Deloitte.

CFO Insights
August 2021

Zero Trust: In the face of escalating cyber-attacks, companies target a new level of security

These days, companies spend an abundance of time, energy, and dollars building trust with their various stakeholders—except, that is, when it comes to those accessing their computer networks. The goal there is to thwart cyber attackers even as they become ever-more sophisticated. And that means removing implicit trust from internal networks.

In other words, the familiar "trust, but verify" doctrine is being supplanted by the principle of "never trust, always verify." And to achieve a "Zero Trust" security framework, companies are starting with the assumption that all network traffic, no matter its pedigree, may be malicious. The aim: restrict network access for all users, apply security controls that hide applications not required by the user, and authenticate and continuously validate identities before allowing them to connect only to the applications they need, whether bolted on premises or afloat in the cloud.

The approach obviously represents a dramatic shift from the castle-and-moat framework, which focuses on fortifying the perimeter to deter outsiders from accessing corporate data, while implicitly trusting insiders. In the past, IT infrastructures had well-defined perimeters. But those boundaries have grown blurry as a result of changes in business models, workforce dynamics, and IT environments. Companies have migrated their applications from data centers to the public cloud, with endpoints expanding to include mobile devices, bring your own device (BYOD) technologies, and a proliferation of web-enabled smart devices (e.g., Internet of Things [IoT]). Far from contained, the modern technology ecosphere can appear dangerously ubiquitous.

CFOs can clearly see the potential costs of *not* investing in Zero Trust. The average cost of a data breach has reached $4.24 million, an increase of nearly 10% over last year, according to a recent study. In instances where higher levels of remote

Prior to starting on a Zero Trust journey, companies should develop a clear understanding of what they need to protect, where those assets reside, who should have access, and under what conditions.

work turned out to be a contributing factor, that cost rose to $4.96 million.[1] High-profile ransomware threats that effectively lock users out of their own systems and demand hefty payments before giving them the key (or not) have drawn attention to the costly reputational—and possibly legal—ramifications of a cyber breach. Supply chain infrastructures, targeted through third-party software and service providers, have also been victimized. Moreover, the pandemic has likely increased finance leaders' awareness of the cost of business disruptions, while having to equip a remote workforce highlighted the need to modernize their system for enabling secure remote access.

Implementing Zero Trust, however, is far from quick, easy, or cheap. In this edition of *CFO Insights*, we'll explain what makes a borderless security strategy so vital, which impediments CFOs can expect to encounter during implementation, and how they can better use investments by prioritizing business drivers and associated use cases.

Trust issues

The appeal of Zero Trust is taking root for different reasons. Finance leaders in the midst of leading or co-leading a broader transformation initiative (42% of CFOs, according to Deloitte's *CFO Signals*™ survey for the second quarter of 2021[2]), for example, may want to make modernizing their security model part of that effort. At the same time, with so many businesses planning to offer a hybrid work model, a Zero Trust approach enables companies to offer flexibility while boosting security.

Still, like the rest of the enterprise—which may need a digital transformation to stay competitive post-pandemic—the security model needs to adapt to a new reality. Where once well-constructed firewalls could wall-off intruders, companies now need modern armaments to fend off attackers from many endpoints, including employee devices and IoT-enabled tools—a distinguishing benefit of the Zero Trust model. Companies also need to secure and manage hybrid and multi-cloud environments alongside legacy infrastructure—an effort that can become mired in complexity and operational overhead, as well as talent and skills shortages.

Such a cumbersome environment only increases complexity and vulnerabilities. Zero Trust, which is both a methodology and a mindset, can help accomplish the task of securing an increasingly intricate IT ecosystem by applying various technologies and governance processes to an ever-challenging risk landscape—one that is characterized by geographically distributed operations, remote workforces, and third-party relationships.

The phrase "Zero Trust" refers to the fact that any attempt to access the corporate network must be treated as if it were a breach. Traditionally, remote users gained access by signing on to a virtual private network (VPN). Their assigned IP address served as a free pass, enabling them to go anywhere in the network. Malicious intruders, for instance, might be able to take advantage of this unfettered access to move laterally within the network by exploiting system vulnerabilities and stolen credentials in hopes of gaining access to sensitive information or critical systems. Zero Trust Network Access (ZTNA), by contrast, employs network level security controls to only expose the applications a user needs, thereby preventing anybody from exploring any part of the network to which they don't need access. In addition, the user's network access can be assessed, and access can be modified dynamically based on changing environmental conditions or user behavior (e.g., detection of malware on the endpoint may result in loss of network access or infrequently accessed applications may require additional step-up authentication).

