# Closing The Zero Trust Gap

## A Quick Read into The Future of Cybersecurity

On January 26, 2022, the White House announced the adoption of a federal Zero Trust strategy.

According to CISA Director Jen Easterly, “As our adversaries continue to pursue innovative ways to breach our infrastructure, we must continue to fundamentally transform our approach to federal cybersecurity.” “Zero trust is a key element of this effort to modernize and strengthen our defenses. CISA will continue to provide technical support and operational expertise to agencies as we strive to achieve a shared baseline of maturity.”

Yet, according to the Microsoft 2021 Zero Trust Adoption Report, only 35 percent of organizations claim to have fully implemented their Zero Trust strategy.

Organizations across markets and industries are choosing for a Zero Trust strategy, which urges us to "never trust, always verify" as security risks become more common and sinister. Organizations that want to improve their entire security posture, end-user experience, and productivity, as well as simplify security procedures for staff and cut costs, should prioritize the Zero Trust strategy.

## Why Zero Trust?

Zero Trust is not a new technology or software. Zero Trust is a security model and an iterative process that seeks to shift the way we approach cybersecurity. Having all computers, servers, and devices in an organization on the same network and trusting each other was the old way of thinking about networks and IT architecture. This design flaw can be exploited by attackers who find their way into the organization by seeking the tiniest door or the slightest vulnerability. Once these intruders are in, they can go anywhere by scaling privileges since the network is coded to trust anything that exists inside of it.

With Zero Trust, we avoid this by rethinking networks and embracing a new philosophy: never trust, always verify–as many times as needed.

## The real costs of not implementing a Zero Trust approach

According to the latest Verizon Data Breach Investigations Report (2021) a single data breach can go from a low $826 to an upper amount of $653,587. But it doesn't stop there. Quoting the data breach findings: "CDB (Computer Data Breach) ranges were even wider with 95% falling between $148 and $1.6 million, and a median loss of $30,000. Finally, for ransomware the median amount lost was $11,150, and the range of losses in 95% of the cases fell between $70 and $1.2 million."

Not enough? Consider the global average cost of a data breach is now $4.24M, and the top three initial attack vectors are compromised credentials (20%), phishing (17%), and cloud misconfiguration (15%). According to IBM and Ponemon Institute.

These numbers are scary alone. That's why more than 90% of companies recognize the value of Zero Trust, (Microsoft, 2021) even when less than a half of them (40%) have assigned a budget for Zero Trust adoption.

## Zero Trust – Three Takeaways

- Organizations that want to safeguard their data and their users must adopt a Zero Trust approach.
- Leadership alignment on how to approach Zero Trust is the biggest obstacle to driving Zero Trust agendas.
- Zero Trust architecture requires time, resources and a plan for successful integration

### Did You Know?

Web Applications receive the most attacks, with a main attack vector of 89% completely overshadowing other hacking vectors. (Verizon Data Breach Report, 2021)

## Picking a starting point

A consistent framework for Zero Trust and continuous visibility is a good place to start. Nonetheless, it does not address where and how to begin implementing Zero Trust in your organization. The answer will be unique to each organization; there is no one-size-fits-all solution for Zero Trust.

In our latest QuickLaunch action centered guide to Zero Trust, we suggest four crucial steps to help organizations implement a Zero Trust architecture:

1. First Phase: Defining Zero Trust for the User and adopting the always verify mantra.
2. Second Phase: Approaching Device Visibility and Trust

3. Third Phase: Using Adaptive Design principles and Policies
4. Final Phase: Merging IT changes towards the Workforce

Implementing Zero Trust is a technical challenge, more than that is also a design challenge that requires a solid integration the end-user and each part of the organization. We know Zero Trust is here to stay and we are ready to help others adopt it. If you are interested in requesting our latest QL guide to Zero Trust, contact us. Or request a demo here and set your first line of defense starting today.

If you are interested in requesting our latest QL guide to Zero Trust, contact us. Or request a demo here and set your first line of defense starting today.