are solutions that operationalize zero trust principles for a hybrid workforce.
- **The "magic pill" problem:** Zero trust is not a security magic pill. Security is not an end state; it is a process. It's not a product, but a solution that needs a foundational element that should be delivered as a platform and is extended with partner solutions such as identity management and endpoint security.
- **Zero trust "washing":** Zero trust is simultaneously clear on its principles and open to interpretation. As a result, some technologies simply approach zero trust from different perspectives. Unfortunately, some marketing messages apply the term "zero trust" incorrectly, which generates confusion in the marketplace. For example, firewalls are unable to block bad actors that imitate legitimate users and don't effectively secure remote users, data, and cloud-based applications outside the network perimeter, and yet try to label them as zero trust solutions. Moreover, they do not provide the granularity, strong identity validation, context-based policies, and access prescribed by zero trust principles. Similarly, cloud security services may be mistaken as zero trust. IDC notes that cloud security services designed around broad access policies or coarse segmentation should not be confused for zero trust.

Alternatives and Complements

- **Secure access service edge (SASE):** SASE is a name for a trend of convergence that has gained popularity in the market. Positively, SASE addresses the much-needed plan for security convergence but also introduces the need for comprehensive WAN capabilities. Unfortunately, SASE has generated significant confusion about the need for converged network and security infrastructure. The cloud/edge delivery model has driven interest as one means to adapt to the demands of the digital transformation era. SASE definitions vary between vendors; some SASE solutions focus on VPN for connectivity rather than ZTNA.
- **Security service edge (SSE):** By comparison, SSE similarly advocates for the integration of a comprehensive network security stack delivered as a cloud service. Importantly, SSE separates the networking function requirements, which has made adoption more straightforward.

Conclusion

The traditional security architecture is showing cracks with each passing year. Yet many organizations continue to take a "go with what you know" approach, attempting to adapt on-premises security tools, firewalls, cloud services, and point solutions, which leads to compounding the challenges of security complexity, gaps, and lack of scalability. Instead, a successful modernization of the security architecture should focus on the incorporation of zero trust principles. In addition, purpose-built, edge-delivered zero trust solutions are an important consideration for enterprise organizations to fully (securely) embrace digitally transformed IT environments comprising a spectrum of users, devices, workloads, and data types.

About the Analyst

Christopher Rodriguez, *Research Director, Network Security Products and Strategies*

Christopher Rodriguez is a Research Director in IDC's Network Security Products and Strategies program covering technologies designed to secure today's complex enterprise networks. The IDC Network Security Products and Strategies practice covers specific technologies including firewall/UTM, intrusion prevention, cloud security gateway, messaging security, web security, and web application firewall.

MESSAGE FROM THE SPONSOR

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at www.zscaler.com or follow us on Twitter @zscaler.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com