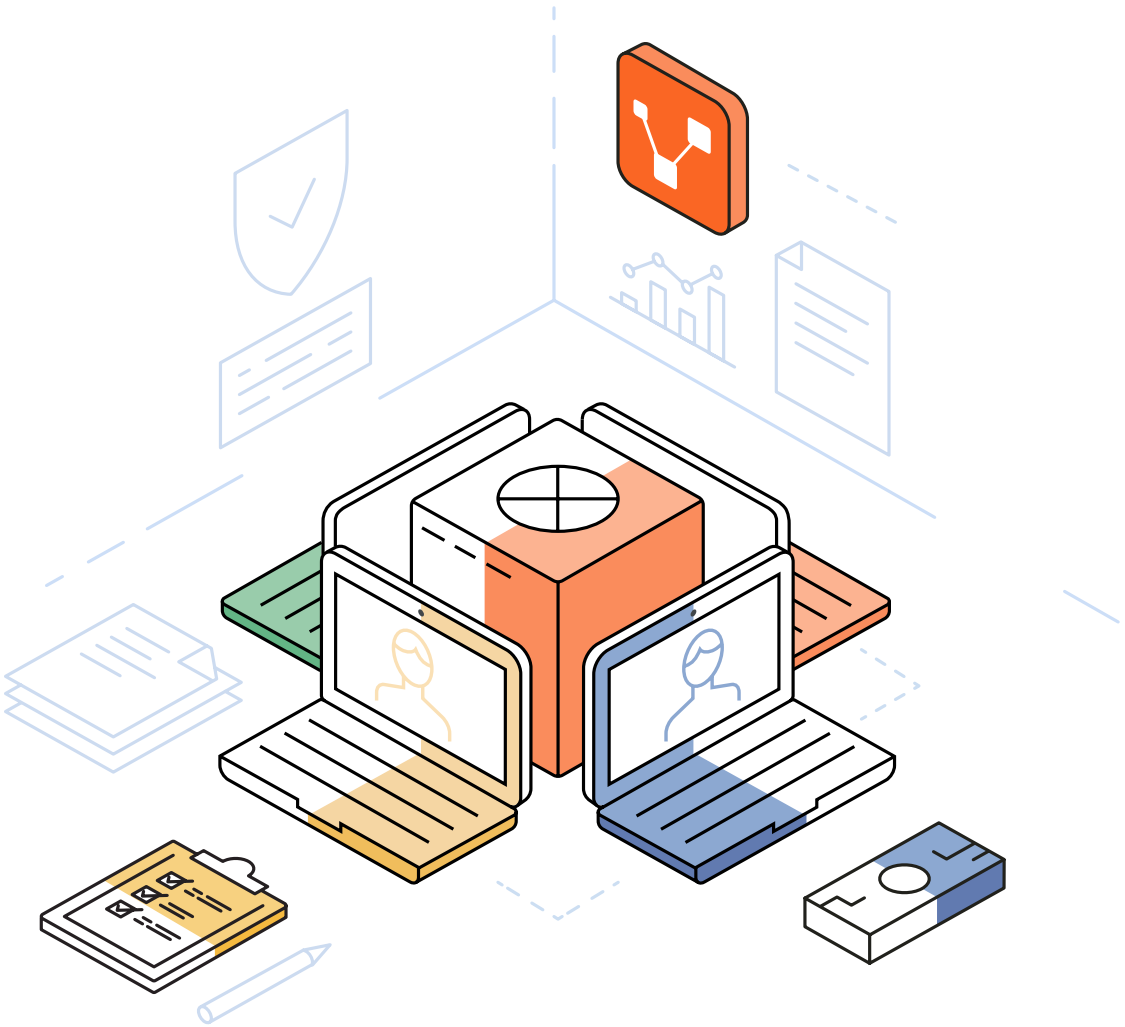
illumio

RESEARCH REPORT

The Current State of Zero Trust in the United Kingdom

Barriers and opportunities for improved security practices



Zero Trust Offers a New Path to Security

The world is changing fast. Businesses in the United Kingdom are set to support new hybrid working practices as they exit the pandemic. Cloud investments have soared. Many organizations have been pushed over a digital tipping point that is changing the way they will do business forever.

