xage

Securing Critical Infrastructure: The Journey to Zero Trust

July 2022 • Wakefield Research

Introduction

Paving a Better Way Forward to Secure Operations

Our critical infrastructure is at an inflection point. Hackers and nation-state actors have targeted the systems that underpin our everyday lives. Predominant cybersecurity practices aren't able to adequately protect operations from these threats. We need a new way forward.

The growing threat landscape has elevated cybersecurity to a top priority for critical infrastructure operators as well as the federal government. The White House, the Transportation Security Administration (TSA) and the Cybersecurity and Infrastructure Security Agency (CISA) have each released requirements and guidelines that push critical industries towards zero trust—the security strategy proven to block cyberattacks outright or significantly mitigate their effects.

In contrast to perimeter-based security models, zero trust is a proactive, identity-based approach that treats the identity of each machine, application, user, and data stream as its own independent "perimeter," allowing for granular access policy enforcement and preventing breaches before they happen. Contrary to popular belief, zero trust can be delivered as an overlay on top of the existing systems—making it possible to implement seamlessly in complex operational technology (OT) environments.

To better understand where OT cybersecurity leaders stand in their journey towards zero trust, Xage partnered with Wakefield Research to survey 250 cybersecurity senior leaders across critical infrastructure organizations, including utilities, oil & gas pipelines, transportation, aerospace, retail supply chain, and warehousing & distribution.

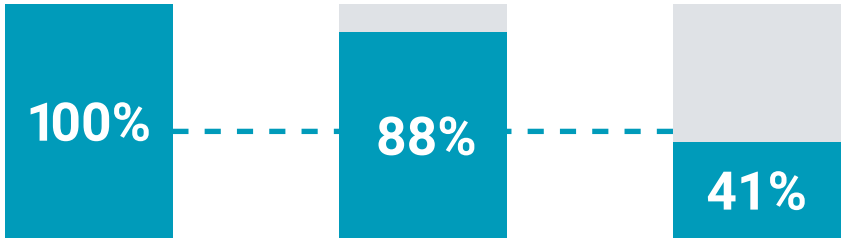
The findings make two things clear. First, cybersecurity leaders agree that zero trust adoption is inevitable. Second, while the majority of the industry understands the effectiveness of zero trust, foreseeing its future and knowing how to integrate it are two very different things. Fortunately, the data reveals where lingering knowledge gaps lie. Overcoming these hurdles and misconceptions will help expedite zero adoption and keep our nation's—and world's—critical infrastructure safe from cyberattacks.

Thanks for reading. If you have any questions about the findings, please don't hesitate to reach out.

Duncan Greatwood
CEO, Xage

Industrial Operations are Rapidly Adopting Zero Trust, But Some Risk Falling Behind

The industrial world is taking action. Cybersecurity leaders recognize the potential of zero trust, and an overwhelming majority are in the process of adopting a zero trust strategy.



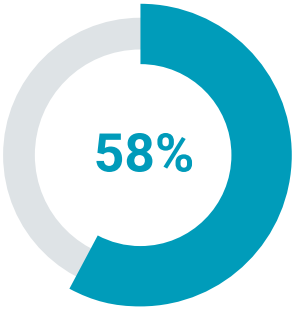
of security leaders have plans to adopt zero trust

of cybersecurity leaders have taken steps to adopt a zero trust security posture

are in early stages of implementation

There are a variety of strategies operators can employ to implement zero trust for OT. Some require organizations to rip and replace legacy technologies, which is costly and disruptive and can cause organizational friction. But this isn't the only option. Some zero trust strategies don't require any upgrades to existing technologies.

What's driving this progress? For a slight majority of respondents, an age-old misconception is wearing off: the notion that implementing zero trust requires a full equipment overhaul. But this leaves nearly half susceptible to a slower timeline and greater disruption.



of the respondents indicated that zero trust implementation will not substantially impact existing OT infrastructure. On the flip side, that means 42% see a rip and replace strategy as their only option.

