FALL 2021

ZERO TRUST
DRIVERS AND DECISION POINTS

Insights from listening to
1,283 InfoSec leaders on Zero Trust

COLORTOKENS

Introduction by Dr. Chase Cunningham

Interest in Zero Trust has soared since the ongoing COVID-19 pandemic caused us all to rethink our approach to cybersecurity, remote work, and cloud-based business. Around the globe, companies were forced to adapt almost overnight to a new set of security and business requirements—and that meant abandoning the outdated paradigm of perimeter-based security.

Zero Trust has become the gold standard for security teams in meeting these new requirements. But implementing Zero Trust introduces new imperatives and new hinderances. It's also apparent that different organizations have different drivers for adopting Zero Trust, and that their strategic approaches vary based on their business priorities.

This study was intended to discover and detail the issues that typically plague the decision-makers and technologists who are actively engaged in enabling Zero Trust for their organizations. In July 2021, we undertook a research initiative independent of any vendor-sponsored collection to get an unbiased, nonpartisan understanding of the dynamics at play in this market.

In simple terms, we wanted to understand several key points:

- Do organizations understand the importance of Zero Trust?
- Do companies plan to implement Zero Trust? If so, when?
- What motivates organizations to implement Zero Trust?
- What challenges do companies face in adopting Zero Trust?

Our survey of 1,283 InfoSec leaders and Zero Trust practitioners found that respondents are concerned about how to begin their Zero Trust journeys. They are motivated by a variety of factors, from worries about increasingly sophisticated cyberattacks to a desire to reduce false positives and lighten the load on security teams. As you might expect, certain best practices around enabling Zero Trust are almost universally agreed upon, while others are points of hot contention between Zero Trust practitioners.

There's no one right way to begin a Zero Trust journey, but people actively working on Zero Trust nevertheless have clear drivers for high-value Zero Trust projects that should be undertaken immediately, and others that can wait while an organization evolves.

Zero Trust, of course, is not a product or a specific technology. It's a strategic approach to intelligently aligning selected technology to solve the security problems inherent to most digital systems. It's clear from our study that most organizations understand that, but there are some intriguing insights to be found in how organizations promote Zero Trust adoption and the specific steps they take to implement Zero Trust.

Read on for a detailed analysis of the survey findings, a discussion of the drivers and decision points that motivate organizations to embrace Zero Trust, and strategies to make your own Zero Trust implementation successful.

Chase Cunningham, PhD is a retired US Navy Chief Cryptologist and a preeminent expert on cybersecurity. He has deep technical expertise and extensive hands-on experience in cyberforensics, analytics, and offensive and defensive cyberoperations. He has worked with the NSA, CIA, FBI and other government agencies, as well as Fortune 500 companies looking to improve their security postures.

REACHING CONSENSUS ON ZERO TRUST

The survey results were very clear: Companies understand the importance of implementing Zero Trust security—sooner rather than later.

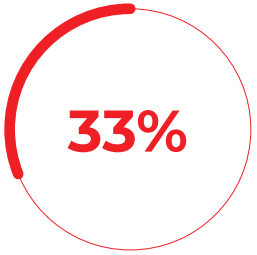
Zero Trust is necessary for thwarting modern cyberattacks

The vast majority of companies appreciate that moving to a Zero Trust security architecture is not just important but necessary: **93% of respondents say their organization sees Zero Trust as a necessity.**

Companies have plenty of good reasons for implementing Zero Trust, but for most respondents, the bottom line is that Zero Trust is a proactive security approach capable of defending against increasingly sophisticated (and expensive) attacks that can come from outside or inside your network.

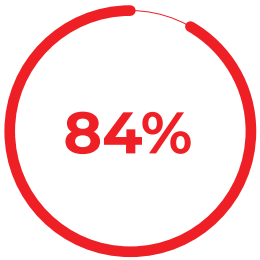
When asked their top reason for implementing or considering implementing Zero Trust:

More than 50% of respondents say Zero Trust is a more proactive approach than conventional, perimeter-based solutions