For IT security leaders, these developments are problematic, to say the least.

Digital transformation broadens the corporate "attack surface" by expanding IT infrastructure — into the cloud, through a dynamic workforce, and across new applications. This makes managing and protecting your network and its resources more challenging than ever.

At the same time, IT leaders and chief information security officers (CISOs) are confronted by an agile and determined adversary capable of targeting remote employees, insecure home networks and supply chains.

Recent multistage attacks have used an insecure entry point (an unprotected device or exposed password) to infiltrate a network and then search until something of value is found.

But if the past six months have taught us anything, it is that breaches are inevitable. Do everything you can to protect against them. Yes. But plan for the worst. And that means stopping lateral movement — keeping cybercriminals from freely traveling throughout your network once they find a way to sneak in.

Besides safeguarding critical digital resources (your customer database, your financial records, your operational systems), stopping or slowing down lateral movement makes it easier for organizations to detect and identify intruders as they search for a way to gain deeper access into your IT infrastructure.

Fortunately, Zero Trust was made for these times. First described more than a decade ago, this vision for a better security strategy is predicated on the notion of "never trust, always verify." That means: Assume all networks (and their applications and devices) are insecure and that the organization has already been breached. Users and devices must be dynamically and continuously authenticated. Access is granted to resources through disciplined verification.

Moving Beyond Traditional Practices

For Zero Trust to work, organizations need to move beyond traditional network segmentation practices. With users and applications able to reside almost anywhere, segmentation must be equally agile.

By creating finer-grained segmentation capabilities, organizations can divide and protect IT resources down to the application, location, user, process or role — helping greatly constrain the area of movement possible for attackers once they get a foothold into a network.

Clearly, Zero Trust has been become a foundational component to digital security. To understand how businesses in the United Kingdom are approaching Zero Trust, we commissioned Sapio Research to conduct an in-depth survey with senior IT and security executives and managers.

Our research found that:

- There's still some confusion over what Zero Trust means.
- The vast majority (91%) of organizations regard it as important to their security strategy.
- Most (98%) organizations plan to or have already implemented Zero Trust.
- The biggest benefit (60%) is building confidence in securing critical/confidential data.
- There are still some technical and cultural barriers to implementing Zero Trust.
- Segmentation is a critical component of Zero Trust: 92% of organizations currently segment their networks to some degree.

The survey was conducted among 203 U.K. Senior IT security decision makers, from companies with more than 250 employees. At an overall level, results are accurate to ± 6.9% at 95% confidence limits assuming a result of 50%. The interviews were conducted online by Sapio Research in June 2021 using an email invitation and an online survey.

KEY FINDING

There is uncertainty about what Zero Trust means

An overwhelming majority (96%) of respondents have an opinion on Zero Trust. But their understanding of the term varies significantly. The largest number (49%) correctly believe it to be a security framework or model.

