RE-THINKING SECURITY FOR RESILIENT BUSINESS

Authors:

Richard Thurston

November 2023

An IDC Vendor Spotlight sponsored by Zscaler

IDC #EUR151198723

Rethinking Security for Resilient Business

Introduction

Zero trust is an enterprise-wide approach — a set of principles — that enables secure access to applications and network resources based on least-privileged access and granular access control. Enterprise networks have transformed as employees have required access to resources wherever they work. Cybersecurity must keep pace with that change.

Zero trust marks a major architectural evolution from traditional perimeter protection, which is no longer fit for purpose. Should a breach occur, zero trust reduces the risk of harm from malicious threats by preventing lateral movement through the network.

A guiding principle of zero trust is to connect users to only limited and specific applications and resources based on the assumption that the network has already been compromised. No user or application is trusted by default. Trust is established based on context (e.g., the user's identity and location, the security posture of the endpoint, the application or service requested) with policy checks at each step.

AT A GLANCE

KEY STATS

Zero trust is an enterprise-wide approach that enables secure access to applications and network resources, reducing the risk of harm from malicious threats. It marks a major architectural evolution that reflects and secures today's enterprise requirements and ways of working. Because enterprise skills shortages continue to grow, organizations are reaching out to security vendors and their partners for assistance in harnessing the benefits of zero trust.

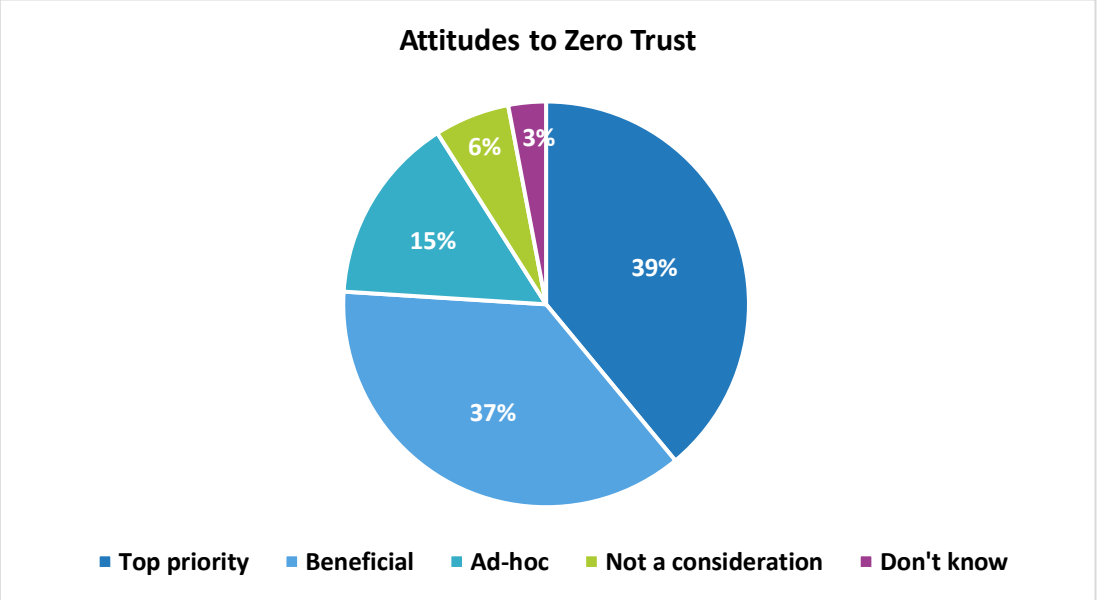
KEY TAKEAWAYS

Two-fifths (39%) of cybersecurity professionals say the adoption of zero trust principles is a top priority for their organization, according to IDC research.

Transformation to a zero trust architecture requires visibility and control over the users and traffic in the IT estate, monitoring and verification of traffic between parts of the network environment, and strong multifactor authentication — and it must be applied across the organization.

Organizations across Europe are at a variety of stages in their transformation to zero trust, but most organizations have embarked on the journey to some extent. According to IDC's *European Security Strategies Survey 2023*, 39% of cybersecurity professionals say the adoption of zero trust principles is a top priority for their organization. Just 6% say it is not a consideration for their organization (see Figure 1).

FIGURE 1
Attitudes to Zero Trust



Source: IDC's *European Security Strategies Survey 2023*, n = 700

The primary factors driving the move to zero trust vary among organizations. Hybrid working and a preference for cloud-based security are two of the most commonly cited reasons, according to IDC research. Some organizations say that, for them, zero trust is driven more by regulatory or reputational concerns, or in reaction to a failure to address previous cybersecurity incidents. The mix of these drivers varies by sector and, to some extent, by the size of the business.

Zero trust must, of course, be deployed organization wide. Otherwise, threat actors will circumvent the controls.

Organizations are, in general, grappling with a shortage of up-to-date cybersecurity skill sets — and zero trust is no exception. Just 29% of cybersecurity professionals in Europe say their organizations have the internal resources and knowledge to audit, design, implement, and manage a zero trust solution. This implies that the remainder — some 70% — will likely seek third-party support and guidance.