Prior to setting off on a transformation to Zero Trust, companies should develop a clear understanding of what they need to protect, determining where the assets that require protection reside, who and what should be able to access these assets, and under what conditions. They should also determine the criticality of different types of data, the distinct classifications they want to apply, the environmental conditions when access occurs, and, ultimately, which people and devices need privileges to access that data. If an attempted access request looks suspicious—say, someone seeking to use an app they don't typically need—a ZTNA solution is designed to block their path.

Pillar talk

Implementing Zero Trust typically requires breaking down the company's IT security domains into its foundational elements. Rather than even attempt to apply Zero Trust across the entire business, CFOs and other business leaders might want to analyze the seven Zero Trust domains that support IT security, prioritizing them and mapping a plan for moving up the maturity model for each. Maturing Zero Trust capabilities should take a risk-based approach to enforcing "least privilege" access, meaning that users and applications should be able to access what they need and nothing more. Below is a list of the Zero Trust domains and associated descriptions within the context of this leading framework.

1. **Identities** serve as the new perimeter and are the core component of any Zero Trust architecture. Centralize authentication and authorization to enable your workforce to access enterprise resources quickly and securely with streamlined authentication and access management.

2. **Workloads** are applications or services being accessed by users—whether they are hosted on legacy infrastructure or in cloud environments. They can be hardened, segmented, and monitored on a granular level with adaptive actions taken in the case of risk, such as limiting access or blocking uploads to specific applications.

3. **Data** is at the core of an effective Zero Trust strategy. It should be classified and protected in-transit over the network, at rest when stored in the cloud, or on-premises, with advanced data discovery, encryption, and loss-prevention capabilities in place to protect sensitive data.

4. **Networks** carry traffic between users, devices, and applications, with controls that segment (block unintended network communications), monitor, and analyze activity, operating on the assumption that all network connection requests are inherently untrustworthy.

5. **Devices** can entail managed/known types as well as unmanaged (e.g., BYOD) and smart devices (e.g., IoT) that connect to an organization's enterprise assets. Devices should be subjected to continuous assessment for risks and threats; the identity of each device, as well as the user logged in and other contextual signals, should be considered to inform risk-based adaptive access decisions—for instance, what applications that user frequently relies on—to catch anomalies that could indicate a potential intruder.

6. **Telemetry and analytics** collects data from relevant security controls into a centralized monitoring system for event correlation and advanced analysis that can detect suspicious and potentially malicious behaviors. Threat intelligence should also be integrated to enable a threat-driven security posture for the organization.

7. **Automation and orchestration** enables a more proactive security posture by automating detection, prevention, and response actions through integrated security controls. Security operations can ultimately be more productive through automation of investigative tasks in response to an ever-growing flood of security alerts. Integration of the organization security systems allows for orchestration of pre-defined incident response activities in near real-time to not only detect threats but also take action to isolate and neutralize them.

