REPORT

The State of Zero Trust

FORTINET

Executive Summary

Distributed networks and a hybrid workforce are rapidly transforming today's network environments. Workers divide their time between the office, home, and somewhere in between. Applications are split between on-premises, cloud, and Software-as-a-Service (SaaS) deployments. And data, once the sole province of the data center, is increasingly distributed across multiple locations. Over the past few years, ensuring that every user and device has secure, reliable access to the critical resources they need has been a top priority for IT teams. And access needs to be easy, no matter where the user is located or where applications and assets have been deployed.

The Fortinet 2023 State of Zero Trust Report looks at the progress IT teams have made in establishing a new sense of normalcy following the network upheaval initiated by the start of the global pandemic. With most employees suddenly working outside the network perimeter, IT teams scrambled to keep businesses operational. This effort often took the form of quick fixes and workarounds that exposed the weaknesses in their remote-worker strategy. It also highlighted the challenges of bringing their rapidly expanding network environments under a unified security umbrella.

Outlier environments, like poorly secured home offices or misconfigured cloud solutions implemented by DevOps teams with little security experience, became new attack vectors for cybercriminals. It quickly became obvious that the implicit trust model in many organizations was a problem. However, too many IT teams tried to solve the issue in the traditional way by throwing technology at the problem. And it wasn't long before they had a new problem of trying to get discrete point solutions to work together. These challenges are reflected in this report, which includes a number of key findings.

Organizations of all sizes are actively implementing zero-trust strategies, but challenges remain.

- Companies have deployed considerably more solutions as part of their zero-trust strategies since 2021.
- Companies are looking to enable zero trust everywhere to minimize the impact of a breach.
- Although companies are moving forward, they still face challenges, including interoperability between solutions, consistent visibility, end-to-end policy enforcement, and application latency issues.
- Respondents also complained about the lack of reliable information to help them select and design a solution.

Solutions must cover both on-premises and remote users with a consistent application access policy, and success has been mixed.

- Many solutions like zero-trust network access (ZTNA) and secure access service edge (SASE) are cloud-only. However, companies need to secure access to applications on-premises and outside of the network. Notably, nearly 40% of organizations still host more than half of their applications on-premises.
- The most significant challenge in any zero-trust strategy is the need for more integration between on-premises and cloud environments.
- Three-fourths of respondents have encountered issues with their hybrid workforce because of relying on cloud-only ZTNA.
- The top priorities for SASE solutions vary, but "security effectiveness" is the most significant, with 58% placing it in their top three priorities.

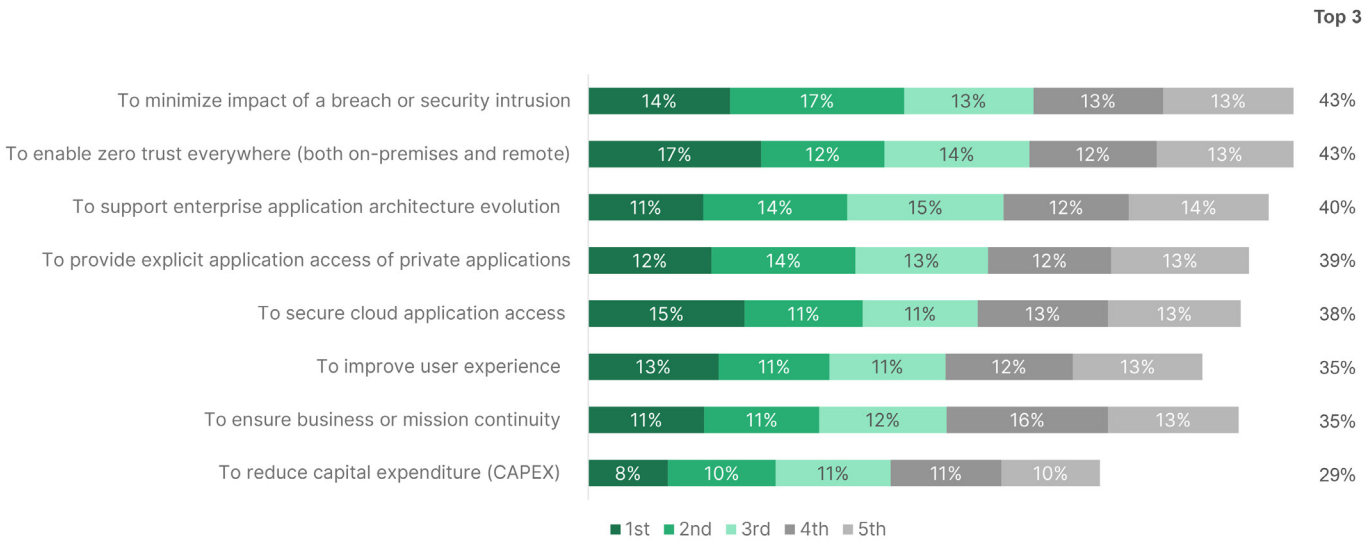
The consolidation of vendors and solution interoperability is crucial.