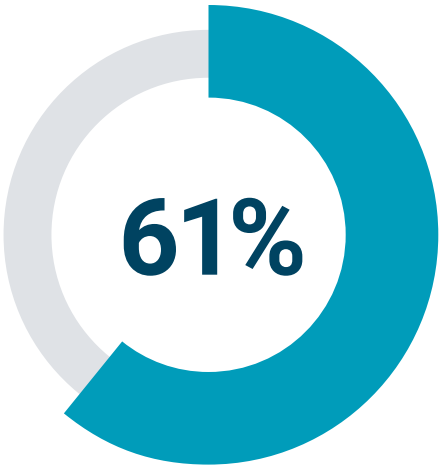
WHAT THIS MEANS

If the remaining 42% realize that there's another way, cybersecurity transformations could accelerate.

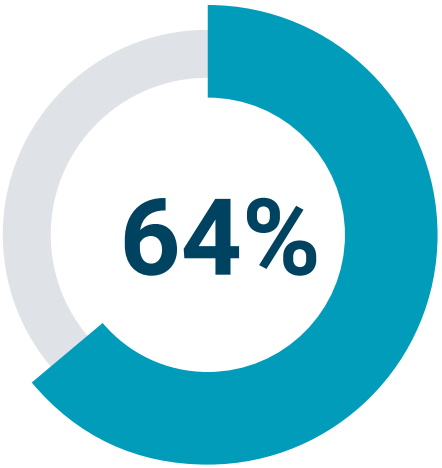
The Big Shift: From Reactive to Proactive Cybersecurity

The move towards zero trust marks a fundamental shift in the way operators approach cybersecurity. The industry is evolving security strategies from purely reactive, to proactive.

Until recently, new security solutions serving real world operations had been primarily focused on visibility and threat detection. But those tools can't prevent hacks from happening—only monitor for and raise the alert once an attack is underway. Alternatively, implementing a zero trust architecture creates an environment where hacking attempts are blocked outright, or contained and mitigated.



of respondents agreed that reactive strategies for OT are not enough to prevent breaches



indicated that they've already moved to a proactive security approach to block and contain attacks

WHAT THIS MEANS

As more critical operations adopt zero trust, we'll start to see the number of cyber compromises of critical infrastructure decrease by orders of magnitude.

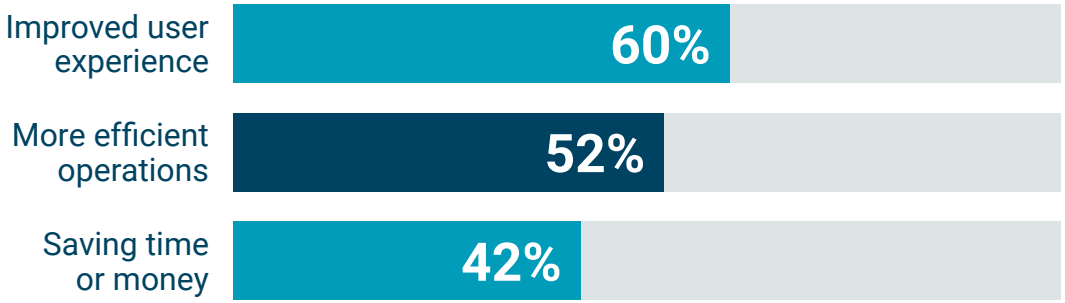
The Benefits of Zero Trust Extend Beyond Security

Those who have started implementing zero trust strategies are reaping benefits that extend beyond protection from cyberattacks.

By adopting a zero trust architecture, operators are expediting digital transformation efforts. When an operator assigns every asset or data stream an identity that can be managed centrally, they're also enabling remote access, efficient data sharing, and convenient collaboration with partners.

agree that adopting zero trust accelerates digital transformation

Top Cited Zero Trust Benefits



WHAT THIS MEANS

The industry-wide push to adopt zero trust will also help modernize the organizations that impact our daily lives.

Zero Trust is Here to Stay, Despite Implementation Challenges

While many organizations working to adopt zero trust are still facing significant roadblocks, the industry is largely in agreement: zero trust is happening, and happening now.