About a third say Zero Trust is the only way to fend off sophisticated attacks

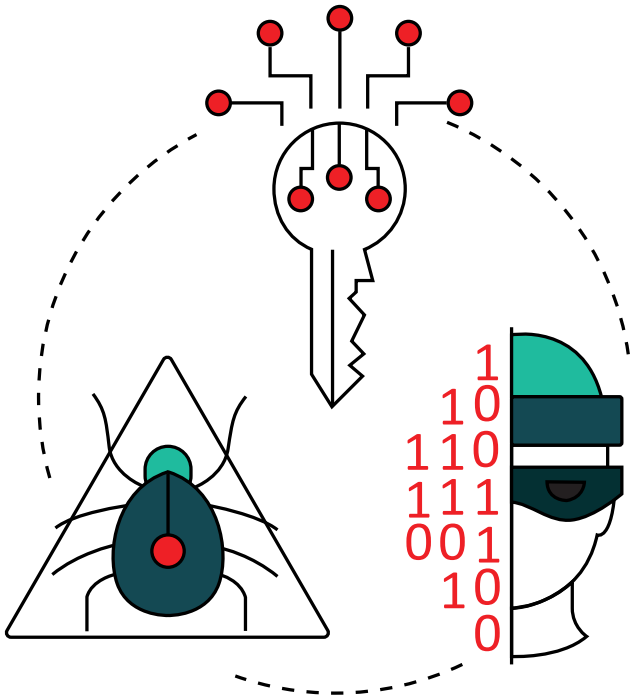
A majority of companies have faith in Zero Trust security to thwart attacks by preventing breaches and limiting lateral movement once a part of the network has been compromised. In other words, companies know that a Zero Trust approach works.



The survey found that 84% of respondents agree that implementing Zero Trust will prevent attacks or limit their success.

Zero Trust implementation can't wait

For most companies, Zero Trust is not a project for "sometime in the future"; it's a pressing business consideration that simply can't wait. **Nearly 40% of survey respondents are planning to enable Zero Trust in three months or less, while 80% say they plan to enable Zero Trust within a year.**
In large part, then, the efficacy and urgency of Zero Trust are not up for debate.



We asked Dr. Cunningham what organizations should take away from these findings, and he highlighted three lessons: Cloud adoption isn't as difficult as it's been perceived. From this survey, it's evident that

1. cloud migration isn't a major hindrance to Zero Trust adoption. Rather, what impedes progress is legacy technology and the ties a business has to those revenue-generating but outdated assets.

2. People often ask, "How soon can we get to Zero Trust?" The answer I usually give is, "As soon as you align to that mission." This survey tells us that most organizations are moving to a more focused Zero Trust approach in the next year, which is significant.

3. Buzzwords can hurt. The fact that 12% of survey respondents cited excessive marketing of Zero Trust solutions as an impediment to actual Zero Trust implementation suggests that marketing every security practice or solution as Zero Trust doesn't help overall adoption rates.

OBSTACLES TO ZERO TRUST IMPLEMENTATION

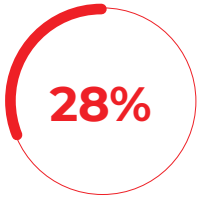
Survey respondents cited a number of reasons why their Zero Trust implementation might be delayed, including tight budgets, business conflicts, and outdated or absent technology.

Budget restrictions and business conflicts

Budget restrictions and business conflicts are the biggest blockers to a successful, timely Zero Trust implementation.

say Zero Trust implementation conflicts with other IT and business frameworks

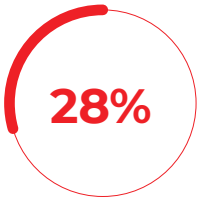
lack the technology needed to enable Zero Trust



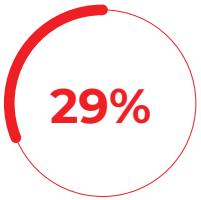
cite budget constraints as their biggest blocker

Legacy technology

Legacy technology is a major drag on enabling Zero Trust. Many organizations also struggle with the inefficiency of using multiple tools to manage their security infrastructure, rather than a single platform with a unified view.



say legacy technology that doesn't keep up with current business requirements is their biggest hinderance

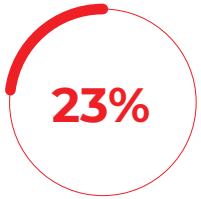


report that their biggest challenge is not having one unified tool: whether to view all cloud and data center resources (13%) or to manage user and application access (16%)

Technical challenges

Companies face a variety of technical challenges when it comes to Zero Trust, from managing policies to dealing with frequent changes to the environment. When asked the most difficult part of Zero Trust to manage from a technical perspective:

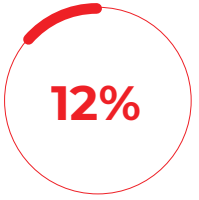
reported that policies are the most difficult to manage



cited frequent changes to the environment

said cloud migration or hybrid cloud systems

cited user requirements



said visibility and analytics

Identity followed by secure access and network security are priorities

To unlock the benefits of Zero Trust security, **42% of respondents** said their company infrastructure must first address identity and access management.