- Deploying solutions from multiple vendors has created many challenges for organizations, including introducing new security gaps and high operations costs.
- Larger companies are especially keen to consolidate solutions to simplify operations and reduce overhead.

Zero-Trust Strategy Priorities

The pandemic initiated a dramatic workforce transformation, with the vast majority of employees who traditionally worked on-premises suddenly working from home. This change triggered a corresponding dramatic upheaval in networks, essentially turning them inside out. Almost overnight, organizations needed to create secure network access to critical applications and resources through the perimeter, which often required upgrading remote access technologies such as edge security tools. At the same time, the limitations of traditional VPNs became apparent as hackers began accessing corporate resources by hijacking VPN tunnels through poorly protected home networks. Plans to move applications to the cloud were accelerated to offload pressure on the network perimeter and to improve the user experience.

Of course, none of these changes were entirely unexpected. The move to a hybrid workforce had been in progress for some time, but the pandemic accelerated the change. Many organizations weren't ready for the sudden transition to remote work, and they didn't have the technologies in place that the circumstances demanded. Despite these issues, two-thirds of organizations have decided to maintain a hybrid workforce, with larger employers more likely to support remote workers than smaller ones. The challenge has been providing consistent access and exceptional user experience for workers who move between on-premises and remote work locations. It has been particularly difficult for the 72% of organizations that opted for a cloud-only ZTNA solution to provide secure access to critical applications.

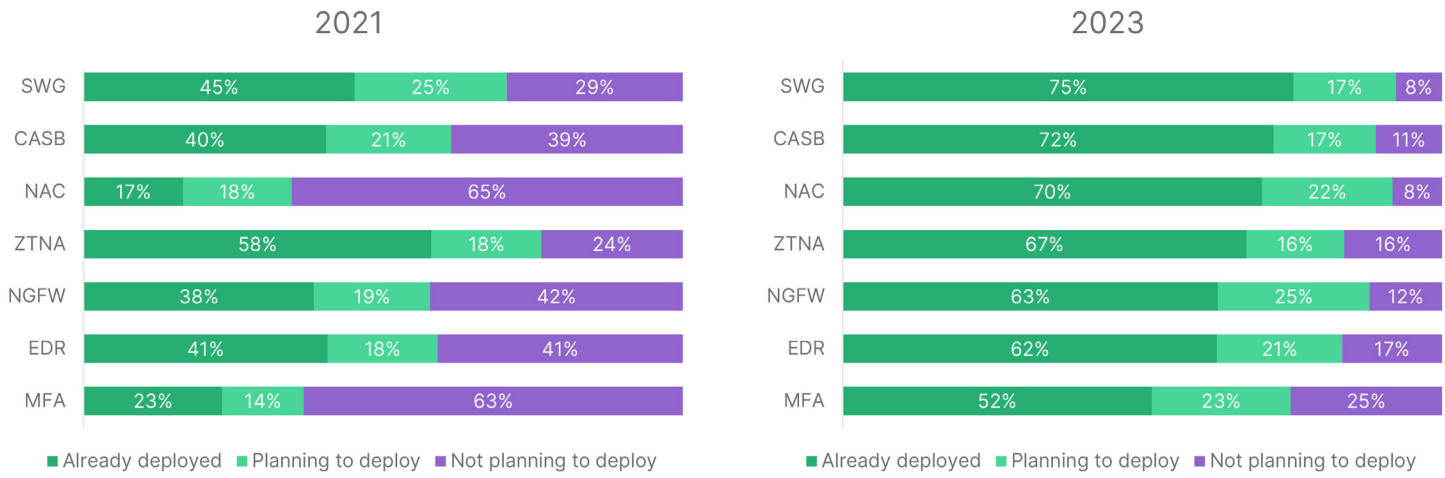


Zero-trust strategy priorities

Early on, it became clear that the best approach for managing and securing a workforce with no permanent location was to initiate a zero-trust strategy, which eliminates implicit trust based on location and enforces the principle of least privilege. The reasons are broad for implementing zero trust, but 34% identified minimizing the impact of breaches and intrusions, and 29% cited enabling zero trust everywhere as their primary incentive. Interestingly, only 18% selected reducing capital expenditure. Although their top objective for choosing a zero-trust solution (ranked as either extremely or very important) was to ensure application-layer security (85%), compatibility with both on-premises and cloud settings (82%), and integration with the rest of their networking and security infrastructure (82%) were also very high.

