REPORT

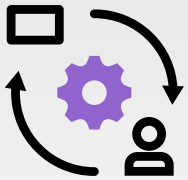
The State of Zero Trust Report

TABLE OF CONTENTS

Executive Summary

The zero-trust network security model has become a pervasive topic for IT professionals. Many organizations have a vision of what they want or need in terms of zero-trust and zero-trust network access (ZTNA), but the completeness of their vision isn't necessarily being translated into the solutions they're able to put in place.

Most organizations claim to either have a zero-trust access (ZTA) or ZTNA strategy either in place or in active deployment. However, most also report that they cannot consistently authenticate users or devices and struggle to monitor users after authentication. Additionally, many organizations also report that implementing zero trust across an extended network is difficult. Because these are generally considered to be fundamental zero-trust functions, it appears that many organizations either misunderstand zero trust or that their solutions are being incompletely deployed.



Most organizations claim to either have a zero-trust access (ZTA) or ZTNA strategy either in place or in active deployment. However, most also report that they cannot consistently authenticate users or devices and struggle to monitor users after authentication.

The State of Zero Trust

The zero-trust network security model isn't new. Data breaches are on the rise, and as organizations move more of their business functions to the cloud, attacks on web applications now represent 39% of all breaches.[1]

Most people involved in cybersecurity agree that the concepts behind the zero-trust security model make sense. Instead of assuming anyone or anything that has gained access to the network can be trusted, a zero-trust mindset assumes the opposite. Nothing can be trusted anywhere, whether outside or inside the network perimeter.

The shift from implicit trust to zero trust is a response to the rising incidents and costs of cyber crime. The global average cost of a data breach is now $4.24M, and the top three initial attack vectors are compromised credentials (20%), phishing (17%), and cloud misconfiguration (15%).[2] A robust implementation of zero-trust solutions can reduce the likelihood of attack using tools such as multi-factor authentication and mitigate the effects of a breach through techniques like microsegmentation.

The rise in remote work and work from anywhere initiatives has put the spotlight on ZTNA in particular. The more people work from anywhere, the less secure a traditional perimeter-based approach becomes. Every time a device or user is automatically trusted, it places the organization's data, applications, and intellectual property at risk. In fact, Gartner predicts that by 2023, 60% of enterprises will phase out traditional virtual private networks (VPNs) and use a ZTNA model.[3]

As more people moved into home offices because of the pandemic, the limitations of traditional VPNs quickly became apparent. They highlighted the need for better approaches—including zero-trust models—for protecting networks against threats posed by workers connecting from weakly protected home networks.[4]

Although there is agreement that zero-trust implementation should happen, a lot of confusion exists about *how*. What exactly is an effective zero-trust strategy? Zero-trust concepts have been discussed for years, yet it is often misunderstood as just "securing access." At its core, however, the zero-trust philosophy is about "securing work and learning everywhere," including the evolution of VPN. Implemented well, true zero trust is an effective strategy for securing hybrid working models going forward.

Zero Trust Survey Overview

Fortinet recently surveyed 472 cybersecurity professionals and business leaders worldwide to learn how far along organizations are in their zero-trust journey. The survey is intended to better understand the following:

- How well zero trust and ZTNA are understood
- The perceived benefits and challenges in implementing a zero-trust strategy
- Adoption of and the elements included in a zero-trust strategy

Top Priorities and Benefits

The increase in breaches and ransomware is in the news constantly, and as intrusions continue to rise, organizations are looking for solutions. Although zero trust is included as part of a comprehensive cybersecurity strategy, the top priorities vary.

"Minimizing the impact of breaches and intrusions" tops the list at 34%, followed closely by "securing remote access" and "ensuring business/mission continuity" at 33%.