Into the breach

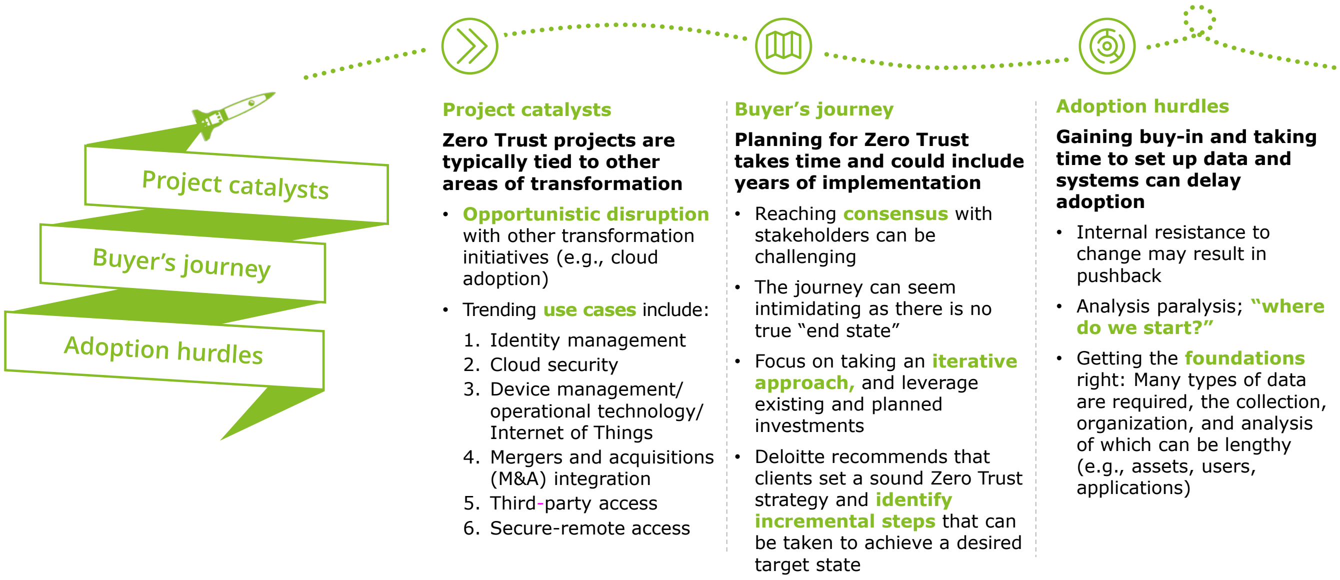
Adopting Zero Trust does not mean an organization has to rip out its existing infrastructure and replace it with a completely different set of technologies. Fortunately, the transformation to Zero Trust can be implemented in phases, such as starting with maturing your identity and access management capabilities with single sign-on (SSO) or leveraging network segmentation to minimize the impact of a malware infection or breach by containing the potential blast radius (see Figure 1).

To decide where to start, CFOs may find it useful to consider the following questions:

- **Do we have an identity crisis?** Zero Trust cannot be effective without strong and centralized identity and access management, implemented across all applications and data locations. At many companies, identity controls have grown fragmented, divided between on-premises directories and separate cloud repositories. Passwords may also be strewn in different directions, negatively affecting user experience. If that's

Figure 1. The Zero Trust Adoption Journey

Zero Trust adoption requires a mindset shift typically driven by broader transformation efforts; full implementation of Zero Trust can take years to accomplish.



Project catalysts

Zero Trust projects are typically tied to other areas of transformation

- **Opportunistic disruption** with other transformation initiatives (e.g., cloud adoption)
- Trending **use cases** include:
  1. Identity management
  2. Cloud security
  3. Device management/ operational technology/ Internet of Things
  4. Mergers and acquisitions (M&A) integration
  5. Third-party access
  6. Secure-remote access

Buyer's journey

Planning for Zero Trust takes time and could include years of implementation

- Reaching **consensus** with stakeholders can be challenging
- The journey can seem intimidating as there is no true "end state"
- Focus on taking an **iterative approach,** and leverage existing and planned investments
- Deloitte recommends that clients set a sound Zero Trust strategy and **identify incremental steps** that can be taken to achieve a desired target state

Adoption hurdles

Gaining buy-in and taking time to set up data and systems can delay adoption

- Internal resistance to change may result in pushback
- Analysis paralysis; **"where do we start?"**
- Getting the **foundations** right: Many types of data are required, the collection, organization, and analysis of which can be lengthy (e.g., assets, users, applications)

Source: "Zero Trust cybersecurity: Never trust, always verify," Dbriefs Governance, Risk, & Compliance series, July 2020

the case, it's worth remembering that cyber-attackers typically try to procure top-level credentials, piggybacking off compromised credentials to gain access throughout the enterprise environment.