Organizations also report being better prepared to support and secure their hybrid workforce with a wide range of solutions already in place to support their zero-trust strategies. The solutions that have been implemented include secure web gateways (SWGs) at 75%, cloud access security brokers (CASB) at 72%, network access control (NAC) at 70%, ZTNA at 67%, next-generation firewalls (NGFWs) at 63%, and endpoint detection and response (EDR) with 62%. The one surprise was the relatively low implementation of multi-factor authentication (MFA) at only 52%, which is critical for preventing unauthorized access to applications and other resources.

Those organizations that have not yet implemented a zero-trust strategy indicate that they plan to invest in many of these same technologies as part of their zero-trust strategy. The numbers have increased significantly from 2021: SWG (75%, up from 45%), CASB (72%, up from 40%), NAC (70%, up from 17%), ZTNA (67%, up from 58%), on-premises NGFW (63%, up from 38%), EDR (63%, up from 41%), and MFA (52%, up from 23%).



Already or planning to deploy as part of zero-trust strategy

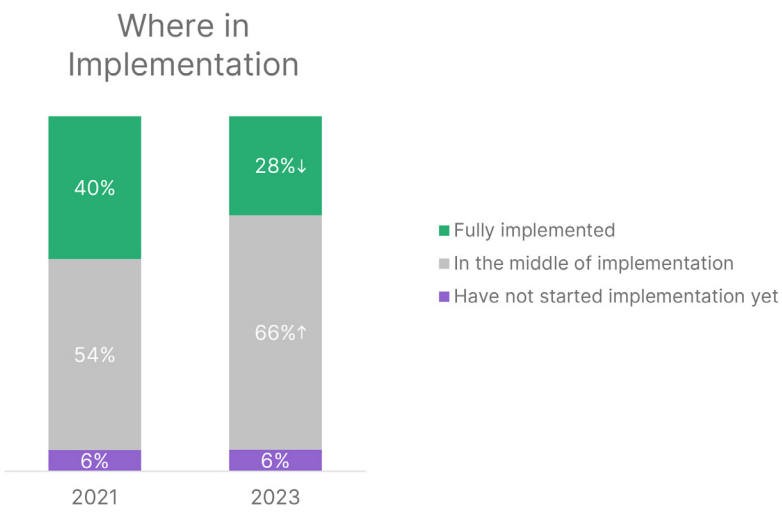
However, organizations also face serious challenges in implementing a zero-trust strategy. Nearly half of respondents (48%) indicated that a lack of integration between the zero-trust solutions deployed on-premises and in the cloud is the most significant gap they need to address. This finding may also be tied to the subsequent most common responses, which are an inability to consistently authenticate users and devices (46%), being unable to provide consistent user experience (40%), and not being able to monitor users post-authentication (38%).

Another significant finding was that nearly a third (31%) also reported latency issues as a significant challenge, and almost a quarter (22%) lament their over-reliance on traditional VPNs. Implementing a low-latency solution is clearly critical to a successful ZTNA deployment.

Status of Implementation and Challenges

The status of zero-trust implementation changed surprisingly between the 2021 and 2023 surveys. In 2021, 40% of respondents indicated that their zero-trust strategy was fully implemented. But in 2023, only 28% reported having a complete zero-trust solution in place. And only 36% of manufacturers claim to be fully implemented, perhaps due to their also having to deal with the integration of IT and operational technology (OT) networks. The number of respondents now reporting being in the process of implementation is 66%, up from 54% in the previous survey.