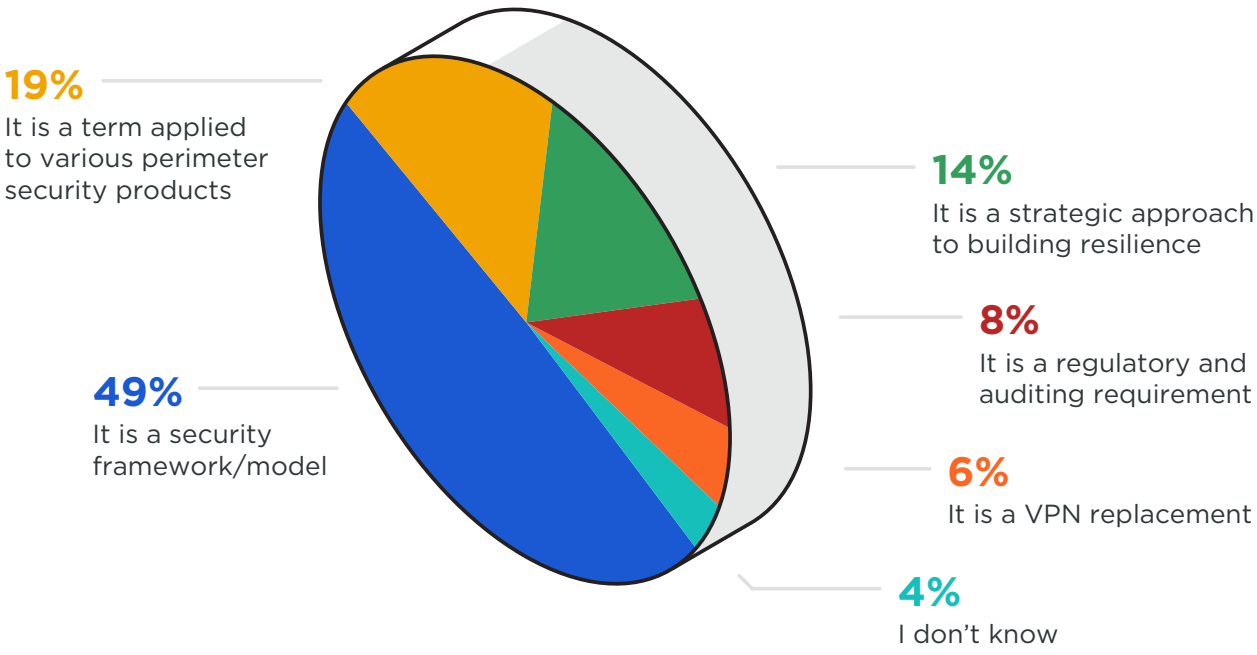
Others are also right in saying it can be a replacement for VPNs (6%) and a strategic approach to build resilience (14%). It's likely that respondents' perceptions of Zero Trust are influenced by their roles and responsibilities in the organization.

It's also true that, with such a nebulous topic, there are bound to be different opinions. Vendors offering products in various areas, including perimeter security, are increasingly using the Zero Trust moniker in marketing efforts.

In Europe, Zero Trust is increasingly thought of as a best practice approach, but buyers should be aware that no single solution can solve all their Zero Trust requirements.

96% of survey respondents have an opinion on Zero Trust, but their understanding of the term varies significantly.

WHAT IS ZERO TRUST?



illumio

KEY FINDING

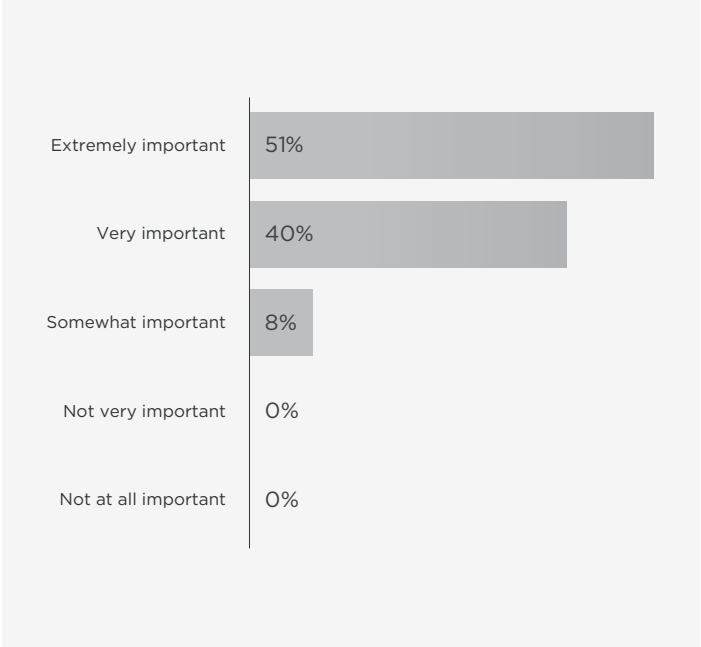
Zero Trust is important and widely implemented

U.K. organisations unanimously agree that Zero Trust is important to their security model, with 91% believing it is “extremely” (51%) or “very” (40%) important. They’re backing this up with concrete action.

