illumio

RESEARCH REPORT

Zero in on Zero Trust

How organizations consider Zero Trust in 2020

It's OK to trust Zero Trust

You have undoubtedly heard a lot about Zero Trust over the past year – online, at events, and from vendors. It has been mentioned frequently, but let's remember why that is.

The chief concern of security teams is keeping threats and attacks out of organizations. This is why we make significant investments in security controls to protect important vectors like the network and data center, email, endpoint, data, web, and the cloud.

This defense-in-depth approach is essential to detect and block threats but must be bolstered with Zero Trust capabilities. Why?

Because attacks and breaches continue to occur.

This is the simple reason we have heard so much about Zero Trust recently.

Even if you don't use the term Zero Trust, it is synonymous with concepts that we all place credence in to contain threats: least privilege, allow lists, or default deny.

These approaches make it harder for attackers to access systems and for threats that gain a foothold to move laterally.

Since Zero Trust (or least privilege) is a global best practice to contain threats, we wanted to get a sense for how organizations view their journey and progress towards Zero Trust. With this perspective, the rest of us can benchmark our efforts against peers.

Illumio teamed up with Virtual Intelligence Briefing (ViB), an interactive online community focused on emerging through rapid growth stage technologies. ViB's community is comprised of more than 1.2M IT practitioners and decision-makers who share their opinions by engaging in sophisticated surveys across IT domains including information security.

This report sums up our findings into the progress of organizational Zero Trust efforts.

A quick summary

Roughly half of the respondents consider Zero Trust to be very important to their enterprise security posture.

Concerns related to breached, reused, or weak passwords are prioritized, with organizations investing in identity-oriented tools.

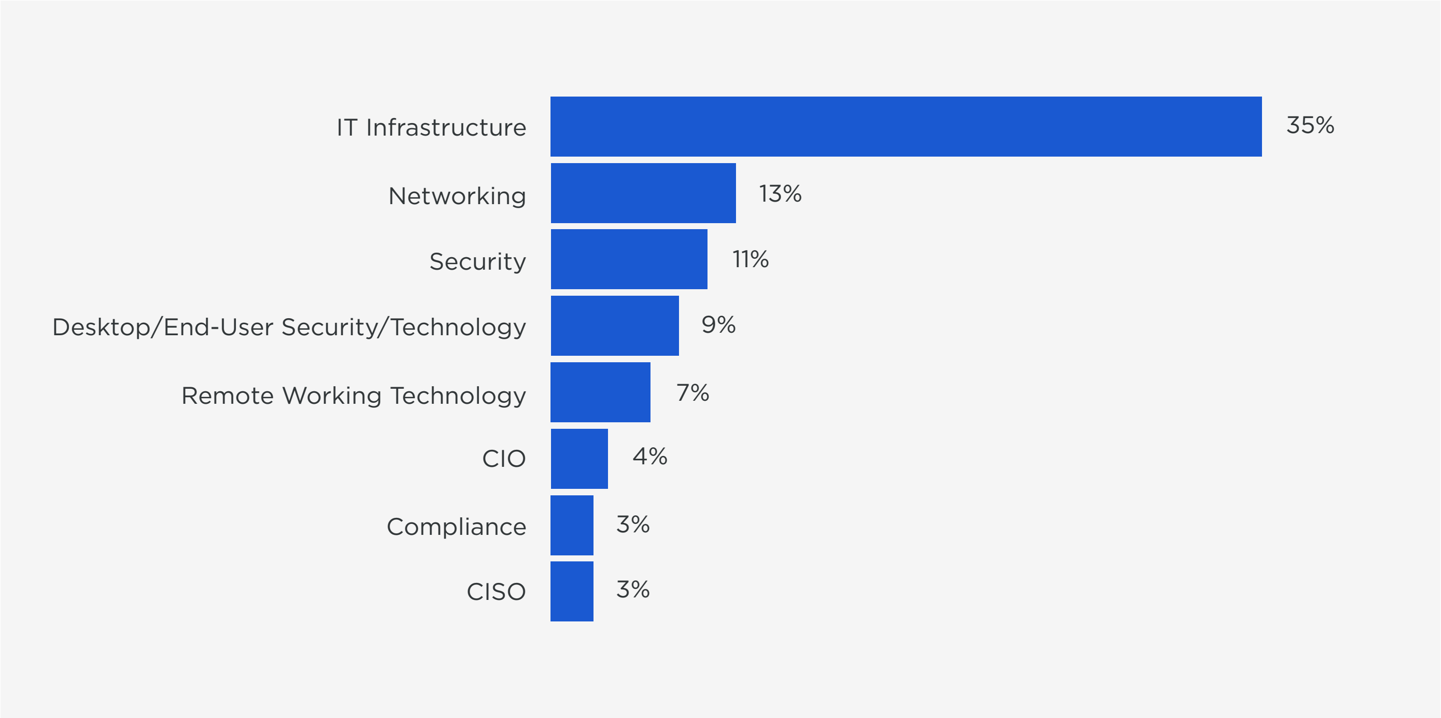
While threats and technologies evolve, barriers to deployment don't, with budgets and team sizes both cited as barriers.