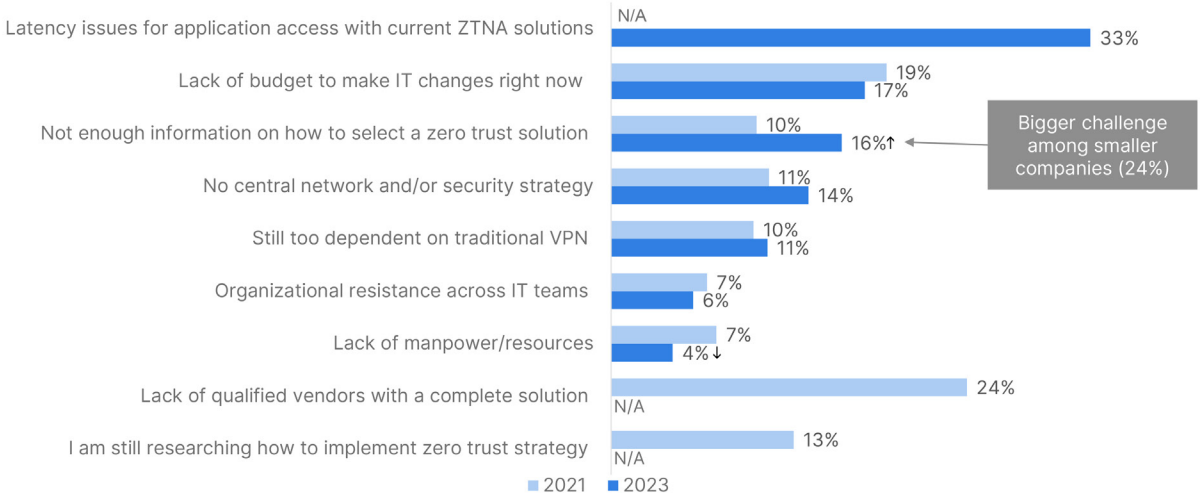
There are several reasons behind this shift in implementation status. The first is that the scope of zero-trust adoption has evolved. The initial impetus was to quickly and securely connect remote workers to applications. But the transition to a hybrid model where users move between on-premises and remote work and data and applications are divided between the cloud and data centers has expanded that objective. Data needs to be equally available regardless of the location of anything, which means more technologies are required than initially assumed.



A shift in the status of zero-trust implementation

Data flows initially thought to simply go from the user to the application and back have also changed. Workflows often span multiple environments in a single transaction, which has significantly complicated and enlarged implementation. Cloud solutions must seamlessly integrate with the on-premises network to detect and prevent the lateral movement of threats and the consistent enforcement of policy end to end.

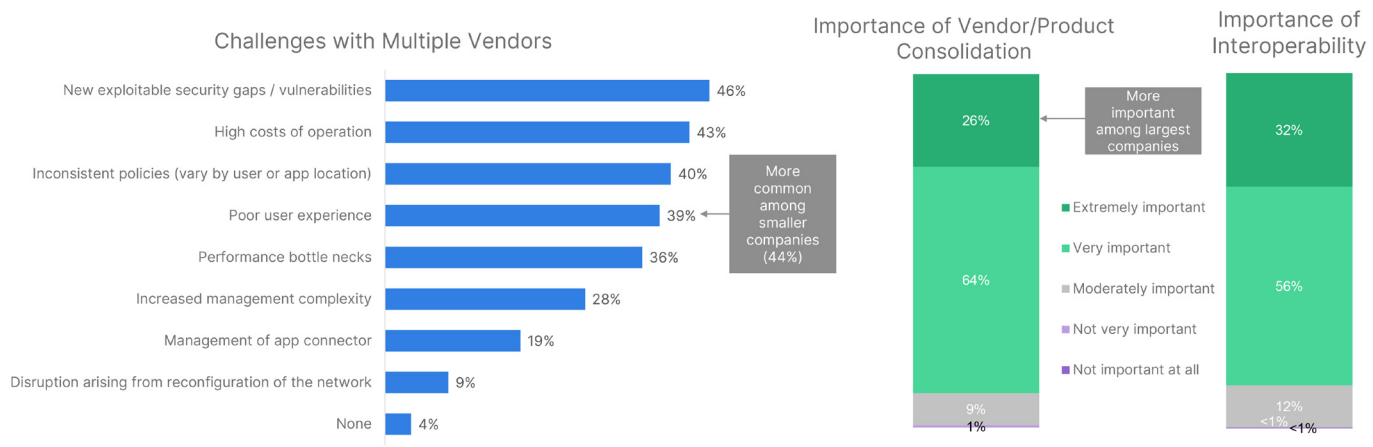
Another reason for the change in implementation is that some issues didn't become apparent until several solutions were already in place, and the need for interoperability between isolated point solutions became essential. Building and troubleshooting workarounds for tools that don't natively work together can quickly consume a significant portion of IT resources. Two of the biggest barriers are that 16% of organizations (24% among smaller companies) complain that insufficient information is available to select a zero-trust solution, and a quarter (24%) cite the lack of qualified vendors able to provide a complete solution, requiring them to cobble something together on their own. Only 4% cited a lack of human resources (down from 7%). Once it became clear that hybrid work wasn't temporary, a more consistent and reliable solution was needed, and resources were made available.