- **Have we built the system with users in mind?** If there are sticky notes around every employee's computer, that's a leading—albeit informal—indicator that users have found the login system cumbersome. While Zero Trust means implementing continuous authentication and risk-based access policies, it shouldn't be so difficult that even those who use it struggle to gain entry. Companies implementing Zero Trust can also switch to a passwordless system, using multi-factor authentication or biometric verification to both strengthen their security posture as well as enhance the end user experience.
- **Are we using technology that can be easily integrated?** The market for Zero Trust technology is fragmented, with no single vendor offering the full range of tools, from cloud integration of apps, to single sign-on, to multi-factor authentication. But what companies don't want to end up doing is having to implement separate security systems for on-premises needs and cloud environments. The aim should be to have a harmonized set of security controls that supports integration across the technology ecosystem and facilitates automation and orchestration across both on-premise and cloud environments. Also consider leveraging or extending existing investments whenever possible in order to minimize financial impact and the associated learning curves for security, engineering, and operations teams.
- **Have we mapped out a strategy with key stakeholders?** Prioritize business needs over technology and adopt Zero Trust through relevant business drivers and areas of transformation, rather than focusing on technology implementation and adoption. In addition to aligning with business risks, it's important for those who plan to implement Zero Trust to spend time with stakeholders from a range of departments, including security, IT, application owners, end users, support functions, and others. Gaining consensus around the need for Zero Trust and understanding the down-stream effects on operational processes and end user experience are often overlooked keys to success.
- **What's our baseline?** Before anything is designed, it's crucial to understand the current environment, what and where are the "crown jewels" in your organization, what threats are most relevant within the context of the existing environment, and what "normal" user and network activity looks like. Once you understand the infrastructure and have documented it, it's possible to layer in additional Zero Trust-aligned controls by taking an iterative and incremental approach. Also, foundational cyber hygiene is crucial to realizing the full benefits of the Zero Trust model (e.g., IT asset management, data inventory/classification/governance, patch, and configuration management).
- **Are we committed to building a security-minded culture?** Zero Trust adoption often requires a cultural shift. Organizations should assess and address the potential impact to end users, operational teams and processes, business stakeholders, and relevant third parties in order to be successful in their journey toward Zero Trust.

The long run

Implementing Zero Trust is hardly a three-month sprint. Still, even in the midst of the COVID-19 pandemic, companies that had begun adopting the Zero Trust model clung to it as a priority. In a Deloitte poll[3] published in September 2020, 37.4% of those at organizations adopting Zero Trust said COVID-19 had accelerated their journeys, with 35.2% reporting that it had not slowed their efforts.

Like broader transformation efforts, the Zero Trust journey may also take years to fully optimize—and face similar impediments, such as resistance to change and analysis paralysis. For CFOs, that means starting with low-risk environments before attempting to implement additional Zero Trust-enabled controls around your crown jewels. As with many types of transformations, it's useful to chalk up quick wins. Those can include reducing costs by requiring that Zero Trust principles and security requirements be part of strategic IT and application transformation programs, such as cloud migrations, network transformations, virtualization/ serverless initiatives, and digital transformation initiatives.

Still, the path to Zero Trust may feel daunting, or, more than that, never-ending. But with every step, the business moves more out of reach of lurking cyber-attackers, ever eager to infiltrate their networks.

End notes

1. IBM Report: Cost of a Data Breach Hits Record High During Pandemic, PRNewswire, July 28, 2021.

2 CFO Signals, Q2 2021, CFO Program, Deloitte LLP.

3 Zero Trust cybersecurity: Never trust, always verify, September 2, 2020, Deloitte Development LLC.

Contacts

Andrew Rafla
Principal, Zero Trust offering leader
Deloitte & Touche LLP
arafla@deloitte.com

Henry Li
Advisory Specialist Leader
Risk & Financial Advisory
Deloitte & Touche LLP
henli@deloitte.com

About Deloitte's CFO Program
The CFO Program brings together a multidisciplinary team of Deloitte leaders and subject-matter specialists to help CFOs stay ahead in the face of growing challenges and demands. The program harnesses our organization's broad capabilities to deliver forward thinking and fresh insights for every stage of a CFO's career—helping CFOs manage the complexities of their roles, tackle their company's most compelling challenges, and adapt to strategic shifts in the market.

For more information about Deloitte's CFO program visit our website at:
www.deloitte.com/us/thecfoprogram.
Follow us @deloittecfo

Deloitte *CFO Insights* are developed with the guidance of Dr. Ajit Kambil, Global Research Director, CFO Program, Deloitte LLP; Lori Calabro, Senior Manager, CFO Education & Events, Deloitte LLP; and Josh Hyatt, Manager/Journalist, CFO Program, Deloitte LLP.

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

About Deloitte
Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (DTTL), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the "Deloitte" name in the United States and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see www.deloitte.com/about to learn more about our global network of member firms.