Deploying Zero Trust, like with many security initiatives, is easier said than done, with many respondents still in the planning phase.

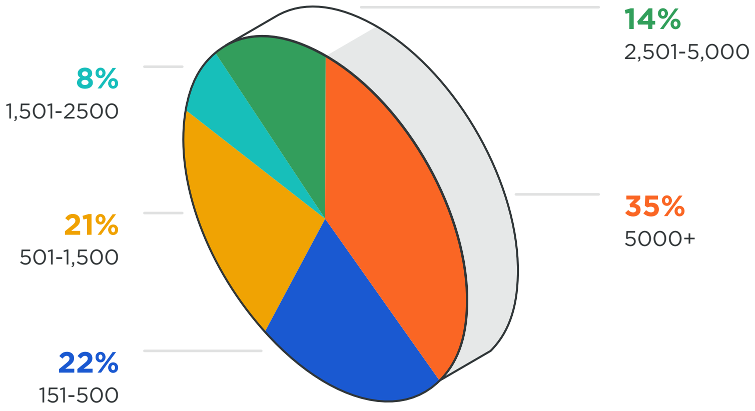
Who did we talk to?

We spoke to 461 IT and security professionals from a cross-section of mid- to large-sized companies, with 57% from companies with over 1,500 employees.

JOB ROLE



COMPANY SIZE



Zero Trust today

As a reminder, Zero Trust eliminates automatic access for any source – internal or external – and assumes that internal network traffic cannot be trusted without prior authorization.

Focusing primarily on perimeter security and firewalls is no longer enough. Many organizations are now adopting the Zero Trust security mindset of “never trust, always verify” to segment internal networks and prevent the spread of breaches. As users move steadily off the campus network to a distributed, work-from-anywhere model, this principle must be extended to endpoints to reduce the attack surface.

Zero Trust is valuable because it addresses the fact that, as the MITRE ATT&CK Framework puts it:

> “The adversary is trying to move through your environment.”

Stopping attacker lateral movement has become so critical to a defender’s job because it is a key attacker tactic laid out in the MITRE ATT&CK Framework.

What are some practical security scenarios that can be addressed with Zero Trust technologies like micro-segmentation or multi-factor authentication?

Imagine an attacker gains access to the username and password combination of an employee. Multi-factor authentication can prevent them from merely logging-in to your enterprise applications. Or suppose an attacker compromises the data center where “crown jewel” data resides. Micro-segmentation will prevent them from moving laterally in the data center as they attempt to exfiltrate data. What about when ransomware hits an employee endpoint? Zero Trust can also ensure that the first laptop infected is also the last one infected.

How important is Zero Trust?

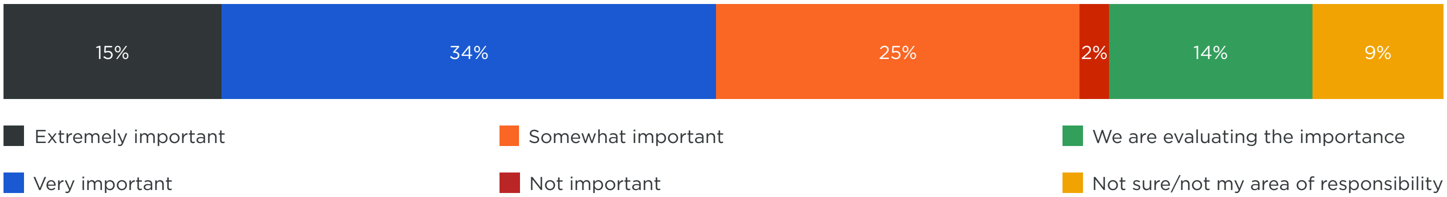
To kick off the survey, we asked organizations just how important Zero Trust is to their organizational security model in 2020.