IDC forecasts that spending on zero trust will increase significantly over the next few years. Indeed, IDC forecasts that revenue in Europe, the Middle East, and Africa from zero trust network access (ZTNA) — part of an enterprise zero trust approach — will increase at a compound annual growth rate (CAGR) of 28.3% over the 2021–2026 period, reaching $340.5 million in 2026.

A number of important business and technological changes are driving the need for zero trust. In many organizations, the cybersecurity function is now positioned to enable business change and innovation, to empower workers in hybrid environments, and to mitigate organizational risk.

The volume and variety of threats facing organizations means that technologies and processes must scale and adapt rapidly. Security architectures must continue to support reliable, high-performance connectivity as networks transform to a software-defined approach that supports employees and resources in multiple locations across multiple devices.

Cybersecurity teams must now work closer with leadership and a range of business functions to ensure the alignment of technology and business goals and the delivery of defined business outcomes. The goal is to ensure that the organization operates in an agile manner and is able to respond to myriad disruptive threats.

Accelerated progress in generative AI (GenAI) is serving as a catalyst for the acceleration of business change. Yet GenAI also has an extensive set of risks, underlining the increasing need for improvements in organizational cybersecurity posture.

Benefits

A holistic approach to zero trust provides a number of benefits for organizations, including:

- **Reduced Risk in the Hybrid Working World:** Legacy technologies, including VPNs, enable lateral access across an organization. This may permit an adversary who penetrates the network to access a large number of network resources. Zero trust prevents lateral movement by only allowing trusted and granular access within the network using practices like least-privileged access, context-aware access by application or resource, and behavior monitoring.
- **Understanding Context:** Zero trust enables organizations to make more powerful context-based decisions, rather than simply allow or block a user unconditionally. This means that unusual activity (benign or malicious) can be treated appropriately.
- **Innovation and Agility:** Zero trust approaches facilitate employees working anywhere. This gives organizations the confidence to digitally transform and become more agile.
- **Compliance:** Organizations can demonstrate they have put processes in place to achieve their compliance obligations. Zero trust may also reduce cyber-insurance premiums.
- **Network and Employees:** Zero trust enables a simpler network architecture, protection across on-premises and cloud environments, and a better user experience.

Trends

The concept of zero trust in its basic form has existed for around 20 years, but recently its relevance to enterprise environments has increased and continues to do so. This is due to:

- The loss of any discernible perimeter to the enterprise. Users now require access from home, on the move, in the office, and at other working locations, on a multitude of devices with workloads spread across on-premises and cloud environments.
- Organizations' increased use of the Internet of Things (IoT) requires management of additional identities. Some IoT applications may be predictable, but they provide another attack vector. Operational technology (OT) is being brought within the IT domain of some

organizations, requiring a greater cybersecurity focus on previously under-protected infrastructure.

- Adversaries often target the supply chain of an organization, gaining access via the weakest point. In legacy perimeter-based technology, an adversary can move around the supply chain to execute the kill chain against the desired target. Zero trust reduces this risk.
- Enterprise skills shortages around cybersecurity continue to grow and many organizations do not have the resources or skill sets to effect security transformation on their own. Accordingly, organizations are reaching out to security vendors and service providers for assistance. A combination of vendor and service provider expertise is required to address organizations' complex, ongoing requirements. A comprehensive range of offerings is now available.

Vendor Profile

San Jose, California-headquartered Zscaler is led by 25-year security veteran and entrepreneur Jay Chaudhry. Zscaler counts 40% of the Fortune 500 among its 6,000 customers. It operates globally, offering support to Europe, the Middle East, and Africa from France, Germany, the Netherlands, and the U.K., and to Asia/Pacific from Australia and India.

Zscaler publicly lists some of its "customer wins." Drivers of these wins include large transformation projects and the U.S. presidential executive order requiring U.S. federal civilian agencies to establish plans to adopt zero trust architecture. For some of these accounts, the company has provided tangible ROI metrics. This is expected to help the company prove the value of its proposition to organizations.

Zscaler focuses on three primary offers:

- Modern workplace enablement (providing secure access with a strong user experience)
- Infrastructure modernization (protecting cloud environments)
- Security transformation (covering IoT and OT environments)

IDC has positioned Zscaler in the Leaders category in its MarketScape: Worldwide Zero Trust Network Access 2023 Vendor Assessment.

Zscaler focuses on delivering security from the cloud using a SaaS-based subscription model. It has built out functionality and integrations to deliver on the value and agility promised by cloud security. Zscaler is noted in IDC's MarketScape as a shortlist vendor for enterprise organizations considering a move to cloud security in a digital transformation initiative or for a specific use case. IDC believes Zscaler's extensive track record in cloud scale and reliability, and the breadth and depth of its security capabilities, have demonstrated its ability to support demanding enterprise organizations.