The most significant challenges in implementing zero trust

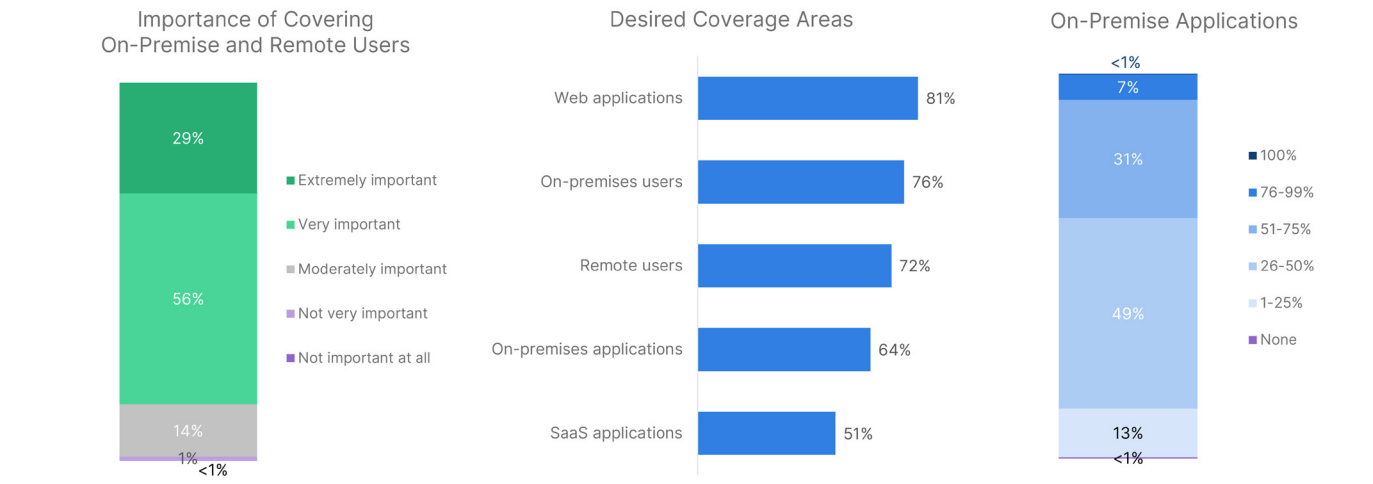
Another key takeaway from this report is that deploying solutions from multiple vendors has created new challenges for organizations, including the inadvertent introduction of security gaps and high operating costs due to vendor and solution sprawl. According to the survey, 90% of organizations now rank vendor and solution consolidation as extremely or very important, and 88% feel the same way about the importance of solution interoperability. One outcome of this is that many organizations that believed they had fully implemented a zero-trust solution are now rethinking that conclusion. It's clear that vendor and product consolidation and interoperability are crucially important to implementation.

For nearly half of respondents (46%), the top concerns are that new exploitable security gaps and vulnerabilities have been created because solutions do not interoperate and cannot communicate. And 40% also report an inability to consistently apply and enforce policies. Related to these findings is the high cost of trying to keep a disjointed solution up and running, with 43% citing this problem as a top challenge. Other related challenges include poor user experience (39%), performance bottlenecks (36%), and increased management complexity (28%).



Why consolidation and interoperability matters

Despite claims that everything is moving to the cloud, most organizations still have a hybrid application and data strategy in place. Surprisingly, 38% of organizations still have more than half of their applications on-premises. And another 49% have somewhere between 26% and 50% deployed there. So, it's no surprise that 85% of survey respondents identified the need for ZTNA solutions that cover both on-premises and remote users as very or extremely important. Zero-trust network access needs to work no matter where applications and users are located, and the top areas that a hybrid ZTNA strategy must cover include web applications (81%), on-premises users (76%), remote users (72%), on-premises applications (64%), and SaaS applications (51%).



