ANALYST CONNECTION

Sponsored by: Comcast Business

Zero trust isn't a single tool that can be deployed; rather, it's a framework applied to a combination of products and technologies. This Analyst Connection examines how organizations can best understand and establish a zero trust framework.

Dispelling the Common Myths of Zero Trust Security

January 2022

Questions posed by: Comcast Business

Answers by: Amita Potnis, Director, Future of Trust Global Practice

Q. What is zero trust?

A. Zero trust is a cybersecurity model in which no level of trust is automatically granted to any end user or computing resource accessing an organization's network. Zero trust has emerged as a cybersecurity strategy to protect modern digital environments where network parameters are no longer clearly defined and because applications and data are often hosted in the cloud instead of being secured on premises.

IDC's 2021 *Future of Trust Survey* found that the biggest challenge to establishing zero trust is the rate of increasingly sophisticated cybersecurity attacks. The digital world consists of data, users, devices, applications, workloads, networks, and deployment models (on premises, hybrid/multicloud). As workloads are increasingly delivered in the cloud and accessed through various devices and locations, the traditional means of safeguarding the network perimeter don't effectively scale or protect digital assets.

Moreover, remote and/or hybrid work is here to stay, thus requiring better controls to protect against potential cyber-risks. Zero trust is designed to address these challenges. Zero trust shifts access controls to the network based on device and user authentication and does not rely solely on perimeter-based firewall security. It requires verification all the time, treating access from within the network the same as access from outside the network.

In other words, no network user is trusted — period. Zero trust also implies more stringent authentication methods and uses a "least privilege" account philosophy. More stringent authentication compels the implementation of live validation of access requests for attempts to use any corporate resource based on the user, the user's privileges, and the nature of the device being used rather than validation only at the network perimeter.

Q. Is zero trust a technology or an approach?

A. This is a common question, so let's decouple it a bit.

We define the following three technologies in our zero trust research: software-defined perimeters, micro-segmentation, and identity-aware proxies. These technologies, as well as others such as artificial intelligence and analytics, are poised to revolutionize the way we think about and implement cybersecurity, primarily from the network perspective.

As organizations consider and adopt these new technologies, it's useful to put them into context as evolving from the following cybersecurity capabilities previously (and currently) used:

- **Software-defined perimeters (SDPs)** have evolved from virtual private networks (VPNs) to provide authentication and encryption that address the needs of multicloud hybrid environments. Organizations can refer to the original Cloud Security Alliance (CSA) specification for SDP that uses a combination of controller, gateways, and clients.
- **Micro-segmentation** has evolved from firewalls to provide network filters to address lateral movement threats inside the datacenter as well as hybrid cloud environments.
- **Identity-aware proxies** have evolved to add user-based access control early in the connection process for advanced authentication (such as multifactor authentication [MFA]) and identity federation. A cloud-based platform proxies, inspects, and routes web traffic to approved applications based on security policy.

Zero trust isn't a single tool that can be deployed; rather, it's a framework that can be applied to a combination of products and technologies based on existing architecture. Zero trust, therefore, is an approach that can be thought of as a cross-technology ecosystem/platform designed to protect and secure digital assets by incorporating the principle of "never trust, always verify."

Q. Is zero trust something IT departments can implement on their own?

A. Well, it's certainly possible for IT departments to adopt zero trust technologies, but the strategy requires a total team effort from the organization. I've defined zero trust as an approach that leverages a variety of technologies, but organizations must also consider who will be impacted by these technologies and then define the stakeholders involved when adopting a zero trust approach. Because zero trust requires that every user and device be authenticated and authorized before granting access to applications and data, user experience is a paramount consideration.
Any organization seeking to adopt zero trust will need to invest in greater coordination across business units to increase awareness and understanding of the potential benefits and advantages.

Adopting zero trust technology requires cultural preparation. Organizations should be prepared to articulate zero trust business benefits to users, provide change management leadership, and prepare ways to address any difficulties that a migration to zero trust may cause.

It's important that users be educated on the risk management and trust score approach that can be part of zero trust. Risk management is the identification, evaluation, and prioritization of risks followed by coordinated application of resources to minimize, monitor, and control the probable impact of unfortunate events and maximize returns. IDC research has indicated that the top investment areas to improve trust perceptions and risk management include security, regulatory compliance, and privacy. Large organizations will need to make specific plans to align management across key areas such as identity, devices, applications, data, infrastructure, and networks.

Issues of regulatory compliance and privacy must be addressed in each of the stated areas. Because this approach is built on cross-functional business unit collaboration, organizations should create a business process committee to lead this initiative. Such a committee would help review and find answers to all the business process speed bumps that may occur with this kind of transition, and it can help establish sets of best practices as the effort expands.

Q. Is zero trust costly and difficult to implement?

A. Not necessarily. Zero trust is interrelated to and complements an organization's digital transformation (DX) efforts. The main tenets of digital transformation involve applying new technologies to radically change processes, customer experience, and value. Technologies such as cloud, mobility, big data and analytics, and the Internet of Things (IoT) will be key enablers for the most advanced zero trust use cases.

Ensuring that this digital foundation is enabled by a security-first approach is a crucial step that can't be skipped in DX. Once the business requirements are defined and the risk assessment is complete, this process lays the foundation for a custom zero trust approach best suited for the particular organization. Organizations must also consider the challenge of legacy workloads and applications that zero trust may not be able to support without significant rewriting of code.

Another consideration to smooth the process of zero trust initiatives would be to evaluate the maturity of existing processes against set goals. An ongoing assessment of key performance indicators (KPIs) is necessary to track progress and incorporate changes in an agile manner. Organizations must understand that zero trust is designed to create superior security and protection of digital assets, but a piecemeal approach can also create gaps that are potential risks. Without a deliberate and measurable approach, zero trust initiatives will prove unsuccessful and expensive.

Q. What areas do organizations typically fail to consider when adopting zero trust?

A. IDC believes that organizations need to consider the following key areas when adopting a zero trust approach:

- Organizations need to understand that frameworks are simply guidelines and that the implementation of zero trust policies should be based on the specific requirements of their business. Organizations that want to start moving to adopt zero trust should study the documents provided by the National Institute of Standards and Technology (SP 800-207) and the National Security Agency (Embracing a Zero Trust Security Model).

- Culturally, the "zero" in zero trust can *appear* to conflict with an organization's overall trust initiatives (e.g., environmental compliance, social governance, diversity and inclusion, transparency), causing misconceptions and resistance to this approach. It is imperative that cybersecurity leaders within an organization clearly articulate the true context of a zero trust security policy: It does not mean zero *inherent* trust in the user; rather, it is simply a mechanism to earn trust in the digital world.
- Adopting a zero trust approach is not just about good access control. Rather, it also offers a good baseline for data collection across data, users, networks, workloads, and applications in a programmatic way that can drastically improve visibility and threat intelligence. For example, an organization can set rules related to connections to devices, what is denied, and how details are logged and reviewed. In other words, the ability to detect and remediate against a threat effectively and in a timely manner enables business outcomes such as greater productivity, improved time to market, and lower false positives.
- Organizations should realize that zero trust requires ongoing administration. Frequent and timely reviews of and updates to access control software and policies are integral to ensuring the right users have access to the right data. If organizations cannot act on this quickly, then data will be vulnerable to many cyberthreats, including insider threats and external attacks.

About the Analyst

Amita Potnis, *Director, Future of Trust Global Practice*

Amita Potnis is the global lead of IDC's Future of Trust research practice. In this role, Amita is responsible for leading the development of IDC's global thought leadership research around the growing influence of security, privacy, GRC, social responsibility, and ethics that contribute to organizational trust. Her research focuses on global trends that can measure, enhance, and amplify trust.

MESSAGE FROM THE SPONSOR

About Comcast Business Cybersecurity Services

Your digital enterprise runs on the cloud, and relies on networks, servers, applications, and Internet-connected devices 24/7. With malicious actors targeting these assets, and new threats continually emerging, a strong security foundation is imperative to protecting the integrity of your network. Comcast Business is ready, with cloud-based and software-defined offerings for cyber solutions. Count on a trusted network provider to simplify the complex and help protect your connected devices.

Learn more: https://business.comcast.com/enterprise/products-services/cybersecurity-services

IDC Custom Solutions

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

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.