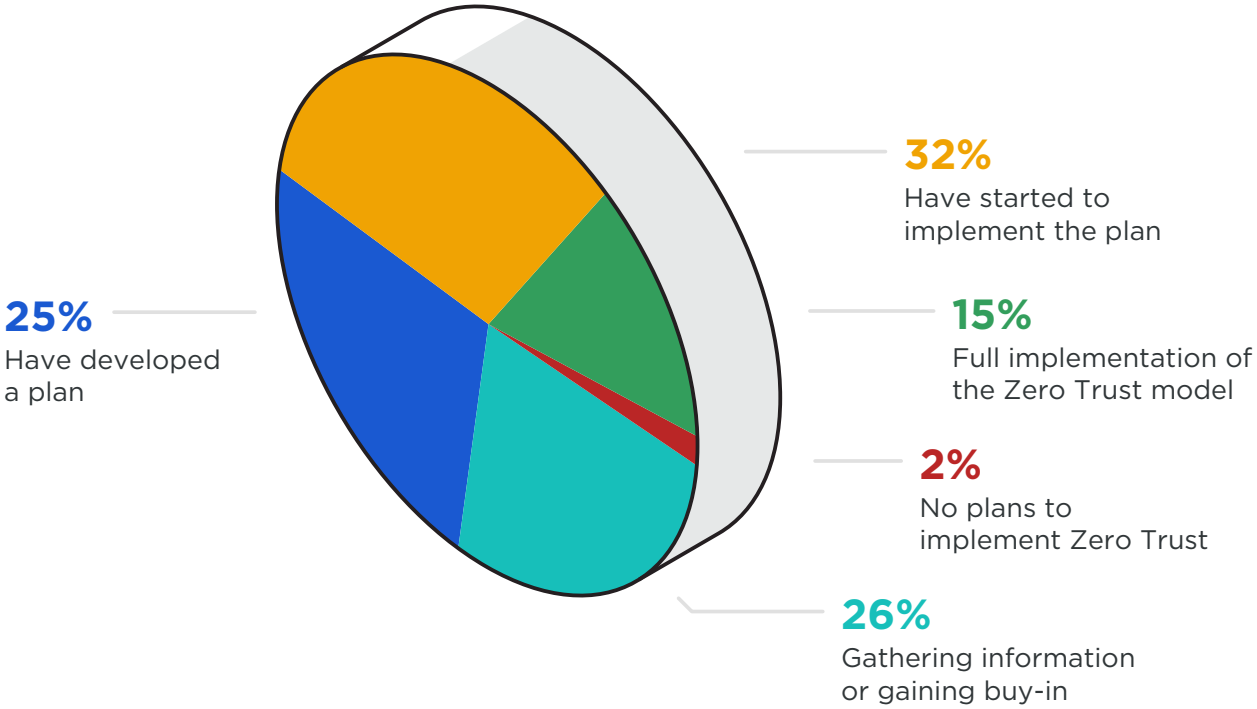
Only 2% have no plans to implement the model in their organization. With institutions such as NIST in the US and the National Cyber Security Centre (NCSC) in the U.K. publishing detailed documentation and guidance, there’s a growing body of work on which security teams can draw.

But, there’s no silver bullet solution for Zero Trust, nor is it the work solely of the security team. It’s a job for the entire organization. This can make it seem like a daunting prospect, with multiple potential roadblocks in the way. This may be why more than half (51%) of respondents are still at an early planning stage, and only 15% can claim to have fully implemented Zero Trust.

PERCEIVED IMPORTANCE OF ZERO TRUST



PLANS TO IMPLEMENT ZERO TRUST



illumio

KEY FINDING

Adopters want greater agility and a fresh approach to security

The survey found no single outstanding driver for Zero Trust projects. The most common reasons were evenly split between “a refresh of security strategy” (48%) and “improve agility for digital transformation” (47%).