Network security was the next priority for **22% of respondents.**

The survey results align with both NIST and Gartner's recommendations for Zero Trust.

In NIST's Special Publication 800-207 on Zero Trust Architecture, enterprises can achieve Zero Trust through these key initiatives:

- Enhanced Identity Governance
- Micro-Segmentation
- Software-Defined Perimeters

Gartner recently published a report titled "What Are Practical Projects for Implementing Zero Trust?". In it, Gartner also recommends that organizations focus on two key initiatives when it comes to Zero Trust: workload-to-workload segmentation (identity-based segmentation) and user-to-application segmentation (ZTNA).

Dr. Cunningham's takeaways: What should organizations learn from these findings?

1. The fact that IAM and identity are first-priority problems for most organizations indicates the importance of access management. The key lesson is that for any Zero Trust project to be successful, identity must be a consideration from day one.

2. Once an organization has laid the foundation of identity governance, it needs to shift its focus to identity-based access control and identity-based segmentation. A Zero Trust-based access control solution should replace traditional, broad-based remote access solutions. It is crucial to micro-segment the network on which critical workloads are running to limit their breach exposure.

3. Money talks. In business, the ultimate driver of any decision is usually money. If your organization can't allocate the necessary budget to Zero Trust efforts, nothing will happen.

MAKING YOUR ZERO TRUST IMPLEMENTATION SUCCESSFUL

After reading these results, you're probably more convinced than ever that your organization should upgrade to a security architecture built on the "never trust, always verify" logic of Zero Trust. But while the importance and efficacy of a Zero Trust approach is widely accepted, the path to Zero Trust is not always clear. Fortunately, you can take strategic steps to help ensure a smooth implementation.

1 Set expectations

Zero Trust is neither a quick fix nor something easy and straightforward to implement in every case. Today's dynamic application environments, cloud-enabled remote work, and BYOD (bring your own device) policies can make Zero Trust implementation complicated. At the same time, the need for Zero Trust security remains urgent, and the complexity of implementation can increase over time the longer you wait.

2 Acknowledge the hype

The Zero Trust concept is sometimes dismissed as marketing jargon. In fact, 78% of survey respondents felt that Zero Trust vendors fail to grasp Zero Trust "strategically" or else "market everything as a solution" by focusing on solutions selling rather than commercial capabilities. To combat this attitude, Zero Trust advocates must educate stakeholders about the proven benefits of a Zero Trust security approach, armed with specific proof points that address stakeholder concerns head-on.

3 Start small and scale

A good way to start your Zero Trust journey is incrementally: tackle specific problems (like secure remote access for contractors and third parties) that roll up to broader strategic goals (like the scalability and reliability of a fully cloud-based network). Herald your successful outcomes to get organization-wide buy-in for Zero Trust adoption.

4 Learn from your mistakes

If we need proof that conventional security methods are no longer up to the task, we have plenty of examples to look to. But past failures can yield future successes if we learn from what went wrong. Use the painful memory of past breaches or the anxiety-inducing headlines about yet another high-profile ransomware attack to guide your organization's current thinking about cybersecurity. Ask yourself critical questions: What went wrong in this case? How could it have been avoided? What steps can we take to prevent a similar breach at our company?

5 Find a partner

Organizations want a partner to help them succeed in their journey to Zero Trust: 70% of respondents say their organization could implement Zero Trust faster with the help of a partner. Entrusting your security to an expert third party frees up your teams to focus on what they do best: delivering value to your customers. A Zero Trust security provider can shoulder the complexity of implementation to ensure a smooth deployment with minimal disruption to your business processes.

Dr. Cunningham's main takeaway: You'll need help implementing Zero Trust—and that's OK. Chances are, Zero Trust implementation is a larger project than you realize, and there are lots of moving parts: rolling out Zero Trust can touch every aspect of your business. If you enlist a partner who's tied to the success of your Zero Trust efforts, you're more likely to be successful.