15% stated it is extremely important, with another 34% saying it is very important. Taken together, 49%, effectively half, find Zero Trust to be critical to their organizational security model.

The other half is still in the consideration or evaluation phase: 25% find it to be somewhat important; 14% are evaluating the importance of Zero Trust; and only 2% don’t think it is important for their enterprise security posture.

Only 2% of organizations don’t think Zero Trust is important for their enterprise security posture.

HOW IMPORTANT IS ZERO TRUST TO YOUR ORGANIZATIONAL SECURITY MODEL?



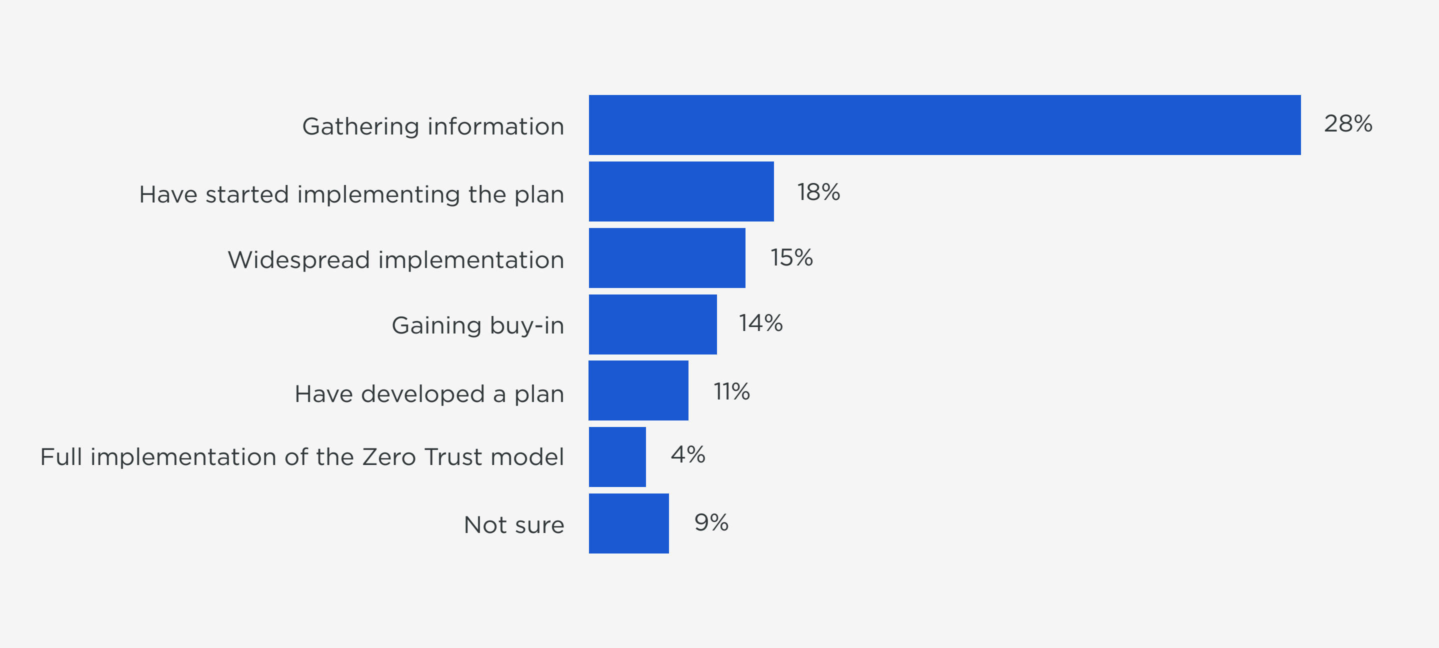
That's quite mature of you

We were also curious to learn more about where respondents are on their Zero Trust journey – their Zero Trust maturity. We asked those who found Zero Trust extremely or very important, "Where are you on your Zero Trust journey?"

Candidly, there is room to run, with most yet to have begun deployment.

28% are still gathering information, while 18% have started to implement their Zero Trust plan. 15% shared they have widely implemented Zero Trust, with another 14% working on gaining buy-in. 11% have developed a plan with 4% claiming full Zero Trust implementation. And the last 9%, well, they are not sure where they stand.