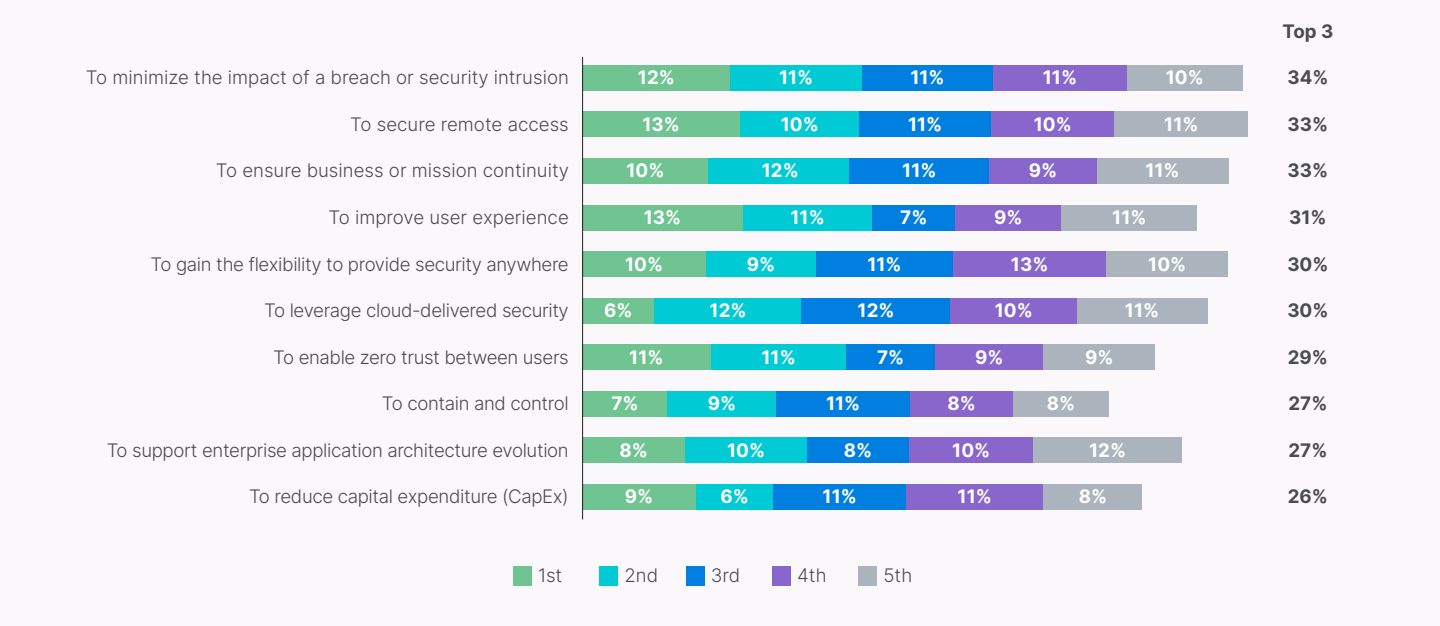


Figure 1: Zero-trust strategy priorities.

When organizations were asked what they perceived as the most significant benefit of a zero-trust solution, 22% said, "security across the entire digital attack surface," followed closely by a "better user experience for remote work (VPN)" and "being able to quickly adapt to rapidly evolving network changes," both at 19%.

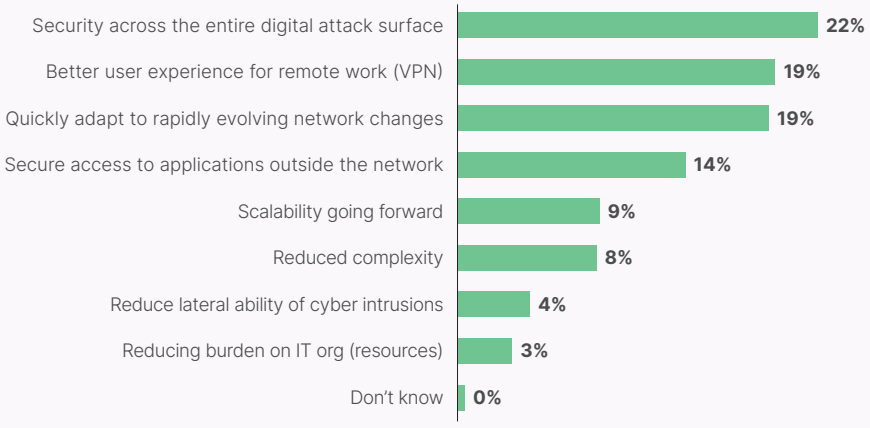


Figure 2: Most significant benefit of zero-trust solution.

The survey also indicated that securing remote access is a common priority across regions, although other priorities are less consistent in different areas of the world.

	NA	EMEA	APJ	LatAm
To ensure business or mission continuity	36%	40%	29%	24%
To secure remote access	35%	34%	32%	32%
To enable zero trust between users	33%	26%	28%	24%
To leverage cloud-delivered security	33%	27%	30%	28%
To minimize impact of a breach or security intrusion	32%	30%	34%	46%
To gain the flexibility to provide security anywhere	31%	29%	32%	24%
To contain and control	27%	22%	27%	32%
To improve user experience	26%	37%	31%	32%
To reduce capital expenditure (CapEx)	25%	30%	25%	26%
To support enterprise application architecture evolution	22%	25%	31%	32%

Figure 3: Zero-trust strategy priorities (top 3).