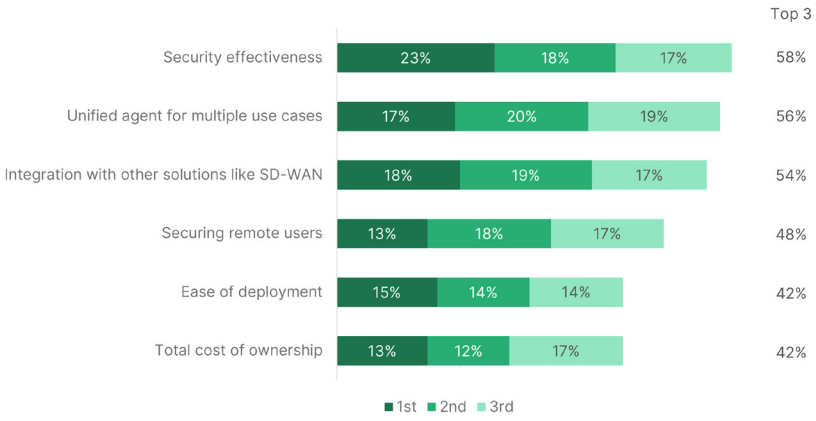
ZTNA solutions need to cover users and applications no matter where they are located

Notably, three-fourths of respondents report encountering issues with their hybrid workforce from relying on cloud-only ZTNA. They need a Universal ZTNA solution that supports applications in the cloud and on-premises, with consistent features and polices across deployments and a per-user licensing model so protections (and licenses) can move seamlessly as work-from-anywhere (WFA) users move between their homes and on-premises offices.

SASE Integration

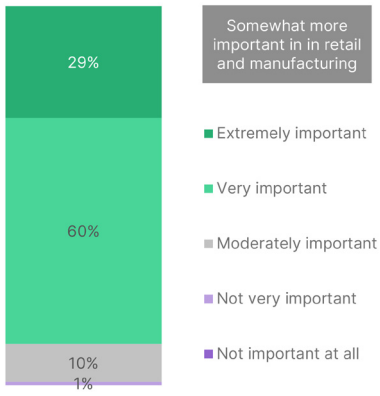
A critical element of any zero-trust strategy is ensuring a simple and seamless mechanism for providing consistent security to employees working remotely and in the office. One of the most significant issues encountered early in the transition to a WFA model was that home offices were notoriously undersecured. But extending enterprise-grade security to those environments was both cost- and resource-intensive, so SASE solutions quickly became a powerful option for providing secure, reliable access to cloud-based applications for remote workers.

However, the challenge is that most SASE solutions do not interoperate with the physical network. Connections, policies, and monitoring need to be handed over using some sort of extra mechanism that needs to be designed and managed. So even though security effectiveness is the top priority for SASE solutions (58%), 56% of respondents also want a unified agent that can support multiple use cases, and 54% want SASE to interoperate with other solutions, like SD-WAN. And 42% want that to include ease of deployment and a manageable total cost of ownership.



SASE solution priorities

According to 89% of respondents, SASE integration with their on-premises solutions is very or extremely important. The value lies in their ability to consistently enhance user experience, simplify operations by consolidating tasks, implement zero-trust policies, and secure access to cloud applications. These findings indicate the value many organizations can gain from single-vendor SASE solutions that provide converged network and security capabilities to all users and devices in distributed locations.



The need for SASE to integrate with the rest of the network

Conclusion

The realities of a permanent hybrid workforce and an expanding network that encompasses on-premises, multi-cloud, and cloud services, such as SaaS, have required organizations to transition from an implicit trust model to a zero-trust strategy. Ensuring reliable application access, consistent security, and an optimized user experience for every user, regardless of location, are the key drivers of this change. The challenge is that most networks are complex, with applications divided between cloud and on-premises deployments while users move back and forth between their homes and workplace offices. As a result, implementing zero trust has been more difficult than many organizations first assumed. And organizations often receive little to no reliable guidance from vendors, many of which provide solutions designed for cloud-only deployments.

As the zero-trust market segment continues to mature, it's becoming clear that organizations that have begun to implement a zero-trust strategy must consolidate their vendor and solution footprint. They need solutions that are designed to span multiple environments and can converge networking, security, and access into a single, integrated framework. By taking this approach, they can seamlessly extend their zero-trust strategy to every user and application in every corner of their network while maintaining broad visibility and control end to end. Only then will organizations be able to take full advantage of the opportunities today's hybrid strategies provide.

June 14, 2023 1:02 PM

2167932-0-0-EN