WHERE ARE YOU ON YOUR ZERO TRUST JOURNEY?



Fortunately, organizations value Zero Trust, even if many of them are early on in their journey.

What Zero Trust technologies are in use?

Naturally, upon learning how Zero Trust fit into organizational strategy, we wanted to double-click on the specifics: what technologies are organizations using in their Zero Trust journeys?

Multi-factor authentication (MFA) tops the list at 70% of respondents using it. It is a straightforward deployment and indeed provides a valuable additional layer of security beyond usernames and passwords should credentials fall into the wrong hands.

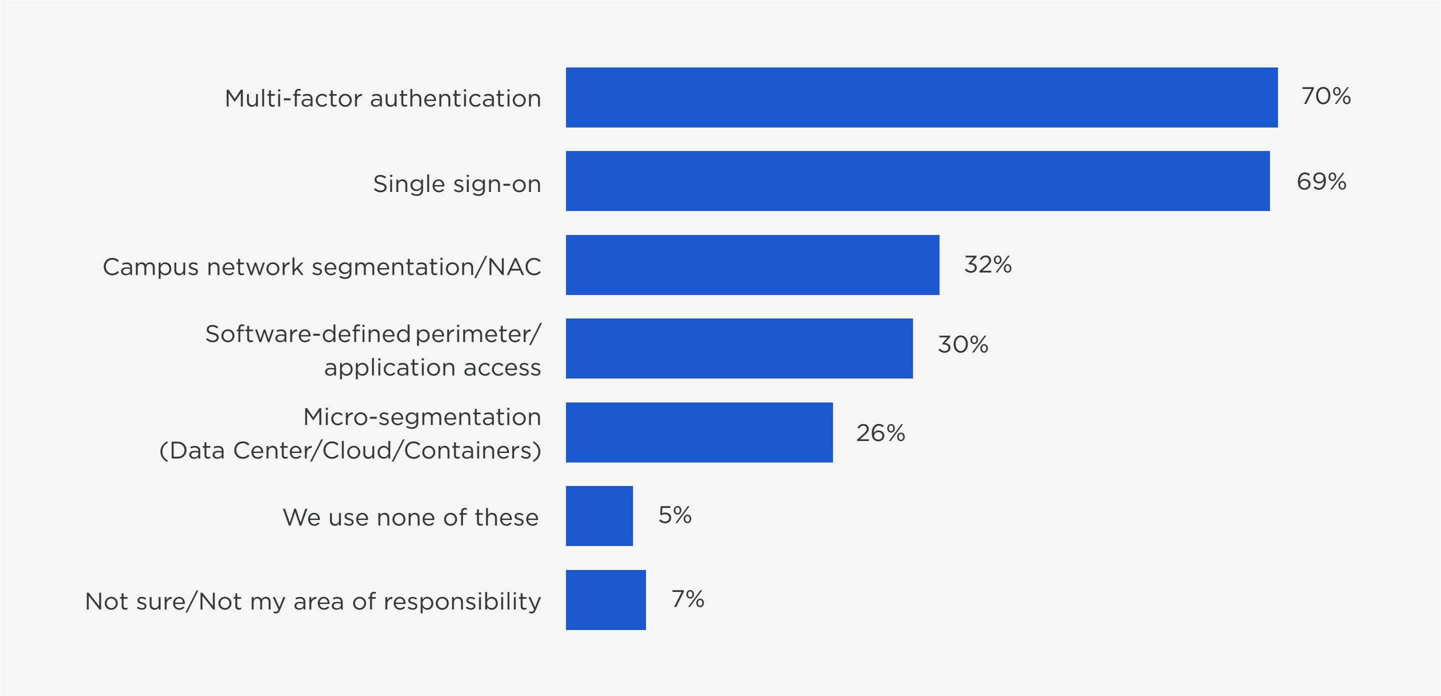
A close second was single sign-on (SSO) at 69%, enabling users to sign in once with strong credentials backed by MFA. This helps eliminate weak and reused passwords while pleasing employees with fewer logins.

Campus segmentation came in at 32%, likely due to the often complex nature of deployments of NAC tools or setting up VLANs. Software-defined perimeter technologies are being used by 30% of respondents, creating individual connections between users and the corporate resources they access, without a VPN.

Micro-segmentation, a key Zero Trust technology to prevent lateral movement of attackers, comes in at 26%.