Level of Understanding and Implementation

One of the key goals of the survey was to determine the level of zero-trust understanding and implementation. Although many networking and security vendors use terms that include zero trust, not everyone uses it to mean the same thing. Adding to the potential for confusion are the terms zero-trust access (ZTA) and zero-trust network access (ZTNA), which often are used interchangeably.

The respondents to the survey indicated that they think they understand zero-trust (77%) and ZTNA (75%) concepts and are confident in providing secure access.

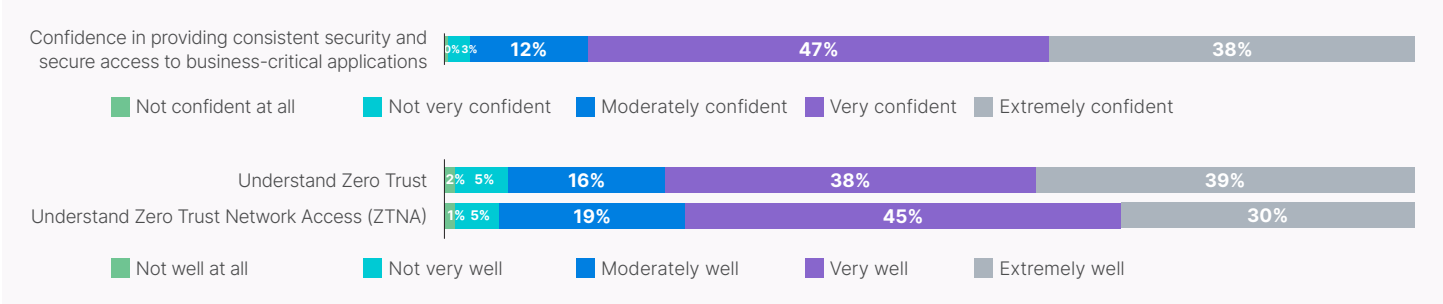


Figure 4: Level of understanding and implementation.

Disconnect Between Implementation and Gaps

One striking statistic was that most survey respondents reported that they already have a zero-trust and/or ZTNA strategy in place or development, with over one-third saying they are fully implemented. Only 6% haven't started implementation yet.

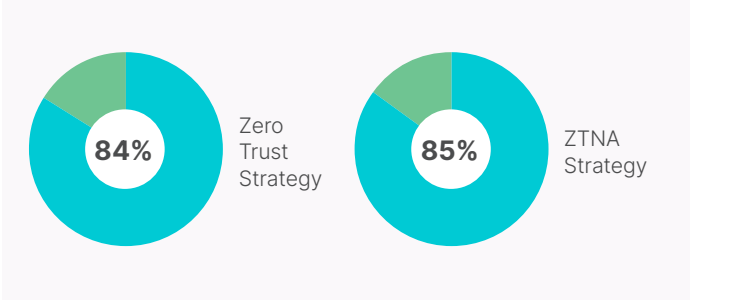


Figure 5: In place or in development.

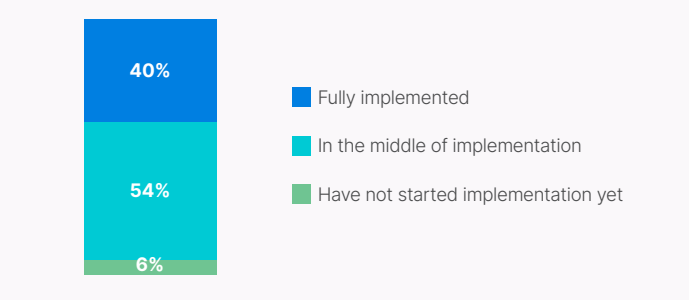


Figure 6: Where in implementation.

Although a significant number of organizations say they've either fully implemented or are in the middle of implementing a ZTNA or zero-trust strategy, more than half don't have the ability to authenticate users and devices on an ongoing basis and are struggling to monitor users post-authentication.

