ENQUIZIT
A CDW COMPANY

Getting Over the "Zero Trust Hurdle"

4 Steps to Organizational Success

By Asim Iqbal

The term "Zero Trust" was coined in 2010 by security strategist John Kindervag. While working at Forrester Research, Kindervag envisioned a new approach to security where organizations assume that no one, and no device, is inherently "trustworthy." According to the Zero Trust philosophy, users must "prove" trustworthiness each time they access the network. Over the past decade, Kindervag has continued to refine the concept, helping organizations avoid common pitfalls, such as assuming that Zero Trust makes a system automatically "trusted," or that identity and multi-factor authentication (MFA) are enough to make a system secure.

In May 2021, the President of the United States issued an executive order laying out new cybersecurity guidelines for federal agencies—including implementing Zero Trust Architecture. The order was issued in response to "persistent and increasingly sophisticated malicious cyber campaigns that threaten… the American people's security and privacy." According to the order, "The Zero Trust Architecture security model assumes that a breach is inevitable or has likely already occurred, so it constantly limits access to only what is needed and looks for anomalous or malicious activity."

While the cybersecurity problem is serious enough that the U.S. government felt it necessary to mandate Zero Trust throughout its operations, moving to a Zero Trust framework is incredibly challenging. It requires a true transformation that can take years to implement. It's a paradox: while Zero Trust is a critical piece of security in an increasingly connected world, who can afford to shut down their operations to make their organization compliant all at once? The process is simultaneously critical and overwhelming.

Fear not—we've got you covered. In this e-book, we'll outline four steps you can take to move past paralysis and get your organization on the road to Zero Trust.

1. Get your people and culture ready

Today, most organizations realize they need Zero Trust, but implementation continues to be a challenge. While a staggering 97% of IT and security pros surveyed in a recent TechRepublic report said Zero Trust is a priority for their orgs, only 14% are in the early adoption stages, with another 17% just taking their initial steps. Why the disconnect? Digging deeper, the report revealed that 92% of respondents felt comfortable with the security of their current remote access infrastructure—even without Zero Trust—while 69% also felt that implementing Zero Trust would be an enormous undertaking.

The Value of Zero Trust

- Organizations with fully deployed Zero Trust experience a 43% savings on data breach costs.
- Orgs with partially deployed Zero Trust see a savings of at least $660,000 per breach.

**Source: IBM's 2021 Cost of a Data Breach Report*

Education, then, is a critical first step to implementation. Security teams will need to fully understand, and buy into, the reasons for undertaking such a big transition. Staff can also be reassured that the transition will occur slowly. As Kindervag notes, "Zero Trust is incremental. It is built out one protect surface at a time so that it is done in an iterative and non-disruptive manner."

Explain why you're moving to Zero Trust as an organization and that Zero Trust will be the standard for all new development—starting now.

2. Add Zero Trust to apps that are in development

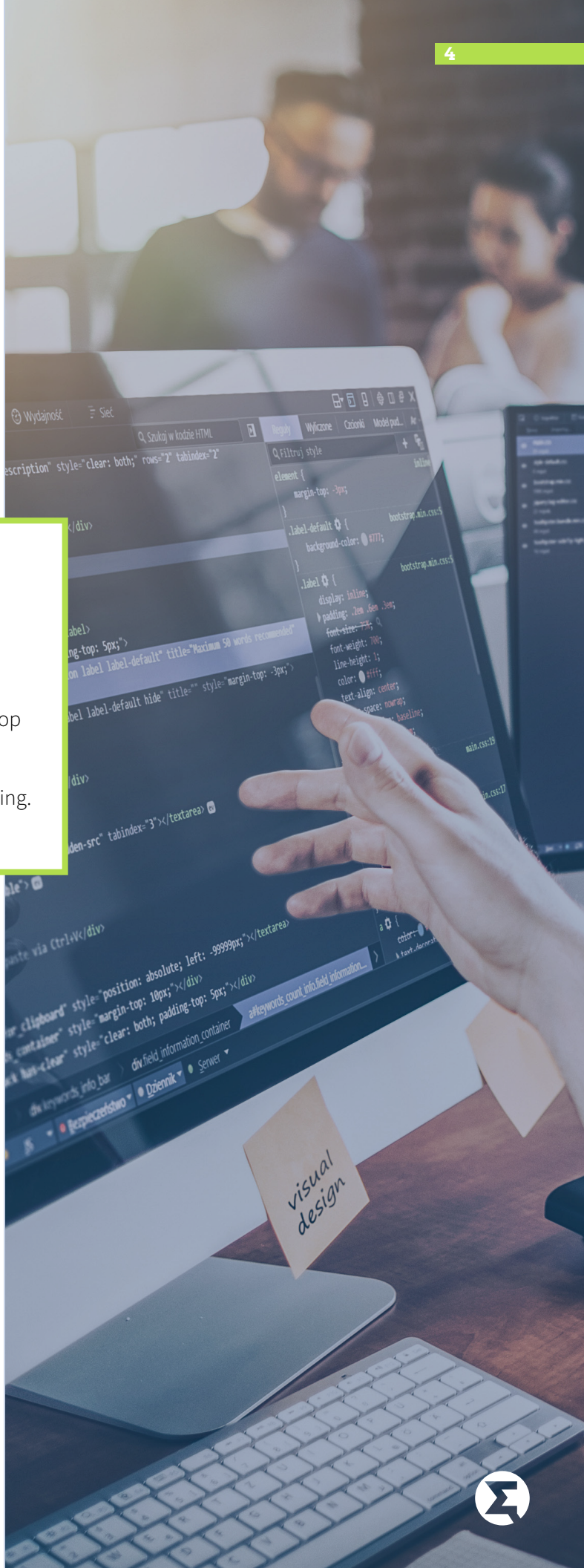
Trying to convert too many systems to Zero Trust at once is a recipe for failure. Instead, commit to injecting Zero Trust into any apps and projects currently in development—and do not allow a new project to kick off without adding Zero Trust. Starting this way will be less overwhelming and will help achieve buy-in organization-wide.