In fact, in larger organizations with 5,000 employees or more, micro-segmentation and network segmentation are relied on equally. We anticipate micro-segmentation overtaking network segmentation, particularly in the data center, as it is more effective and less onerous than network segmentation with firewalls, ACLs, or NAC.

WHAT ZERO TRUST TECHNOLOGIES DO YOU USE TODAY?



Zero Trust tomorrow

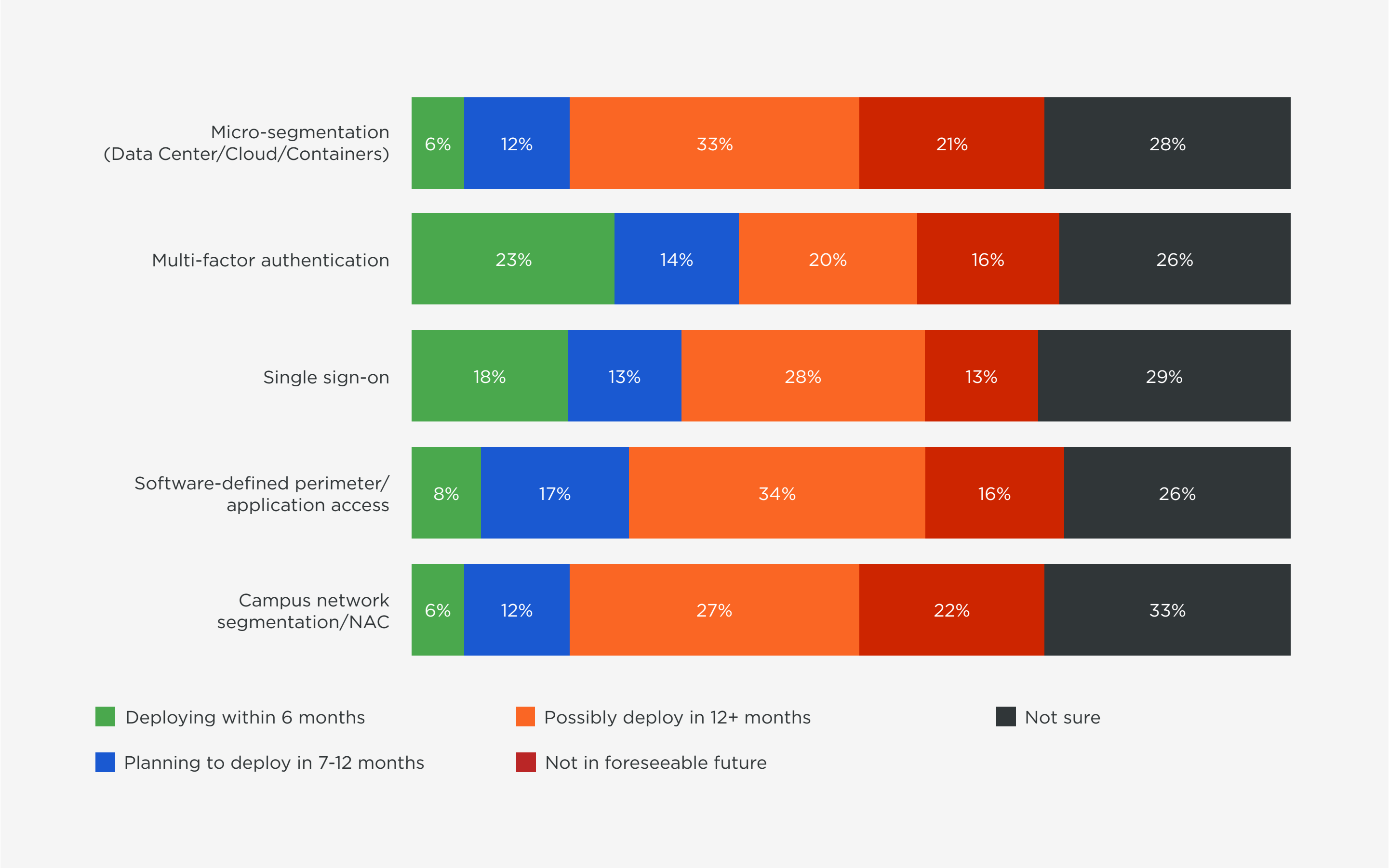
We know where Zero Trust fits in our plans, and even what is in use today. But what is next in terms of the technologies soon to be deployed, both in the short- and intermediate-term?