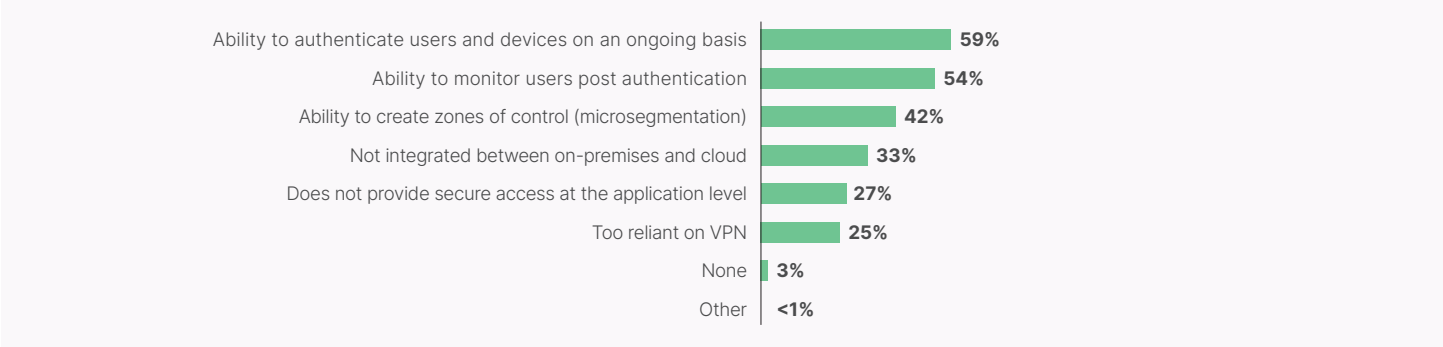


Figure 7: Gaps to address in zero-trust strategy.

These gaps are concerning because these functions are critical tenets of the zero-trust philosophy, which begs the question: What type of zero-trust implementation do organizations actually have in place? It's possible that while respondents feel they have implemented zero trust, they may not have done so. Or perhaps, that they have incomplete deployments.

The survey results indicate a disconnect between the solutions organizations have and what they need for complete security.

All regions report these gaps, so this isn't a regional difference. User authentication and monitoring appear to be a problem worldwide.