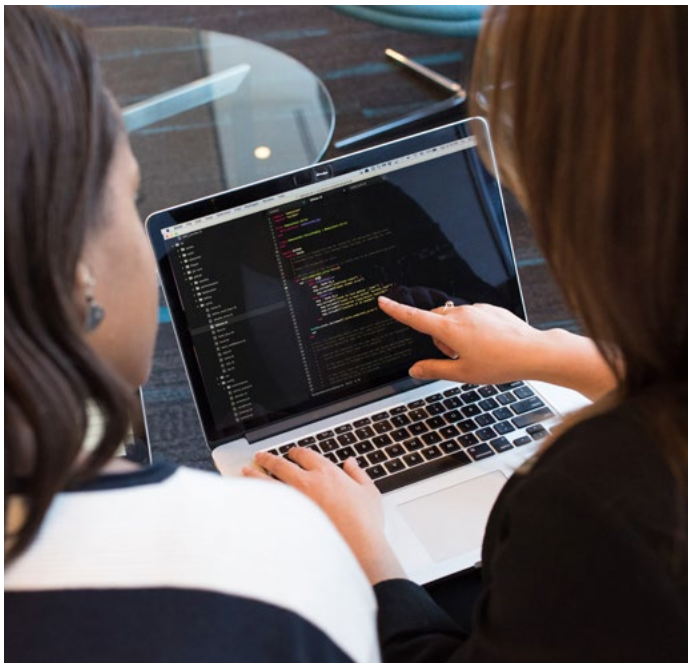
In addition, 57% believe that the adoption of Zero Trust is accelerating due to cloud migration.

With an effective Zero Trust model in place, it’s certainly true that organizations can drive digital projects with greater confidence. Zero Trust helps manage risks across distributed endpoints, IoT devices, cloud systems and other resources.

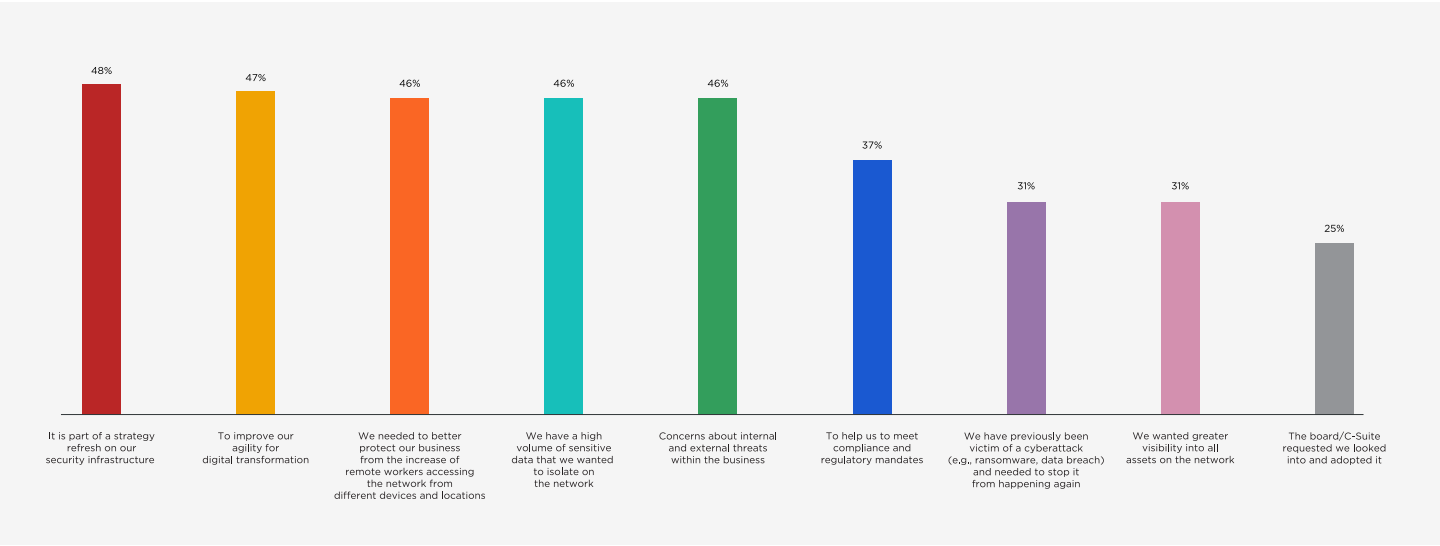
A desire to protect sensitive data, concerns about internal and external threats, and a need to mitigate the risk of fully remote employees are also key drivers for Zero Trust.

The model’s “never trust, always verify” mantra means there’s less need to focus on the location of user or workload. This fits neatly with the increasingly distributed nature of corporate assets and users today.

57% of survey respondents believe a greater move to the cloud is accelerating adoption.



REASONS FOR ADOPTING ZERO TRUST



illumio

KEY FINDING

U.K. organisations see benefits across the board

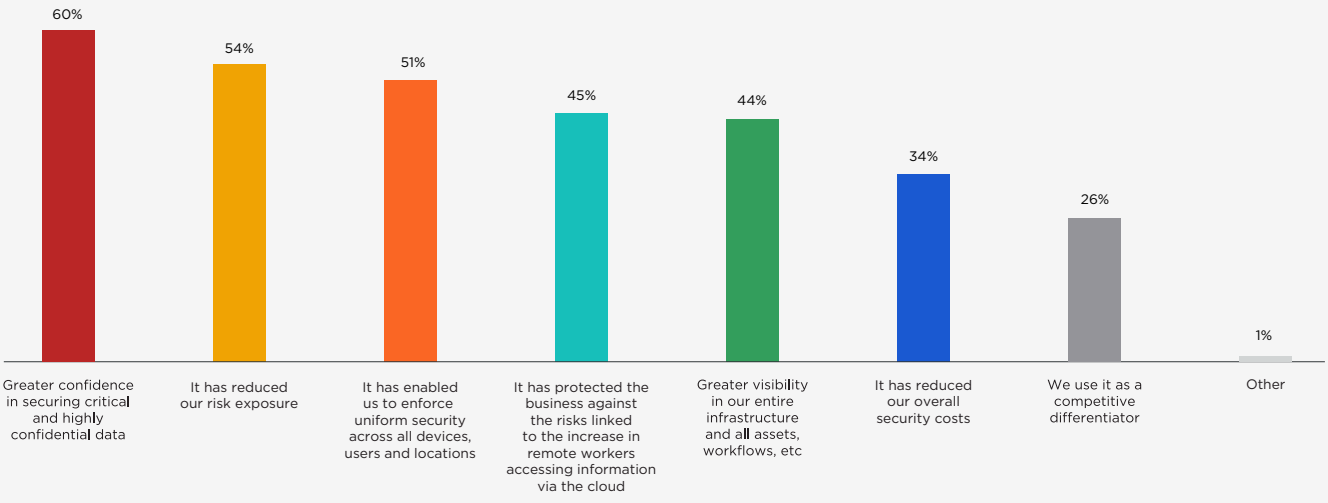
Zero Trust is not just another security buzzword. It's already helping U.K. organizations achieve tangible benefits. Top of the list is greater confidence in securing critical and confidential data (60%).

More than half also reveal that it's helped to reduce their risk exposure (54%) and enforce uniform security across all devices, users and locations (51%).

Zero Trust is protecting many businesses from the exposure associated with remote workers accessing cloud resources, a key challenge in the emerging hybrid workplace. And in a world of increasing IT complexity, it's providing greater visibility into infrastructure and assets.

Given that threat actors thrive in the shadows, anything that can shine a light on the IT environment in this way is welcomed. Many organizations claim they've even reduced their security costs and been able to use Zero Trust as a differentiator.

BENEFITS FROM IMPLEMENTING ZERO TRUST



illumio

KEY FINDING

Technological barriers are common, but not insurmountable

Some 80% of respondents say they've faced technological or operational barriers to implementing Zero Trust. This is understandable given that many projects are still in their infancy. But, it's heartening to note that most barriers were cited by only a third of organizations or fewer.

For the 35% who say they already have a strong user authentication program in place, it's important to note that this technology could certainly be integrated into a Zero Trust program.

Rather than being a barrier, it's a great start. Legacy technology (29%) and cost (22%) and resource (19%) challenges are also cited by some respondents.

Experts agree that Zero Trust is a major undertaking. But, rather than trying to boil the ocean, organizations should choose to execute smaller projects sequentially. That will boost their chances of success by breaking the work into manageable stages.

KEY FINDING

Resistance to change is the top cultural barrier

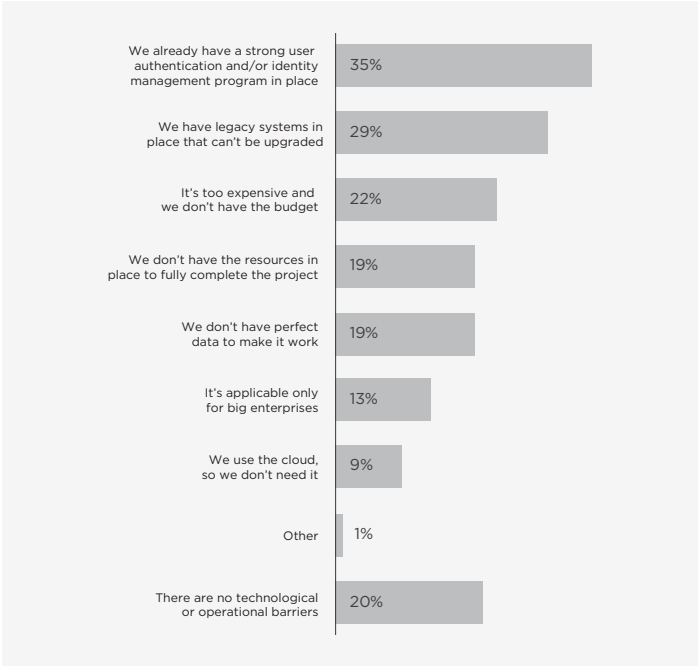
Perhaps more concerning than technological barriers are those related to cultural issues, as these can impact provision of budget. But even here there is optimism for the future.

A fifth (21%) of respondents say they don't face significant challenges. And of those who do experience them, the main roadblock is "resistance to change" unless there's a clear compliance mandate.

Perhaps if the U.K. government followed its American counterpart in demanding departments and suppliers adopt Zero Trust, these attitudes would soften.

The other barriers respondents cite could be overcome with education within and outside the cybersecurity community.

TECHNOLOGICAL AND OPERATIONAL BARRIERS TO ADOPTION

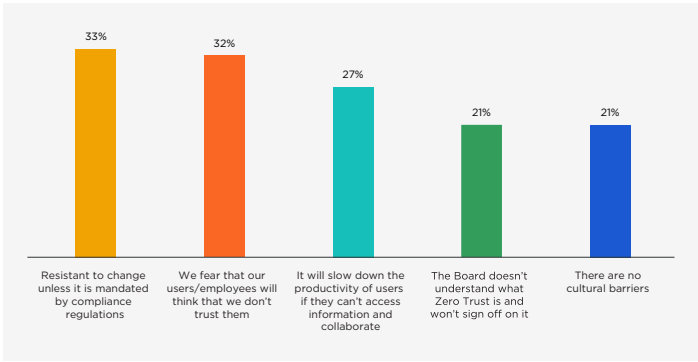


Nearly a third (32%) of respondents are afraid that users will think they aren't to be trusted.

In fact, Zero Trust is about not trusting users, applications or devices until they're verified, which is an important distinction. The ease with which threat actors can hijack user accounts makes it critical that organizations don't blindly trust anyone logging into the network until they are confirmed safe.

Similarly, Zero Trust will not slow down productivity; it merely limits access to only what an employee needs to do their job, no more.

CULTURAL BARRIERS TO ADOPTION



illumio

KEY FINDING

Network segmentation is widespread, but approaches differ

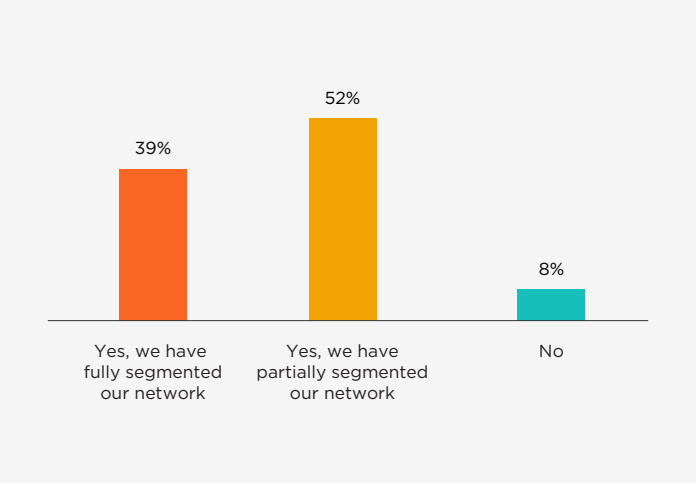
Alongside identity and access management, segmentation is a critical element of any Zero Trust approach.

So, it's good news that most U.K. organizations (92%) currently segment their networks. The most popular ways of doing so are via the legacy methods of using virtual firewalls (52%) and network-based segmentation (49%).

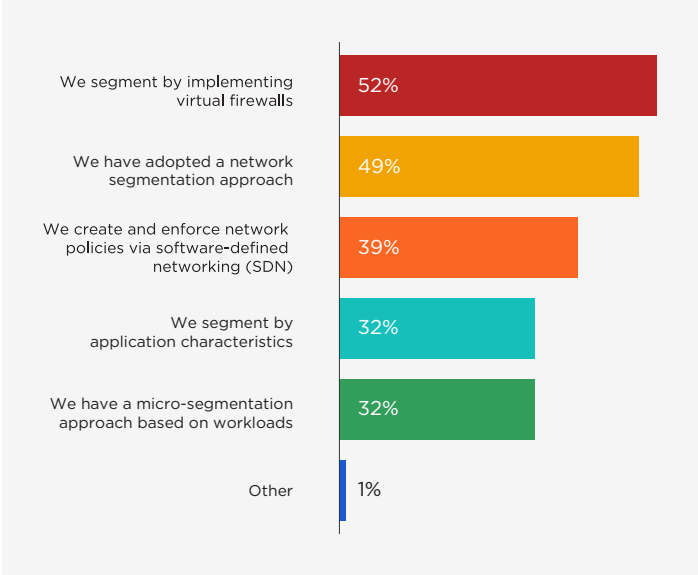
But, as applications become more distributed across multiple platforms, and regulators tighten their rules, there will be an increasing need for enhanced segmentation between apps and environments.

Unfortunately, the above legacy methods won't deliver the scale that organizations need and typically don't provide a user-friendly way to manage large volumes of firewall rules. That's why newer approaches are gaining in popularity, ones focused on ensuring the verified identity of a resource and enforcing fine-grained segmentation of applications, users, devices, etc.

ORGS WITH SEGMENTED NETWORKS



CURRENT SEGMENTATION METHODS



Many respondents say they segment by application characteristics (32%) and carrying out micro-segmentation based on workloads (32%), for example.

The latter offers the best opportunity for organizations. The right tools will deliver intelligent visibility into workload communications between applications, clouds, containers, data centers and endpoints.

Based on how these workloads communicate, they'll automatically generate optimized segmentation policies and enforce the appropriate firewall rules. That's the path to fine-grained segmentation that's easy to deploy and enforce.

illumio

Time for a New Approach to Digital Security

The surge in ransomware and other cybercrimes during the past year has shown just how vulnerable businesses and society are to these threats.

From fuel and food supply chains in the U.S. to railway stations in the U.K., no organization is safe. But a holistic Zero Trust approach provides a way forward.

Organizations should remember that Zero Trust is easier when broken down into more manageable bite-size pieces. Starting off small to gain some early wins may be the best way of bringing senior management on board and demonstrating the value of Zero Trust to business leaders.

To get there, organizations will need to focus much of their efforts on identity management and Zero Trust segmentation. Scalability and ease-of-use should be their watchwords.

From a network perspective, they need tools that provide detailed visibility into communications among resources.

The same tools must then test and automatically deploy relevant policies to segment verified resources with stateful firewalls. Success or failure may depend on how streamlined this policy generation is and whether it works consistently across environments at any scale.

Ultimately, when done right, Zero Trust can help businesses and governments become more resilient, reduce cyber-risk in the face of continuously evolving threats, and drive digital transformation. As we exit the COVID pandemic, that's exactly what's needed to create a new generation of innovation and growth.

Illumio: Lighting a Path to Zero Trust

Illumio pioneered Zero Trust segmentation (micro-segmentation) and leads the industry in providing fine-grained control of your infrastructure, down to the workload level.

Illumio's intelligent visibility and automated security enforcement stops lateral movement, preventing malware and cybercriminals from infiltrating your network, data centers and devices.

To learn more about how Illumio can help you build stronger digital security through Zero Trust segmentation, visit www.illumio.com/solutions/zero-trust or contact us.

CONTACT US
www.illumio.com/contact-sales