To realize the benefits of Zero Trust, companies need a cost-effective solution that won't disrupt business operations, especially customer service.

They need a solution that can be deployed alongside their existing security tools, so they can implement their new Zero Trust framework seamlessly and start realizing value in minutes

CONCLUSION BY TONY SCOTT: NOW IS THE TIME FOR ZERO TRUST

Tony Scott was the third federal CIO (2015-2018) in United States history. One of the world's foremost security and IT experts, Tony has served as CIO at VMware, CIO at Microsoft Corporation, CIO at The Walt Disney Company, and CTO at General Motors.

For too long, companies and governments have relied on outdated cybersecurity models rather than investing in the systemic overhauls necessary to protect businesses in today's increasingly treacherous landscape. As high-profile attacks like the Colonial Pipeline ransomware attack and the SolarWinds breach make headlines, however, more organizations are realizing that they need a proactive security approach capable of defeating isolated actors, sophisticated nation-states, and ransomware-as-a-service providers.

Today's supply chains have porous perimeters packed with vulnerabilities intruders can use not only to wreak havoc on individual companies and end-users, but also to create national panic by disrupting critical infrastructure like energy and healthcare.

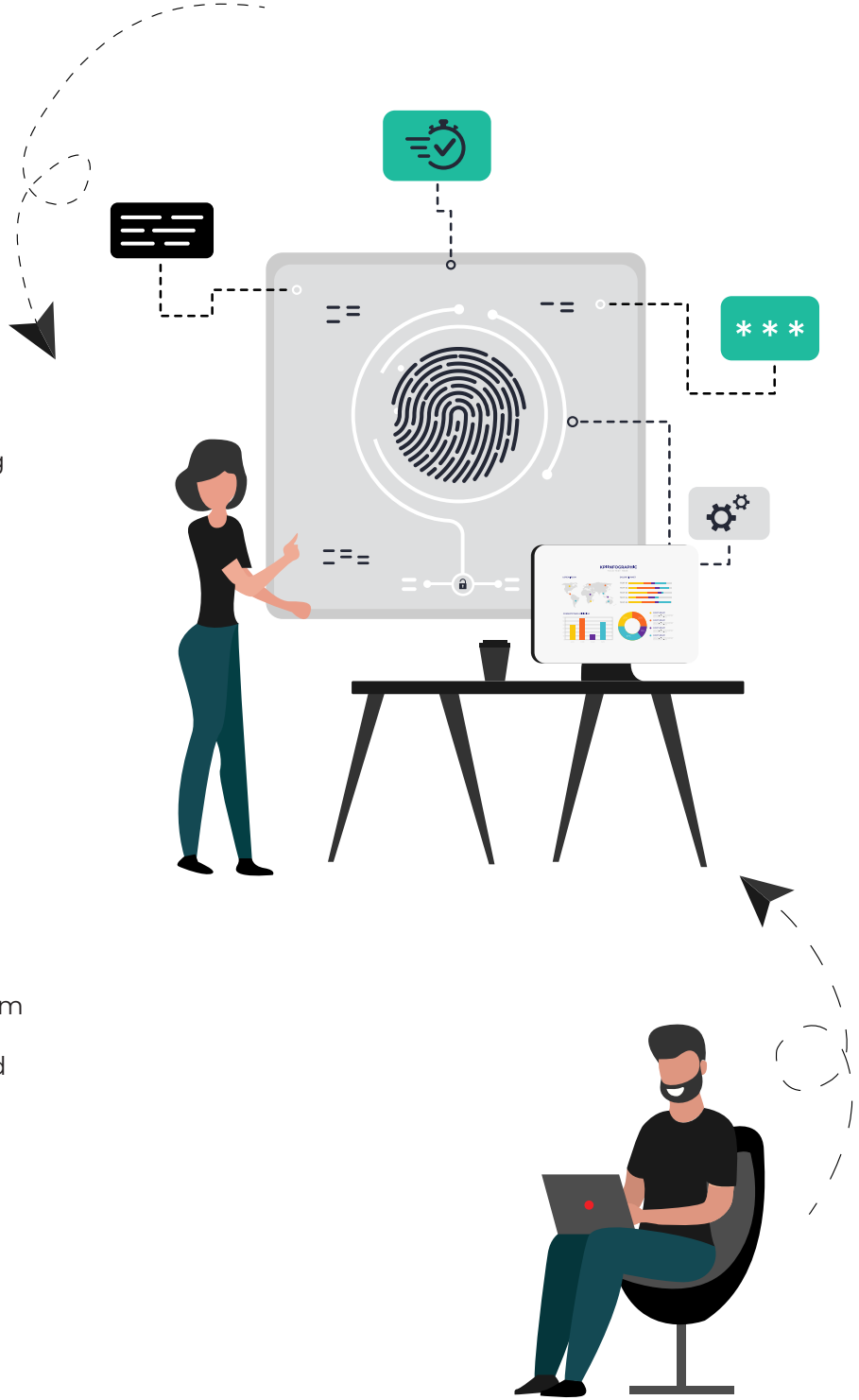
Supply chain attacks aren't just becoming more frequent; they're also getting more expensive. These attacks cost money in the form of business disruption, customer churn, regulatory penalties, brand erosion, and other setbacks. And they will continue as long as they're possible and profitable.