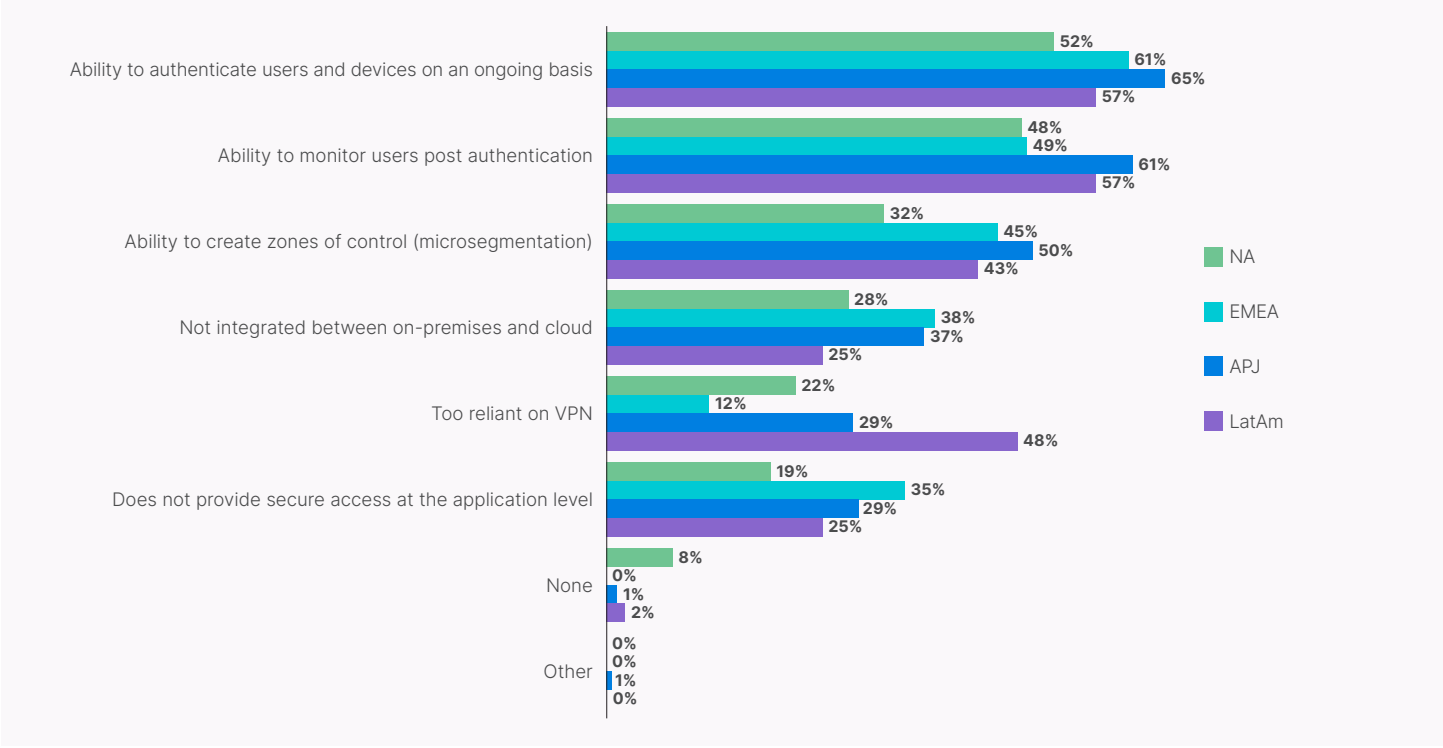


Figure 8: Gaps to address in zero-trust strategy.

Additionally, while respondents report that they're well-versed in zero-trust concepts, over 80% felt that implementing a zero-trust strategy across an extended network wasn't going to be easy. Most of them (60%) report it would be moderately or very difficult, and another 21% said it would be extremely difficult.

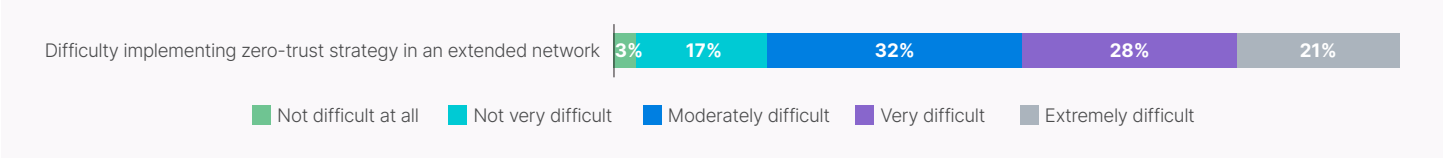


Figure 9: Difficulty in implementation.

These reported gaps reinforce the idea that while organizations may have some elements of zero trust in place, many have not implemented a complete set of essential capabilities.

Hurdles to Zero-trust Implementation

Zero-trust concepts sound great on paper, and there's almost universal agreement that it's a good idea, but adding yet another product or suite of products to an already challenging networking environment is more daunting than a lot of people would like to admit.

Often, organizations attempt to deploy disparate security components because they can't find a vendor capable of providing a complete solution. The result is often a partial, nonintegrated solution that is complex to deploy and difficult to maintain, and lacks good visibility into what is happening across the network.

A vast majority of the survey respondents acknowledge that it is vital for zero-trust security solutions to be integrated with their infrastructure, work across cloud and on-premises environments, and be secure at the application layer.

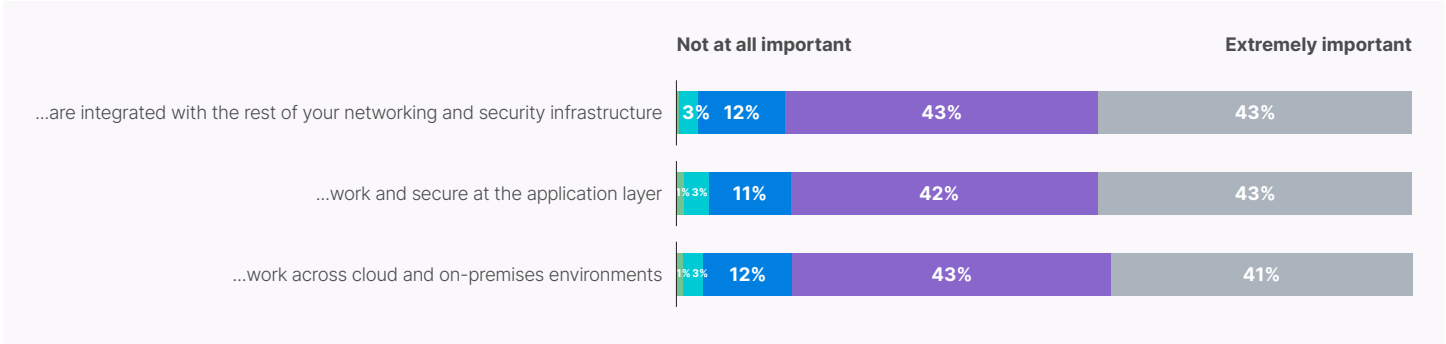


Figure 10: Importance that zero-trust strategy consists of security solutions that ...