What's More Important Than Zero Trust? Almost Nothing

In many fast-paced organizations, it's common for everything to feel like a priority—but Zero Trust should be your organization's top focus. Remember, the idea of Zero Trust is to be proactive about your security, not reactive. Instead of putting out security fires, you're implementing a new system to prevent the fires from starting.

Similarly, Zero Trust must be added to all project guidelines for vendors bidding on new projects. If you don't write it into the guidelines, you might have to discard a substantial portion of the project later and start over. That's because it's nearly impossible to shift to Zero Trust mid-development. When it is possible, it's exceedingly expensive to do so—as is starting over.

As you evaluate vendors, remember that Zero Trust is a strategy, not a product. "There are products that work well in Zero Trust environments," says Kindervag, "but if a vendor comes in to sell you their 'Zero Trust' product, that's a pretty good indication that they don't understand the concept."



3. Evaluate your existing systems and make a priority list

Once you've finished adding Zero Trust to your newly developed apps, Kindervag advises working through your old systems, starting with the least sensitive protect surfaces first. This allows your team time to learn on less-critical projects, where any mistakes will be less disruptive. Over time, you can slowly work toward implementing Zero Trust for your more critical systems.

The Value of Zero Trust

Apps with low "downtime cost" and low visibility are good candidates to convert first.

- **Downtime cost:** If the app goes down, what is the cost—both in terms of dollars and reputation among customers and employees?
- **Visibility:** How "visible" is the app? If your payroll system goes down mid-month, for example, no one might notice, making it a low-visibility app. The opposite is true for a high-visibility website interface.

When prioritizing, ask the following questions:

- **How difficult is it to convert the app to Zero Trust?** Starting with easier apps is recommended unless there is a specific reason to do a harder app first (see criteria below).
- **What is the value of Zero Trust for this app?** To minimize the impact of any mistakes, look to start with apps with low "downtime cost" and low visibility.
- **Are there regulations related to the app?** If an app will be out of compliance without Zero Trust, that app will need to be prioritized.

Determining the answers to these questions will help you to decide the order in which to apply Zero Trust to your existing systems.

4. Choose the right partner to help you

While the phrase was coined in 2010, Zero Trust is still a new endeavor for many companies. In searching for a partner, look for one who has deep experience working with the varied components of Zero Trust. That vendor must be able to look holistically at your entire organization before diving in to deploy Zero Trust at the individual application level. And if your organization is a government agency, it's also essential to know whether they've done Zero Trust work at the federal and state level.

When considering a Zero Trust transformation partner, consider these questions:

- **What is their process?** The right vendor is not one that passively waits to take orders. Instead, look for a vendor who makes recommendations on how to solve key business problems and ensure customer needs are met—from issuing RFPs to purchasing the correct products and solutions.
- **How do they evaluate operations and networks?** The vendor should be able to audit your existing operational practices and ensure they are set up for Zero Trust. If you are not ready, the vendor should be able to create a plan for Zero Trust transformation.
- **How secure is the vendor?** Don't trust a vendor who is not practicing Zero Trust themselves. That means they practice continuous authentication, encryption, and no continued trust across their own operations. Any data moving from A to B must be encrypted, no matter how far it's traveling. Similarly, their authentication process should only permit access to an application for as long as needed.

Enquizit: Doing Zero Trust From the Start

Enquizit has been using AWS Cloud tools to help organizations achieve Zero Trust for more than a decade, before the term was even coined. As a result, our team is always thinking not only about how Zero Trust will touch an entire organization, but also about how individual applications, products, and systems will be affected by Zero Trust transformation.

Using tools like the AWS Cloud Adoption Framework (CAF), Migration Evaluator, and Migration Acceleration Program (MAP), our team helps plan, evaluate, and transition your data and applications to the cloud while applying a Zero Trust framework to increase your organization's overall security—and stay compliant.

Want to know more about how Enquizit can assist with your organization's Zero Trust transition? Visit www.enquizit.com to learn more today.