In terms of architecture, ZeroTrust Exchange (ZTX) is Zscaler's zero trust platform that protects data in the cloud, in datacenters, and on premises. It reduces organizations' attack surfaces and helps prevent lateral movement and data loss. It provides per-session policy decisions and enforcement from the vendor's 150 worldwide datacenters. Zscaler reports that use of the

platform doubles every 18 months, which is perhaps not surprising given the escalating threat landscape and the company's customer growth.

The ZTX platform would enable some enterprise customers to consolidate the number of infrastructure vendors, offering potential cost savings and greater network simplicity.

The company continues to expand its offering, with four services announced in June 2023:

- A risk quantification and visualization framework for remediating cybersecurity risk
- An AI/ML-powered zero trust solution to eliminate lateral movement in a branch office IT environment
- A detection and response solution that mitigates the risk of identity attacks
- A feature to streamline the admin experience

Zscaler also made announcements focused around helping customers secure AI deployments, including preventing data loss, risk scoring for AI applications, and greater visibility over AI applications. In the future, due to its advancements in GenAI, Zscaler should be able to offer data leakage protection across video, audio, image, and text formats, and offer more predictive breach capabilities. The company is working on an AI-based natural language interface to its products.

Zscaler's use of AI is not new — it is currently harnessing both GPT4 and an in-house large language model — but these timely offerings will become increasingly important as customers increase their use of AI technologies and establish new use cases.

Zscaler works with an ecosystem of established partners, including Microsoft, CrowdStrike, and AWS. It provides integrations with companies offering cloud, data, endpoint, identity, network, and operations solutions, and provides a large number of solution briefs and deployment guides for enterprises.

Challenges

Zscaler is growing faster than the rates forecast by IDC for the cybersecurity solution and services markets. This demonstrates the strong resonance the company's offerings have with organizations. As with any rapidly growing company, Zscaler will need to ensure continued internal transformation to scale and continue meeting customer needs.

Its channel is a significant asset but this must be optimized. Zscaler fosters a partner ecosystem, based on what is sees as current opportunities, and is striving for greater consistency and proactivity in managing it. The vendor is looking to develop joint solutions and co-selling approaches with the right partners, rather than just measuring partners on top-of-funnel success.

The storms of disruption that IDC often refers to work more favorably for Zscaler than for other companies. Organizations' focus on digital transformation is a tailwind for Zscaler's solutions. Other macro factors such as skills shortages and the shift to hybrid working can (unlike other organizations) work in its favor.

Technology budget constraints, long purchase cycles, and a highly competitive market remain a headwind for all technology vendors. Zscaler's ability to offer examples of proven ROI — and the architectural approach described above — will help it overcome those barriers.

Conclusion

Zero trust offers multiple benefits for organizations, including reducing risk and empowering hybrid working. Organizations are at varying stages of transformation to zero trust, propelled by clear business drivers. IDC forecasts spending on zero trust to continue to increase significantly, with many organizations needing third-party assistance to improve their cybersecurity postures. The threat landscape is complex and changing rapidly. A zero trust approach to these challenges provides a firm foundation for building a more resilient and sustainable business.

MESSAGE FROM THE SPONSOR

Zero trust is an approach rather than one single technology. Zscaler's platform is built to ensure the technology implementation of a zero trust approach, reducing operational costs while also improving the security posture of an organization. Together with Capgemini, Zscaler can ensure that organizations have access not just to excellent technology, but also to world-class advisory and transformational consulting to ensure that their transformation journey toward a zero trust platform is seamless and comprehensive. Through their strategic partnership, Zscaler and Capgemini provide customers with a holistic set of services, from advisory and transformation consulting to implementation and managed services, focusing on both the business processes as well as the technology controls.

To learn more about Zscaler Zero Trust offering with Capgemini, please visit www.zscaler.com or contact cybersecurity.in@capgemini.com

About the Analyst

Richard Thurston, Research Manager, European Security Services

Richard Thurston is a research manager in IDC's European Security Services program. He has 20+ years of experience in the technology sector, working as a journalist and analyst (including in IDC's Infrastructure and Telecoms team), working for U.K. regulator Ofcom, and in a number of research, insight, and thought leadership roles for cybersecurity and communications service providers. Richard is based in the U.K. and holds a degree in Mathematical Statistics and Operational Research and a diploma in Economics and Econometrics from the University of Exeter.

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 1,300+ analysts worldwide, IDC offers global, regional, and local expertise on technology and industry opportunities and trends in 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.), the world's leading tech media, data and marketing services company.

IDC U.K.

5th Floor, Ealing Cross,
85 Uxbridge Road
London
W5 5TH, United Kingdom
44.208.987.7100
Twitter: @IDC
idc-community.com
www.uk.idc.com

Global Headquarters

140 Kendrick Street,
Building B
Needham,
MA 02494
+1.508.872.8200
www.idc.com

IDC Custom Solutions

This publication was produced by IDC Custom Solutions. As a premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets, IDC's Custom Solutions group helps clients plan, market, sell and succeed in the global marketplace. We create actionable market intelligence and influential content marketing programs that yield measurable results.