Yet even with the knowledge that they need such integration, the most prominent challenge organizations report facing in building a zero-trust strategy is the lack of qualified vendors with a complete solution.

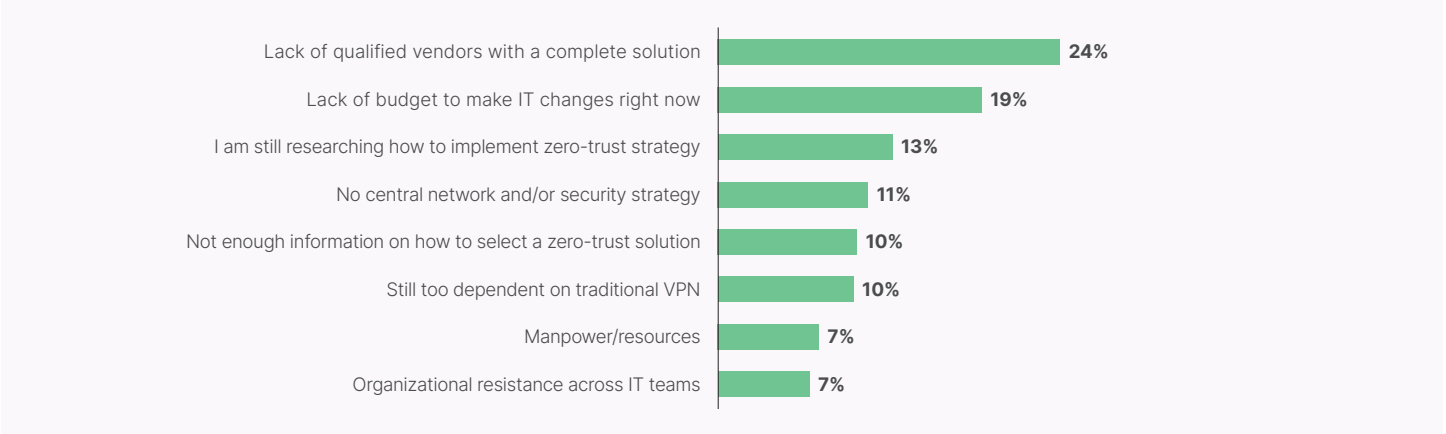


Figure 11: Most significant challenge building zero-trust strategy.

Conclusion

Although organizations report they are working on implementing zero trust, given the reported gaps in implementation, these efforts aren't as seamless or easy as some vendors might make it sound.

A proper zero-trust solution is all about knowing exactly who and what is on the network at any given moment and that authenticated users and devices are only provided with the minimum level of access for them to do their job. So, when organizations report that they aren't able to authenticate users and devices on an ongoing basis and struggle to monitor users for authentication, zero trust isn't doing its job.

Authentication, access control, and user identity are all critical elements of zero trust. To understand what's on the network, organizations should be using network access control (NAC) to discover and identify each device on or seeking access to the network and ensure that it hasn't already been compromised.

User identity is another cornerstone of zero trust. Like devices, every user needs to be identified. Authentication, authorization, and account (AAA) services, access management, and single sign-on (SSO) are used to identify and apply appropriate user access policies based on their role within the organization. Access should be combined with things like microsegmentation to maintain control of where a user can go in the network, and users and devices should be continually monitored to ensure they comply with policies. And those controls need to be applied uniformly at any place in the network and move seamlessly between network environments.

An effective zero-trust solution should address all of these tasks, and if it can't, organizations may want to rethink their zero-trust strategies and products. Complete, integrated solutions exist for implementing zero trust across the entire network, including cloud and on-premises.

Building an ad hoc solution using disparate security tools can create security gaps and management and configuration issues. On the other hand, a unified platform-based solution—with security controls that are seamlessly integrated and consolidated management, orchestration, and reporting tools—can reduce the overhead associated with deployment, configuration, and troubleshooting.

An effective zero-trust solution requires elements designed to work together as an integrated system to prevent the security and management gaps that have created challenges for survey respondents.

[1] "Verizon 2021 Data Breach Investigations Report," Verizon, 2021.

[2] "Cost of a Data Breach Report 2021," IBM and Ponemon Institute, July 2021.

[3] Mike Wronski, "Since Remote Work Isn't Going Away, Security Should Be the Focus," Dark Reading, September 24, 2020.

[4] "Global Threat Landscape Report," FortiGuard Labs, August 2020.

January 10, 2022 6:51 PM

1310666-0-0-EN