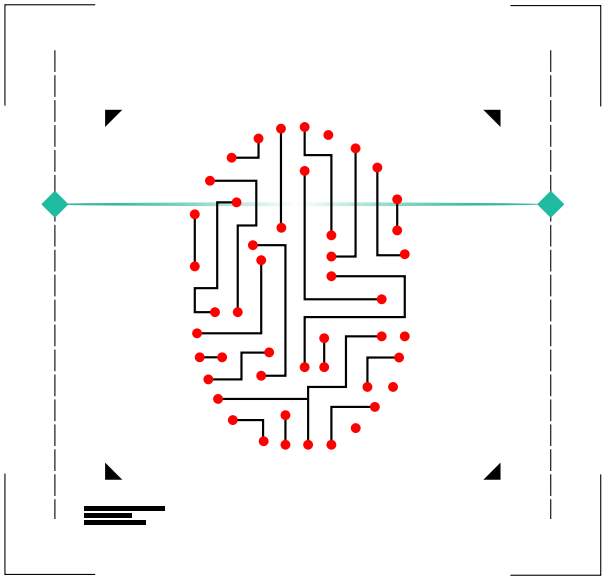
In response to these developments, President Biden signed an **Executive Order on Improving the Nation's Cybersecurity** in May 2021, urging government agencies and businesses to implement Zero Trust. The EO identified network segmentation as a crucial first step in implementation, echoing ColorTokens' belief that micro-segmentation is an integral part of your Zero Trust implementation. The expansive (EO) is a long-awaited step toward securing federal networks, improving information-sharing practices between public- and private-sector entities, and bolstering the nation's ability to detect and respond to incidents when they occur.

With this order, the federal government is wholeheartedly endorsing the concept of Zero Trust security. In fact, the order is explicitly intended to use the purchasing power of the federal government to encourage developers to build Zero Trust-based security into all new software, from ideation all the way through to implementation.

What does this mean? If you're creating software or supply chains you want any office of the US federal government to use, you need Zero Trust baked into your solutions.
For the many organizations that have hesitated to make Zero Trust a line-item priority, the White House's order certainly turns up the pressure. But implementing Zero Trust isn't guaranteed to be confusing, time-consuming, or expensive, and it doesn't have to throw your core business operations into disarray.

Partnering with an expert in Zero Trust implementation is a great way to expedite your journey to Zero Trust, strengthen your security posture, and maximize the ROI of your cybersecurity solutions. Our infrastructure-agnostic, cloud-delivered Xtended ZeroTrust™ Platform secures applications, endpoints, and workloads across hybrid, cloud, and multi-cloud environments. It's the industry's first fully integrated Zero Trust platform, to empower you to implement Zero Trust faster and without disruption.





COLORTOKENS

TAKE THE NEXT STEP ON YOUR ZERO TRUST JOURNEY WITH COLORTOKENS

Zero Trust security is a critical business enabler for our increasingly cloud-based, BYOD future. ColorTokens offers SaaS-delivered Zero Trust security to protect your entire network, from endpoint to cloud. We've built the industry's first fully integrated Zero Trust platform, to empower you to implement Zero Trust faster and without disruption. We also provide progressive Zero Trust-as-a-service to help companies plan, implement, and maintain a proactive security posture leveraging Zero Trust principles.

To learn more about our award-winning solutions, please visit **colortokens.com** or email us at **contactus@colortokens.com**.

Request a Demo