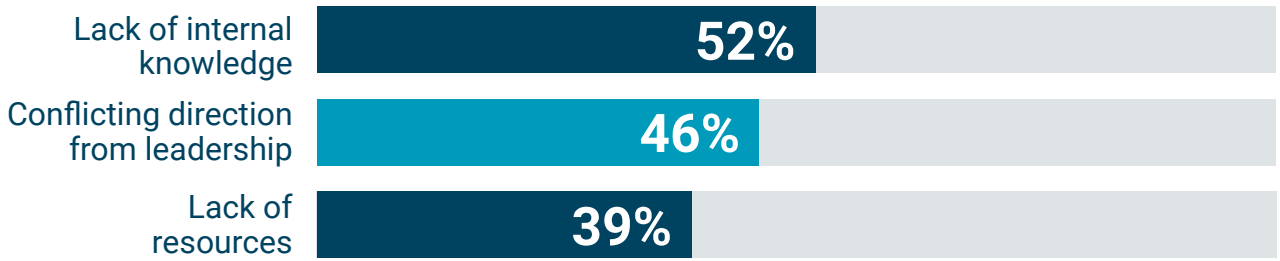
93%

believe that zero trust adoption is inevitable across the industry

WHAT THIS MEANS

Industry buy-in is there, but the nuances of zero trust principles, and the process of applying them in OT environments, remain a work in progress.

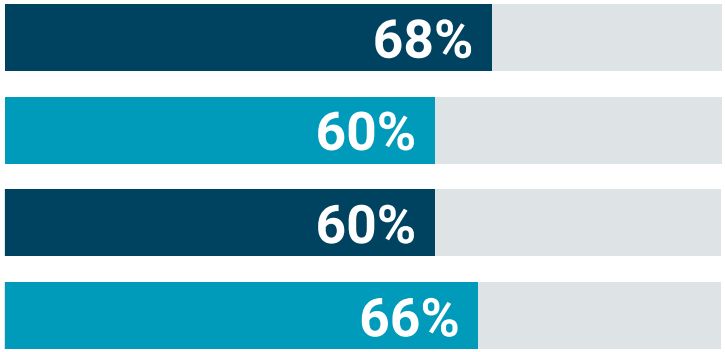
Challenges Slowing Down Implementations



The Road to Zero Trust: Strategies for Expediting Adoption

Nearly half of all respondents agree: implementing zero trust is a years-long process. Fortunately, there are several tactics that have proven helpful for getting buy-in and avoiding unnecessary delays.

Overcoming Hurdles



46%

of the respondents noted that it will take more than 3 years to complete their zero trust objectives for OT.

WHAT THIS MEANS

It's important to pursue zero trust strategies that minimize OT impact, that bring OT and security teams together, that center security management around identity and access control, and that can be executed in a reasonable timeframe.

Methodology

The Xage survey was conducted by Wakefield Research (wakefieldresearch.com) among 250 US Cybersecurity Professionals, with a minimum seniority of Director, working in any of the following industries: Energy, Aerospace/Space, Rail, Port Operations, Transportation, Pipeline operators, Utilities, Retail Supply Chain & Warehousing/Distribution, between May 20th and May 31st, 2022, using an email invitation and an online survey.

Results of any sample are subject to sampling variation. The magnitude of the variation is measurable and is affected by the number of interviews and the level of the percentages expressing the results. For the interviews conducted in this particular study, the chances are 95 in 100 that a survey result does not vary, plus or minus, by more than 6.2 percentage points from the result that would be obtained if interviews had been conducted with all persons in the universe represented by the sample.

xage

About Xage Security

Xage is the first and only zero trust real-world security company. Xage simplifies the way enterprises secure, manage, and transform digital operations across OT, IT, and cloud.

The patented Xage Fabric seamlessly overlays every element of an operation to impose granular control over all digital interactions. It also prevents cyberattacks at the source, isolating threats so that essential operations remain undisturbed.

Xage offers a variety of solutions, all powered by the Fabric, designed specifically for real-world operations. These solutions include Identity & Access Management (IAM), Zero Trust Remote Access (ZTRA), Dynamic Data Security, and Multi-layer Multi-Factor Authentication (MFA).

Xage enables security and operations teams to come together to accelerate the zero trust journey with optimal total cost of ownership and minimal impact to operations while enabling business benefits such as improved employee productivity.

To learn more about how the Xage Fabric can secure and transform your organization, visit Xage.com

xage