Defining Zero Trust

July 12, 2022

Director, Community Ecosystem Engagement - Cybersecurity

Michael is a world-leading IT industry analyst. He has led North American and global initiatives focused on developing insights and strategies that connect technology solutions with business needs, combining data, knowledge, analysis and advanced content delivery to define options for IT and buy-side businesses.

Submitted by Michael O'Neil on 12, Jul 2022
Defining Zero Trust

Zero trust thought leadership group members: Geeta Kapoor (BHSH System), Noah Davis (Trane Technologies), Leon Ravenna (KAR Global), Barney Baldwin (ex-MUFG, Columbia), Chase Cunningham (Ericom), Eve Maler (ForgeRock), Sean Frazier (Okta).

A zero trust (ZT) strategy enables an organization to validate access and authorization each time a human or non-human (“carbon or non-carbon based”) user requests access to an asset. Zero trust is often described as a “journey” or as a “framework.” “Journey” articulates the need for ongoing effort, and a holistic program discrete from individual projects or the various technologies that can be deployed to meet ZT objectives. “Framework” denotes a guiding series of principles that directs the zero trust program within and across the six ZT pillars (identity, devices, network, infrastructure, applications, and data), in line with the organization’s ZT strategic objectives.

Executive summary

CISOs must integrate zero trust principles into the business's IT, security, governance, risk, compliance, and privacy strategies. With cloud and mobility integrated into every IT environment, it is not feasible to pursue a security strategy based on a defined perimeter. Zero trust addresses multiple CISO objectives: it defines an incremental, continuous improvement path, it deals with the need to limit intrusions and the "blast radius" from exploits, and most importantly, it enables the CISO to adopt a proactive approach rather than continuously responding to threats. Zero trust is not a technology, and can't be achieved through deployment of a specific product: it requires coordination across all areas of the enterprise, including security and business processes, and security within and across the six ZT technology pillars – identity, devices, network, infrastructure, applications, and data.

Why define ZT?

Zero trust is fraught with confusion. Like many terms in cybersecurity, it's become a buzzword (ab)used in myriad ways by vendors and consultants, making it challenging for CISOs to articulate its true value to executive leadership.

CISOs are tasked with establishing a vision and shared understanding of zero trust within their organizations in order to realize the value of the framework as part of their own zero trust journeys.

What defines ZT?

The zero trust thought leadership group focused on two key points of emphasis: that zero trust is about managing access to important digital resources, and that it is a journey that has no rigidly-defined endpoint.

Access and authority define ZT's key objectives

- Zero trust is an approach to "identifying and securing key assets."
- Zero trust is "right sizing access at every moment."

- “A well-oiled process from when a user or asset joins our environment or ecosystem – that is allowed the least amount of access it needs (regardless of whether it is a person, an application, or a piece of hardware) – that, when it goes from having network connectivity to having access to an application, data, or other resources, is orchestrated in a way that we know exactly what it is, where it is, what its job function is, how much access it needs – and it gets access only to needed resources – that orchestration to me is zero trust.”
- “When people talk about zero trust, they often have these grandiose ideas about what they're going to do. But for me, a lot of zero trust is just reinforcing the concept of least privilege so users only have the appropriate amount of access to do their job and no more.”

Executives who have managed successful ZT initiatives describe a need to balance the breadth of a framework that touches most areas of the business and nearly all aspects of its technology with a requirement to focus ZT activity by highlighting a specific, critical objective. For the thought leadership group, this objective is defined by active, continuous management of *access to* and *authorization to use* data or other IP – particularly, sensitive, confidential, or regulated resources.

Appropriate framing of executive-level discussions about access and authority can be difficult; while executives readily grasp the business rationale for protecting corporate data, the “how” conversation can become quite technical.

Senior leadership team (SLT) executives may appreciate that (to use an example from our thought leader discussions) management of identities after a major acquisition is “extremely problematic,” but still, the cost and time associated with steps needed to remediate this issue – which could include cleaning old directory data, reassigning and limiting permissions, applying segmentation to networks and data infrastructure, and redefining how access and permissions are governed – are difficult for a non-technical leader to grasp.

But the discussion does not lead to a dead end: for example, M&A can create a shared appreciation of the need for a holistic approach to security, and an opportunity to meaningfully and visibly infuse ZT into corporate strategy. To gain buy-in, however, security leaders will need to couch technology objectives in terms accessible to business leaders who lack technical expertise.

The “well-oiled process” quote illustrates one way to bridge this divide. By identifying how all interactions involving corporate assets should be managed through orchestration, the CISO articulates ZT’s technical and business benefits in terms that are relevant to the business leader.

Sticks and carrots drive executive understanding of ZT

Executives most readily grasp the importance of access and authority when they are presented with the upside and downside scenarios that ZT will address. The upside is reflected in the “well-oiled” quote: a ZT-based business can quickly and securely add users, devices, and data from external sources – even entire companies in the case of M&A. Organizations with advanced ZT capabilities achieve a level of agility that less-advanced competitors can’t safely match. The downside to security gaps is written in the headlines of the business press. Executives know that a significant breach will cause major financial and reputational harm. Reducing both the potential for and the impact of breaches is a critical ZT objective: ZT can be seen as a primary means of “limiting the blast radius when something bad happens.”