In the short term, over the next six months, multi-factor authentication, at 23%, is the most popular technology that will be deployed, followed by single sign-on at 18%. The use of these tools is best practice and something that is part of good defense-in-depth.

Over the next year? Micro-segmentation and SDP. More than half of respondents' overall plan to deploy micro-segmentation as one of their primary Zero Trust controls starting in the next year, given its importance in preventing high-profile breaches by stopping lateral movement. Amongst larger organizations, 70% of organizations with 2,500-5,000 employees and 61% or organizations with 5,000 employees or more have micro-segmentation deployment plans in place.

Respondents are also serious about deploying software-defined perimeter (SDP) technology.

WHAT ZERO TRUST TECHNOLOGIES DO YOU PLAN TO DEPLOY IN THE COMING QUARTERS?



The why nots of Zero Trust

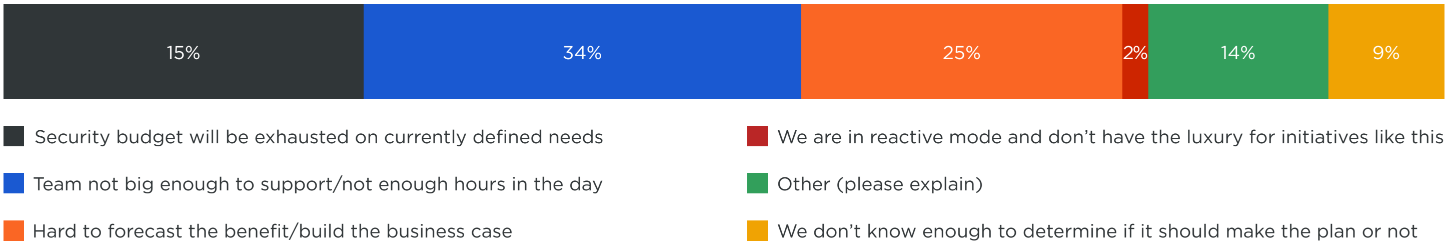
Most Zero Trust technologies seem to make good sense, so we figured we should inquire into the valid reasons why organizations will not deploy them.

For those who don't plan to deploy Zero Trust technologies in the foreseeable future, why is that?

First and foremost, budgets are finite. Nearly 30% told us they won't have enough budget to pursue additional technologies. Another common reason for 20% of respondents was the simple fact that teams are not big enough to support another new technology.

At 16% each, respondents split third place answers between trouble building a business case for Zero Trust and being in reactive mode, merely trying to keep their head above water.

WHAT IS KEEPING YOU FROM IMPLEMENTING A ZERO TRUST INITIATIVE?



SURVEY RESPONSES

> "We're keeping our eye on developments in the space."
>
> "Zero Trust has become more important over the past 12 months."
>
> "For now, we're using tools such as SSO company wide."

Deeper defense-in-depth with Zero Trust

We all have a common security objective: We want to make it more difficult for attackers to access systems and for threats to move laterally. As you've learned in this report, most organizations are considering Zero Trust to bolster their existing tools focused on threat detection that will occasionally miss a threat. And they're seeking to integrate security defenses to reduce operational complexity and better automate and enforce dynamic security for Zero Trust.

However, it is easier said than done, so you would not be alone if you have yet to start your journey.

But all in all, where does your organization stand relative to respondents? In good shape with at least a plan? Or still getting around to it? If you are still getting around to it, remember that there are many good ways to begin – and operationalize – Zero Trust.

Find an integrated platform for Zero Trust that addresses a comprehensive set of requirements and helps you to build a case for deploying. That is a good start – and as Aristotle said, a job well begun is half done. In other words, just get some momentum.

Remember, Zero Trust is not a product, but a strategy and philosophy based on least privilege.

With the right strategy, people, process, and technology, you can achieve an effective Zero Trust outcome.

Illumio enables organizations to realize a future without high-profile breaches by preventing the lateral movement of attackers across any organization. Founded on the principle of least privilege in 2013, Illumio provides visibility and segmentation for endpoints, data centers or clouds. The world's leading organizations, including Morgan Stanley, BNP Paribas, Salesforce, and Oracle NetSuite, trust Illumio to reduce cyber risk. For more information, visit www.illumio.com/what-we-do