VansonBourne

illumio

Cloud Security Index

Redefine Cloud Security with Zero Trust Segmentation

Introduction

Modern organizations rely on the cloud to run their critical systems and store their most valuable data. Despite this, it's evident that today's cloud security solutions are continuing to fail when it comes to safeguarding companies against cybercriminals who regularly cause massive disruption by exfiltrating data and demanding exorbitant ransoms.

Complicated IT infrastructure and security misconfigurations mean that organizations are often left overexposed. Without taking a modern, proactive approach to securing cloud environments, it's becoming increasingly difficult to stop breaches before it's too late.

Digital transformation has brought with it an onslaught of attacks that make every organization a target, regardless of its size, geographic location, or industry. And failing cloud security solutions are hindering organizations' cloud adoption plans and economic returns. Organizations must take a new approach to address the increasingly complex nature of the cloud, where applications and workloads spin up and down continually and new exploits get introduced just as frequently.

This research identifies the three main cloud-based weaknesses that attackers are exploiting:

1. **Complexity** of applications and workloads, and the immense overlap of cloud and on-premises environments.
2. **Diversity** and the expansive number of services that cloud providers offer such as IaaS, PaaS, containers, and serverless computing.
3. **Poor visibility** over all the above, including the inability to identify weak points and proactively ensure protection rather than just reactively locking down compromised systems.

Organizations must modernize their cloud security solutions

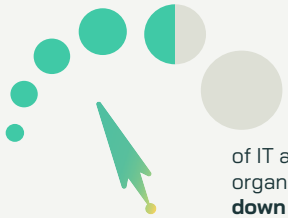
Illumio partnered with technology research specialist Vanson Bourne for a research report assessing the current state of cloud security. The aim was to assess current security tools alongside the experiences and sentiments of IT security decision makers. Using this data, we've provided insights on where to best focus your efforts to overcome the most common and pressing cloud challenges.

Read on to discover more about the shortcomings in current IT security defenses and how to combat them, so that your organization can scale and improve its security and resilience in the cloud — without upscaling cloud exposure risk.

Key global findings

Results demonstrate that traditional cloud security isn't up to the task:

More than 6 in 10 respondents believe **cloud security** at their organization **poses a severe risk.**



74%

of IT and security decision makers say that their organization's **current approach to security slows down cloud adoption.**

Why aren't traditional security tools enough? Organizations that use cloud-based services need more efficiency, visibility, and capabilities to reduce risks in their environment:

95%
need better visibility into connectivity from third-party software.

95%
need better reaction times to cloud breaches.

95%
seek to reduce workloads / increase efficiency for security operations (SecOps) teams.

Over 9 in 10
are concerned that connectivity between their cloud services and on-premises environments increases the likelihood of a breach.

46%
don't have full visibility into the connectivity of their organization's cloud services, increasing the likelihood of unauthorized connections.

Only 24%
are highly confident they can stop attackers from lateral movement through their networks.

What repercussions are organizations facing because of insufficient protection?

- Nearly **half the data breaches** suffered over the past year **originated in the cloud**.
- The average organization **lost nearly $4.1 million** due to **cloud breaches** in the past year.

Applied correctly, Zero Trust Segmentation (ZTS) – i.e., microsegmentation – contains and effectively mitigates the risk of an attack:

93% of IT and security decision makers believe that segmentation of critical assets is a necessary step to secure cloud-based projects.

100% of organizations would stand to benefit from proper ZTS implementation.

The findings reveal that the top ways ZTS improves an organization's cloud security posture is through:

55%
Continuous monitoring of cloud applications, data, and workloads

45%
Offering insights into unnecessary connectivity that could result in exposure

51%
Minimizing the "blast radius" of an attack

The Pervasiveness of Cloud Breaches

Organizations cannot be competitive or deliver the services their customers and users so desperately need without leveraging the advantages of the cloud. Simply stated, cloud offers increased productivity, greater flexibility, and unparalleled IT cost-optimization to name some of its benefits. That said, cloud usage is not risk-free. The rising popularity of the cloud, coupled with security often being an architectural afterthought, has made cybercriminals eager to look for ways to exploit weaknesses and vulnerabilities in critical systems hosted in the cloud.

The biggest problems currently facing organizations when it comes to cloud security are:

- **Increased risk**, where organizations are more vulnerable and environments more complex.
- **Cloud adoption is growing fast** because it's essential for organizations to scale at speed.

Above all, it's essential that the risks are not taken lightly, especially when almost half (47 percent) of all breaches originated in the cloud.

98%

of organizations are currently holding **sensitive data** in the cloud.

47%

of all the data breaches suffered over the past year around half **originated in the cloud**, highlighting cloud as a security weak point.

3/4

of organizations acknowledge that **breaches are inevitable**.

Cloud is a prime target for cybercriminals

One hundred percent of organizations surveyed report using cloud-based services, making cloud usage ubiquitous. While the extent of its use is varied, nearly 9 in 10 (89 percent) are running the majority or all of their services in the cloud. And with 38 percent describing their organization as fully cloud native, it makes sense that almost all (98 percent) are storing sensitive data in the cloud — such as financial information, business data, or some form of customer or employee personally identifiable information (PII). Additionally, the vast majority (89 percent) of organizations report running their highest-value applications in the cloud. These facts make it easy to see why cloud environments are often targeted by cybercriminals.

Data that organizations are handling in the cloud

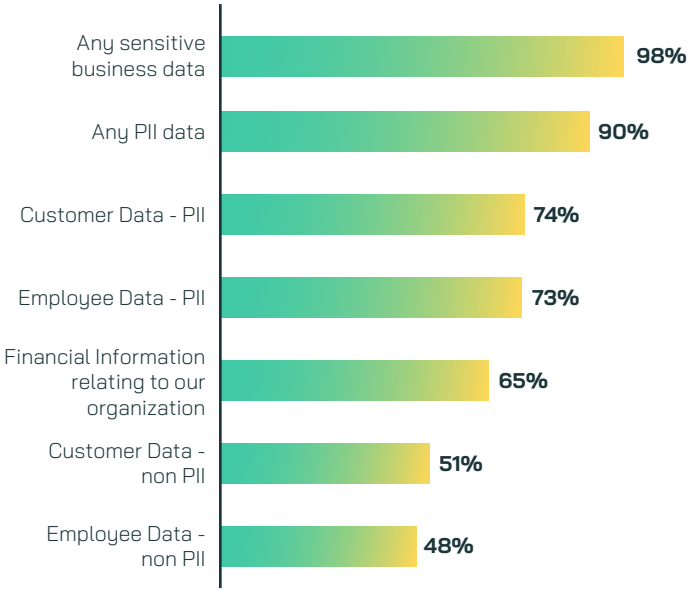


Figure 1: What types of data is your organization handling in the cloud? Asked to organizations using cloud-based services; not showing all answer options (1597)

IT security decision makers are generally aware of the threats posed to their organization's cloud security posture, but there are some geographic discrepancies. For example, while 55 percent of U.S. respondents report that they understand their organization's cloud security risk exposure very well, only 39 percent of Australians can say the same. After digging deeper, findings demonstrate that the three biggest perceived threats to cloud resilience are the overlapping traditional boundaries of workloads and data (i.e., on-premises, cloud, virtual (43 percent)); a lack of understanding of division of responsibility between cloud providers and vendors (41 percent); and concerns regarding social engineering to gain unauthorized access (36 percent). Given these threats, and the existential risk that any cloud workload is just one misconfiguration away from being exposed to the internet, adopting a security strategy that enables safe productivity in such an untrustworthy environment is a must. Enter Zero Trust.

Zero Trust is a strategy designed to stop data breaches and prevent the successful culmination of a cyberattack by eliminating the trust from digital systems. Rather than making assumptions about the underlying environment of where a resource is running, Zero Trust focuses on granting access to resources based on who needs access, what the resource is, and where the resource is at any given time. This limited, least-privileged access between resources prevents attacks from spreading, contains attacks across cloud environments, and allows organizations to keep their cloud assets safe.

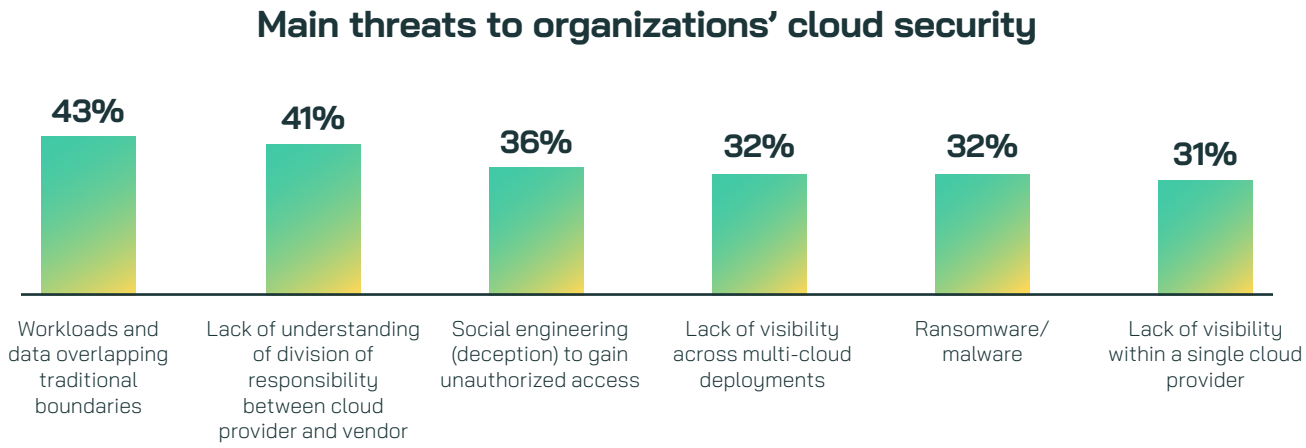


Figure 2: What do you consider to be the main threats to cloud security at your organization today? Combination of responses ranked first, second, and third. Asked to organizations using cloud-based services; not showing all answer options (1597)

Views on cloud security

Three out of four organizations (74 percent) agree that breaches are inevitable. Although this varies by country (Australia is least likely to agree (50 percent), whereas the UK (82 percent) and UAE (88 percent) are the most likely), organizations recognize that the odds of never encountering a breach are low. Therefore, security stacks must have the tools and technologies that deliver resilience in the event of a breach (not if, but *when* it will occur). Today, only 21 percent of organizations report using dedicated microsegmentation technology to contain attacks, prevent lateral movement, and boost resilience. This clearly highlights misplaced investment and trust in the wrong tools. Insufficient strategies put organizations at a disadvantage against cybercriminals who are continually capitalizing on the latest technologies to evade perimeter defenses, bypass identity access management solutions, and override firewalls.

People everywhere are desperate to make sense of the increasingly complicated scams that are targeting and exposing the weak areas in their digital lives. The same is true within organizations. Our research shows that on average the cloud breaches that businesses have endured during the last 12 months were a roughly even split — either originating from the organization's own cloud environment (51 percent) or from a third-party / vendor's cloud environment (49 percent). With that in mind, it's clear that visibility, consistency, and control across cloud environments are what organizations need most. One of the most effective ways to achieve this is with security tools that can map workloads and connections, and also provide real-time monitoring of potential security risks before a compromise of the IT ecosystem. The next section shows that traditional cloud security tools that are perimeter-based, static, or merely detect vulnerabilities have cost many organizations significantly.

Shortcomings of Existing Security Tools

A breach may make headlines for the volume of data lost or the number of customers affected, but there is a long list of indirect financial consequences that are just as serious. Of all the impacts associated with a cloud breach, IT security decision makers highlight reputational damage as their primary business concern (it's particularly high in the UK (47 percent) and Singapore (45 percent)). Big brands suffering data breaches over the past two decades have shown that trust in an organization takes a long time to establish and can be destroyed in an instant. And the business implications of breaches go far beyond the downtime, regulatory fines, and immediate stress placed upon security operations teams during a breach and in the aftermath.

Rather than being caught off guard when breaches occur, an organization's best defense is proactively preparing for an attack in advance. This is especially true when almost two-thirds (63 percent) of IT security decision makers believe their organization's cloud security is lacking and poses a severe risk to the business. Organizations must be prepared for, and assume, that they'll inevitably be breached. Otherwise, they risk catastrophic business consequences.

95%

Say their organization needs **better visibility into connectivity** from third-party software.

63%

Believe that their organization's **cloud security is lacking and poses a severe risk**.

95%

Say their organization needs **better reaction times to cloud breaches**.

The devastating impact of a cloud breach

The average cost of a cloud-based data breach over the past year is estimated to total over $4 million USD — and that's before one considers the impacts on reputation and customer trust. To break this down, of the respondents whose organizations suffered a cloud breach in the last year, 35 percent said they lost more than $1 million as a result. The severity of the impact is likely connected to the fact that half of those surveyed (48 percent) would find normal operations impossible during a cloud breach since their most critical services run in the cloud. Given the high stakes, investing in the right security solutions seems like an obvious choice, but it isn't always as easy to find the right tools. Organizations must ask themselves, why aren't their current solutions effective? And why invest in the same solutions when confidence in your organization's cloud posture is clearly lacking? Asking and answering these questions can pave the way for more informed and impactful security decisions.

Top five impacts of a cloud breach

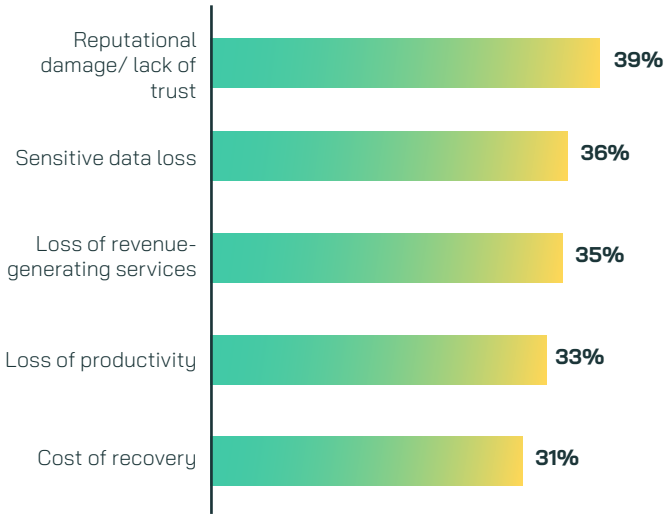


Figure 3: What are the top three impacts a cloud breach would have on your organization? Combination of responses ranked first, second, and third. Asked to organizations using cloud-based services; not showing all answer options (1597)

Where IT security tools fall short

The concern over existing security tools is clear from the large proportion of IT security decision makers that have called out the need for improvements. IT leaders agree that currently cloud security tools fall short because of the lack of visibility into third-party software connectivity (95 percent) and the poor cloud breach reaction times (95 percent). Additionally, limitations are identified around enforcement of security protocols and rules such as least-privilege access (94 percent) and ease of use when adopting cloud security best practices (96 percent). Visibility across systems and continuous improvement of security systems is an advanced way to fend off evolving threats. That said, with a majority of the respondents claiming these areas of IT security require either a lot of improvement or a complete overhaul, it's clear that many of the current approaches to cloud security are inadequate.

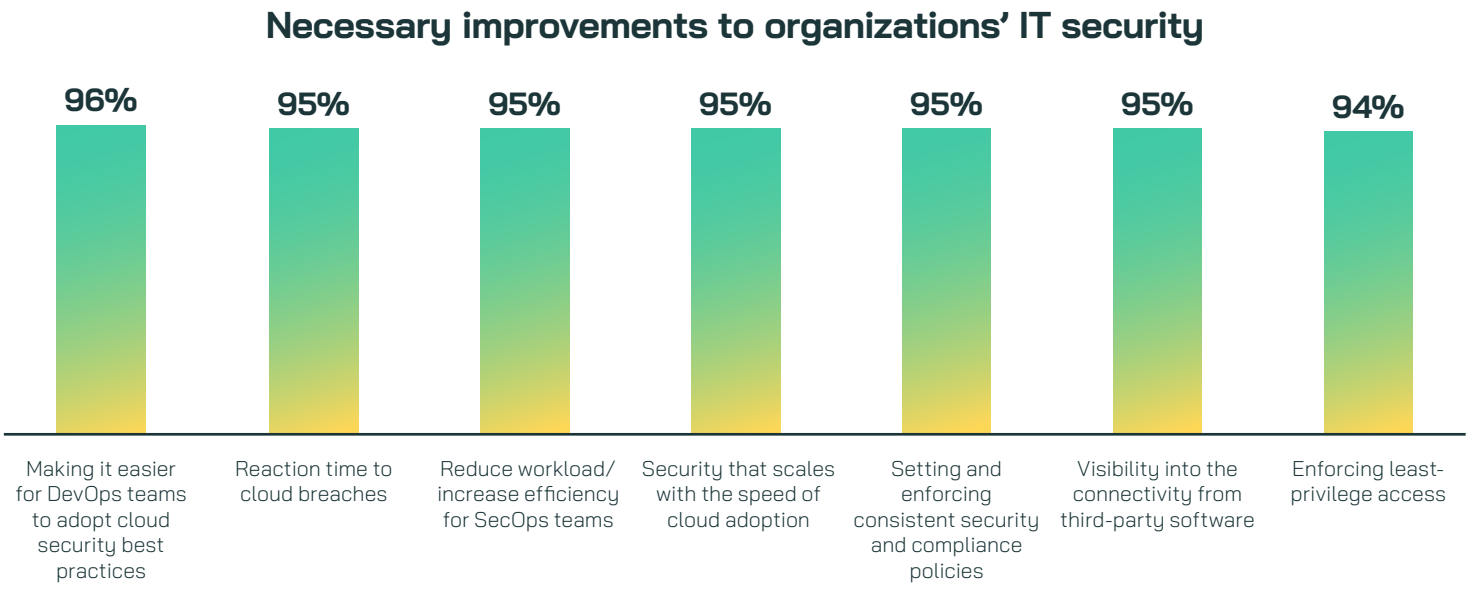


Figure 4: Do the following areas require improvement at your organization? Asked to organizations using cloud-based services; not showing all answer options (1597)

Another aspect to consider is how lackluster cloud security solutions can impede an organization's larger cloud adoption plans — inhibiting cloud progress and potentially stifling other innovations that will allow them to scale and generate additional revenue. Three quarters of respondents (74 percent) say their organization's security function slows down cloud adoption, and 92 percent are concerned that connectivity between their cloud services and on-premises environments increases the likelihood of a breach. Additionally, close to half (47 percent) are seeking to improve collaboration between security teams and application developers. Ideally, organizations should be confident of taking advantage of the democratization of technology with cloud adoption. However, these findings show that cloud security shortcomings are impeding their progress.

Additional insights reveal that only 24 percent of security teams are highly confident they can stop attackers from lateral movement in their networks. This is a major red flag. It means that most organizations won't have the resilience to maintain operations during an attack, and what's more, that the severity of the breach and business losses will increase as cybercriminals gain access to additional systems. Also, despite practically all respondents (99 percent) saying that integration between cloud security tools is important to their organization, as many as two in five (38 percent) are willing to forgo this at the outset of their cloud migration plans. Cybersecurity is a proven concern for business decision makers; therefore, the willingness to go without may be indicative of current tools failing to offer ready-to-integrate or easily implemented and scalable solutions. If these capabilities are obtainable at the outset, then surely it should be more of a priority during the purchasing process.

Using Zero Trust Segmentation (ZTS) to Increase Cloud Resilience

Despite the widening, complex cloud landscape, IT security decision makers are confident that Zero Trust Segmentation (also known as microsegmentation) plays a critical role in helping their organization achieve a more robust and resilient cloud security posture. Ninety-seven percent believe ZTS has the potential to greatly improve cloud security at their organization by containing breaches and other attacks upon impact and ensuring that critical business operations continue unimpeded. The importance of trust and brand reputation, alongside business continuity and cyber resilience, are imperative for success. Therefore, it's comforting to know that IT security professionals are confident that Zero Trust Segmentation can improve all of these:

61%

Say securing all cloud services with ZTS would improve **digital trust**.

59%

State securing all cloud services with ZTS would improve **business continuity**.

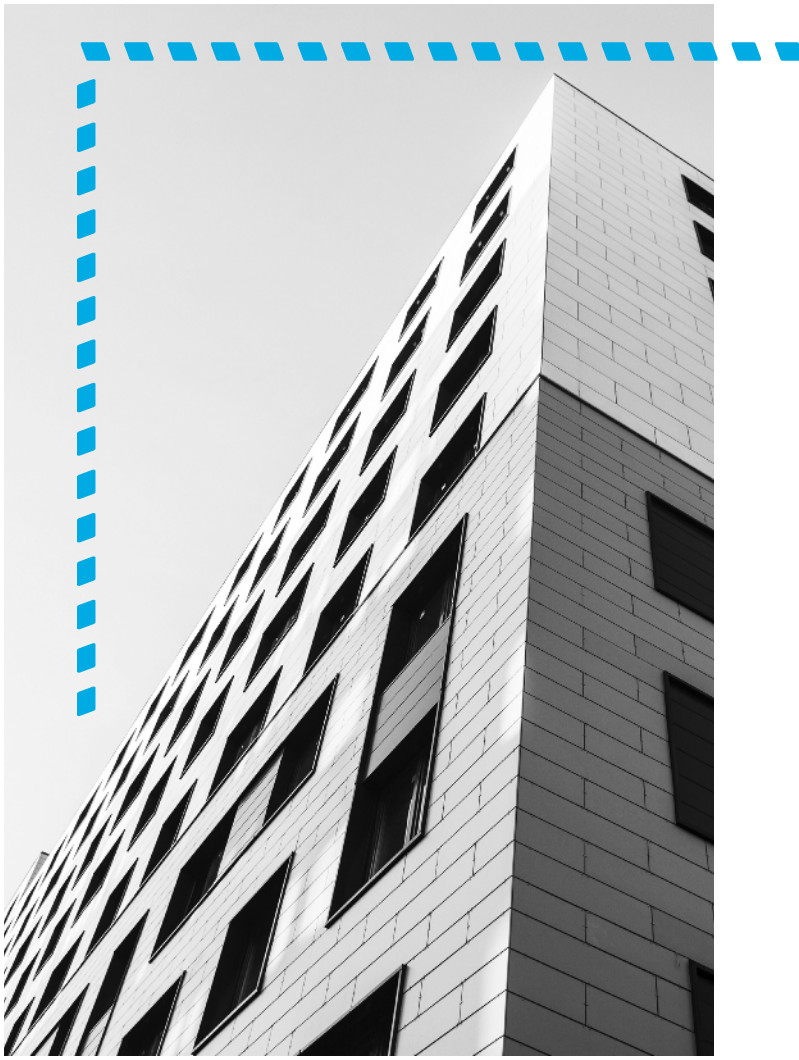
61%

Report securing all cloud services with ZTS would improve **cyber resilience**.

A closer look at ZTS employment and its benefits

The vast majority of IT security decision makers (95 percent) say their organization will prioritize improving cloud security over the next year. In addition, a similar proportion believe that segmentation of critical assets is a necessary step to secure cloud-based projects and resources (93 percent). Despite this, only a fifth (21 percent) of cloud-utilizing organizations are applying a viable approach to Zero Trust Segmentation through dedicated microsegmentation technology. Where microsegmentation is concerned, attempts to use technologies that are unsuitable for solving the hyperconnectivity problem (such as virtual firewall appliances) or are irrelevant to the problem (such as Zero Trust Network Access (ZTNA)) only add to the complexity and confusion in the cloud, leaving organizations more exposed to breaches. Meanwhile, organizations with dedicated microsegmentation technology are less likely to have suffered a cloud breach in the last year (35 percent) compared to those without it (43 percent).

According to respondents, some of the top technical benefits of Zero Trust Segmentation include continuous monitoring of the connectivity between cloud applications, data, and workloads (55 percent); minimizing incident damage to contain the spread of an attack (51 percent); and offering insights into unnecessary connectivity that could result in exposure (45 percent) without compromising productivity.



Importantly, employing dedicated microsegmentation software should address the top cloud challenges causing security gaps. This includes dealing with the complexity of connectivity of data and workloads operating across different environments plus providing SecOps teams with visibility and control to effectively mitigate the risks posed by a breach. If a breach occurs, the value lies in stopping the attacker in their tracks so that access and damage does not spread, so that business operations can continue largely undeterred. The proportion of organizations capable of stopping a cloud breach within minutes was higher among those with dedicated microsegmentation technology (30 percent) versus those without it (19 percent).

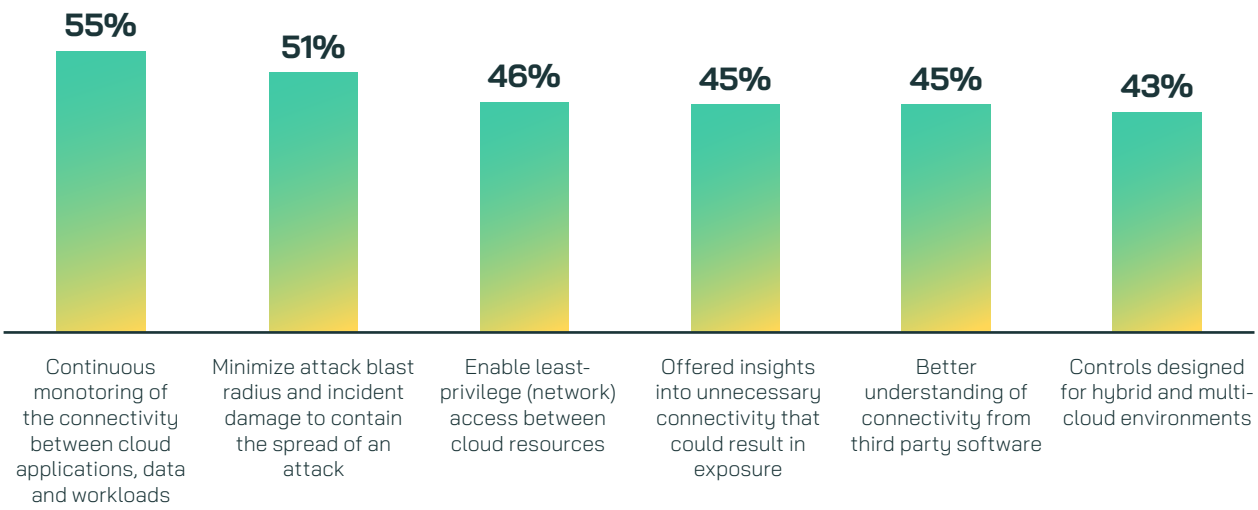


Figure 5: How has / would Zero Trust Segmentation improve your organization's cloud security? Asked to organizations using cloud-based services; not showing all answer options (1597)

Conclusion

To keep pace with the organic, fast-changing nature of the cloud and relentless, sophisticated attackers, a modern cloud security approach requires Zero Trust Segmentation. In a hyperconnected world, Zero Trust Segmentation guarantees three things: digital trust, business continuity, and cyber resilience. And a holistic, dedicated microsegmentation solution provides:

1. **Simplicity** – To combat the drawbacks of complex IT infrastructure by using a platform that supports integration with other security tools, and an agentless approach that provides real-time application and workload insights to lessen the burden on IT professionals.
2. **Scale** – Offering comprehensive traffic flow visibility of applications and workloads so that SecOps teams can gain the confidence to keep pace with company growth, making the security function an active enabler of an organization's cloud adoption.
3. **Savings** – Provide a significant ROI by reducing the likelihood and impact of a data breach. By leveraging Zero Trust Segmentation technology , your organization will quantifiably reduce time spent identifying and remediating potential attacks while minimizing the blast radius and resulting financial losses.

The fast-paced nature of technology means that IT personnel are under constant pressure to better manage their IT estate and improve its effectiveness companywide, all while battling relentless cyberattacks. That said, it's evident that traditional, static legacy tools aren't enough to ensure that critical assets are secure in the cloud. Taking steps towards increased cloud resilience is about improving confidence in the security tools in your organization's arsenal. This research reveals that confidence in the cloud is rooted in end-to-end visibility – being able to see and respond to risk across cloud applications and workloads, and over complex infrastructure, systems, and environments.

For far too long, the lack of visibility, transparency, and flexibility have prevented organizations from realizing the full potential of the cloud. Now, IT and security leaders can move forward with their cyber resilience journeys equipped with a better understanding of what toolkits are needed to secure modern cloud environments as their business scales. Teams can also better identify how modern security solutions like microsegmentation can increase lasting resilience, add business value, and ultimately restore confidence in cloud operations.

Methodology

A total of 1,600 IT security decision makers from public and private sector organizations were interviewed in September 2023 across multiple countries. Organizations were required to have a minimum of 500 employees, and respondents taking part were required to be manager level or higher.

The interviews were conducted online and were undertaken using a rigorous multi-level screening process to ensure that only suitable candidates were given the opportunity to participate.

Respondent country

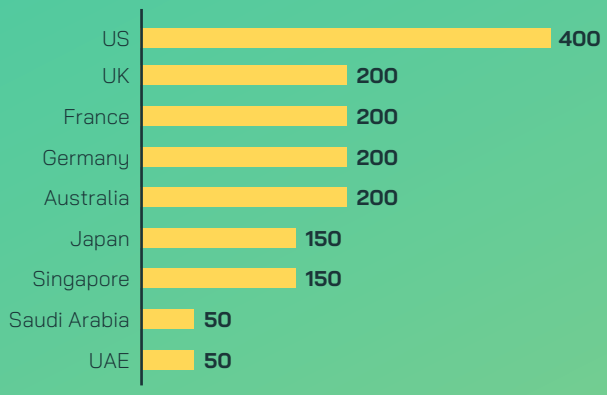
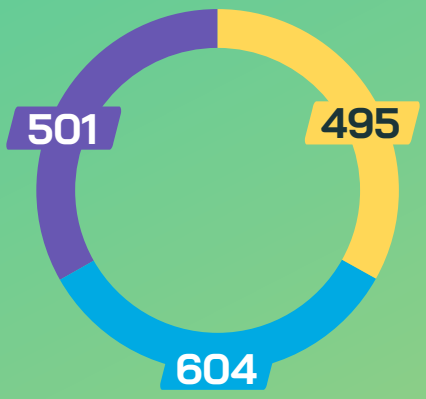


Figure D1: Showing respondent country (1600)

Organization size



500-999 employees

1,000 - 2,499 employees

2,500 or more employees

Figure D3: Showing organization size (1600)

Organization sector

Figure D2: Showing organization sector (1600)

About Vanson Bourne

Vanson Bourne is an independent specialist in market research for the technology sector. Our reputation for robust and credible research-based analysis is founded upon rigorous research principles and our ability to seek the opinions of senior decision makers across technical and business functions, in all business sectors and all major markets.

For more information, visit *www.vansonbourne.com*

About Illumio

Illumio, the Zero Trust Segmentation company, stops breaches and ransomware from spreading across the hybrid attack surface. The Illumio ZTS Platform visualizes all traffic flows between workloads, devices, and the internet, automatically sets granular segmentation policies to control communications, and isolates high-value assets and compromised systems proactively or in response to active attacks. Illumio protects organizations of all sizes, from Fortune 100 to small business, by stopping breaches and ransomware in minutes, saving millions of dollars in application downtime, and accelerating cloud and digital transformation projects.