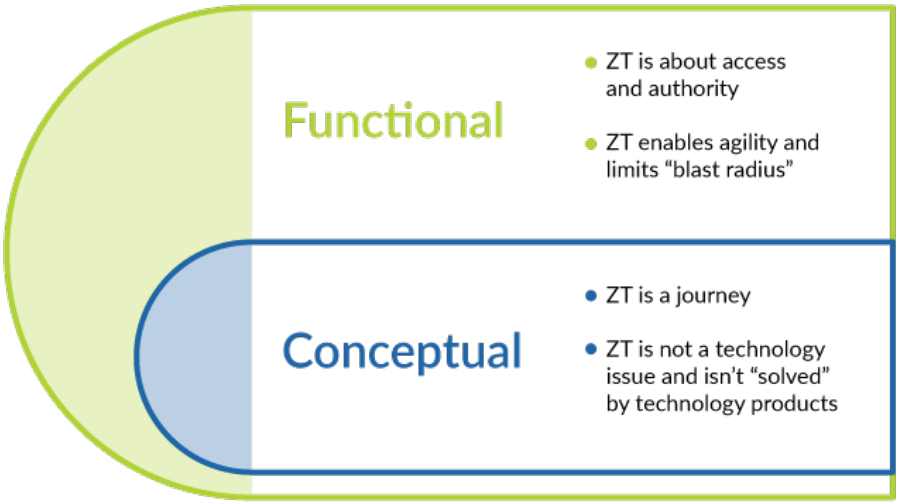
ZT is about a journey – and it is not about technology

- “The first thing you have to do to be successful in zero trust is to *not* look at it as a technology problem. And that's the first thing that people tend to do.”
- “Zero trust is not a product you buy and you deploy and then you're done. It is a mindset.”
- “For me, the organizations who have been most successful with zero trust have adopted it as a lifestyle change and have really looked at it as being able to build security holistically into their entire organization.”

One of the key attributes of zero trust is also one of its key constraints: it is defined by enterprise-wide attention to identifying and protecting critical assets, and not by deployment of a product or set of technologies. In an ideal state, “security functions are baked into business activities, and aligned seamlessly with IT operations;” the security team, IT function, and business operations all view ZT through a common lens.

Emphasizing protection of critical assets is essential for gaining ZT attention and buy-in from the business. While IT may join security in understanding why ZT is strategically important, “zero trust isn't necessarily a huge factor for business executives.”

Discussions around access to corporate intellectual property (IP) can help senior leadership appreciate why ZT is important to the enterprise as a whole: they understand the magnitude of corporate investment in IP and the business harm that would result if IP were stolen. This awareness will build demand for best management of identity and access; CISOs can build on that awareness by articulating the interrelationship between identity and the other ZT pillars.



Source: Stratascale 2022

Working with this content

CISOs looking to integrate this perspective on zero trust within executive-level strategy discussions can use the following challenges/constraints and takeaways to inform their approach.

Key challenges/constraints to building executive endorsement for a ZT strategy

- A journey without a defined end point is difficult to plan and budget for, and a strategy that spans all aspects of technology and many business functions is difficult to encapsulate in discrete, time-limited activities and objectives.
- It's difficult for business leaders "to visualize all the flows and paths for data and how they use it. They are each concerned with a relatively narrow set [of data and data uses based on their function or department.]" The enterprise-wide understanding of data that is inherent to IT perspectives isn't widely shared; CISOs must build awareness of the scope of the problem that ZT is targeted at.
- At a fundamental level, ZT allows for very granular treatment of entities and access requests – but it requires alignment across IT, and between security and the business. CISOs are constrained by the fact that "any enterprise is chock full of people for whom their day job is clicking on links and emails." Navigating the gap between safest and business-critical activities is a major CISO job requirement: "A lot of the big challenges of security are actually misalignment of incentives."

Takeaways from "Defining Zero Trust"

- "Zero trust is the ability to execute security functions in a business context faster, with less pain for everybody involved.**"**
- Digital business **is** business, and requires constant and pervasive internal and external connections. ZT provides the best way to address the dynamic technical needs of the business, offers a holistic approach to managing the volatile threat environment, and supports agility across the business.
- When dealing with business leaders, "take the technical jargon out of the discussion. What does zero trust actually look like, what are the three or five things that have to be done to implement it, and what does this mean (process and objectives both) for the business?"

This is the first of eight source documents included in Stratascale's "An Executive Guide to Zero Trust" research series. We will also publish a capstone report

connecting these eight pieces, plus a six-part companion series (“The Technical Manager’s Guide to Zero Trust”) and several compilations and ancillary documents and tools. Readers interested in specific executive-level perspectives on zero trust may wish to read the upcoming publications in this series: