HOW TO AVOID TRADEOFFS BETWEEN SECURITY AND THE USER EXPERIENCE

A Global Survey of Executives and Security Professionals

June
2022

dimensional research

Sponsored by BROADCOM SOFTWARE

HOW TO AVOID TRADEOFFS BETWEEN SECURITY AND THE USER EXPERIENCE

A Global Survey of Executives and Security Professionals

Dimensional Research | June 2022

Introduction

This paper reviews key findings from a global primary research survey to understand how security is affecting the end user experience, productivity, and customer satisfaction. The study focused on learning how companies prioritize security versus productivity, and customer satisfaction. The research also investigated the adoption rate of Zero-Trust, SASE, and hybrid network security models as well as their impact on user experiences and visibility. The paper concludes by revealing what capabilities are needed to better measure the end-user experience and minimize the impact security has.

Executive Summary

This research finds that most companies are prioritizing security over all else, with a majority indicating security takes precedence over the user experience. 4 out of 10 companies also stated security is more important than end users' satisfaction and productivity. Thus, security is an obstacle to what companies need to do: be efficient, competitive, and please their customers. This is not lost on those within the companies where nearly half (46%) admit to bypassing security to improve the user experience, but it is also alarming for obvious reasons.

92% of security and technology professionals state the impact of security initiatives and solutions on the user experience must be measured and monitored. Hybrid workers and increasing utilization of cloud resources led 90% to state end-to-end paths for cloud-based applications must be monitored. Yet those surveyed point out that remote workers, 3rd party ISPs, and cloud resources directly limit visibility into the user experience. These challenges led to numerous requirements for user experience solutions, citing remote worker visibility, scalability, ease of deployment, robust integration, and more. More than 60% of the participants indicated it is very important for network security management and monitoring solutions to provide the information within the context of the full system (on-prem and cloud environments, applications, network, infrastructure, etc.).

Security is never stagnant. With most companies using hybrid environments, 83% reported they have a hybrid network security approach, leveraging both cloud and on-premises solutions. Rapid adoption of Zero-Trust (97%) and SASE (96%) further limits visibility into the user experience, state security and technology professionals. Yet 91% indicated that visibility into the end-user experience is critical to the successful adoption of SASE. New security initiatives and lack of visibility result in security being prioritized above all else, placing companies on a path to be 'securely' out of business. Security should not be at odds with customer satisfaction, productivity, or the user experience. As companies roll out Zero-Trust and SASE, they need to find complementary solutions that provide clear user visibility while still providing the security expected.

Key Findings

Companies Prioritize Security Above All Else but Capitulate, Creating Increased Business Risk

- 54% of companies have the philosophy that security is more important than the user experience
- 46% will impact productivity for the sake of increased security
- 44% are willing to impact customer satisfaction for increased security
- 46% admit they have bypassed security to improve user experiences

The Impact of Security on End-Users Must be Measured and Tracked by Increasing Visibility

- 92% state the impact of security solutions on user experience needs to be monitored
- 90% report end-to-end user access paths for cloud-based applications should be monitored
- Hybrid workers, 3rd party networks, and public clouds utilize technologies that inhibit end-user experience visibility
- 68% state it is very important to monitor network security within the context of the entire system

Zero-Trust and SASE Being Rapidly Adopted but Often Further Limit Visibility into the User Experience

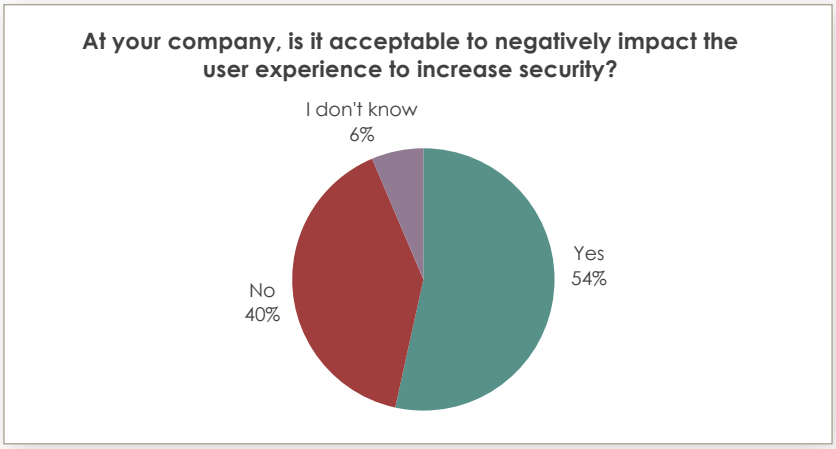
- 83% of companies employ a hybrid network security approach
- 97% will implement a zero-trust strategy, and 19% are already fully deployed
- 96% plan on utilizing SASE but adoption is just beginning with only 16% fully deployed
- 91% note that visibility into the end-user experience is key to adopting SASE

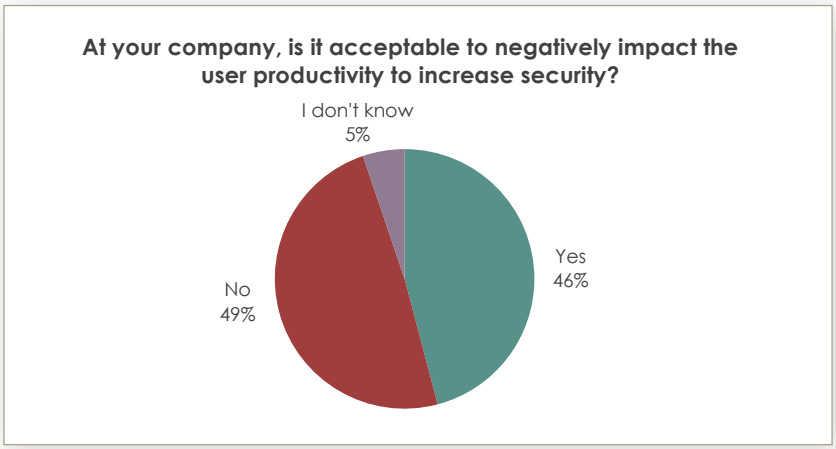
Detailed Findings

Companies Prioritizing Security Above All Else

It is not news that security has been the top initiative for years for IT organizations, thanks to an ever growing and changing threat landscape populated by increasingly sophisticated bad actors. But the traditional concept of a defense perimeter has also changed with the adaptation to hybrid workers and increasing reliance on cloud applications and resources. This research sought to understand where the balance is between the business and its need for security.

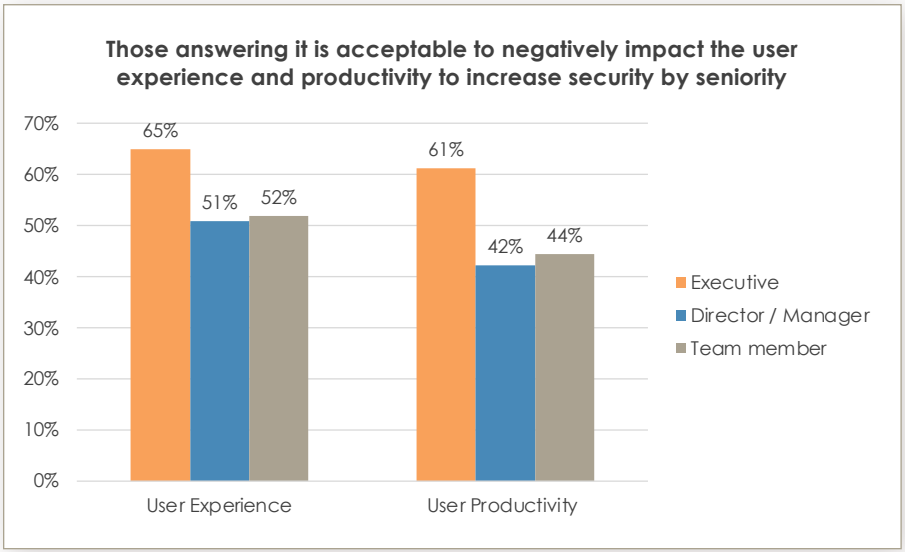
More than half of companies (54%) state it is ok to negatively affect the user experience for the sake of improved security. And nearly half (46%) admitted that it is acceptable to diminish user productivity to further increase security. It is key to acknowledge that the term "users" encompasses customers, employees, and partners. Thus, companies are today consciously losing employee productivity and making applications and services more frustrating to use for the sake of security. Applications and services that are difficult to use often result in customers leaving to find easier to use solutions, thus companies may be trading customers for increased security.





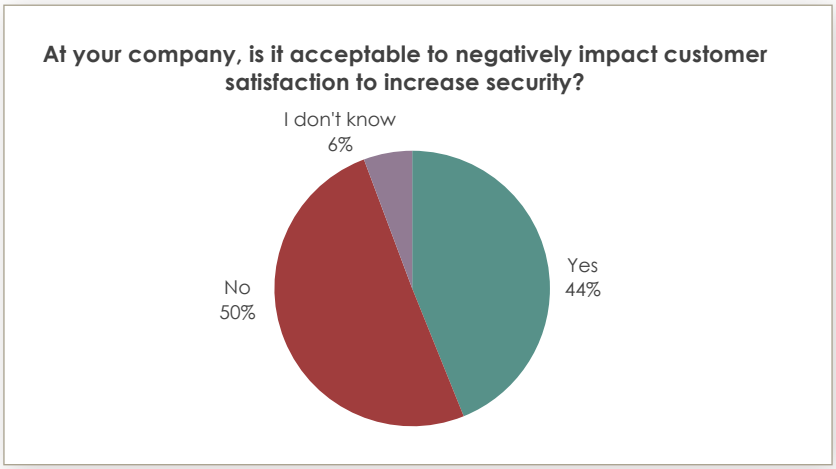
Executives Heavily Focused on Security, Driving Significant Business Tradeoffs

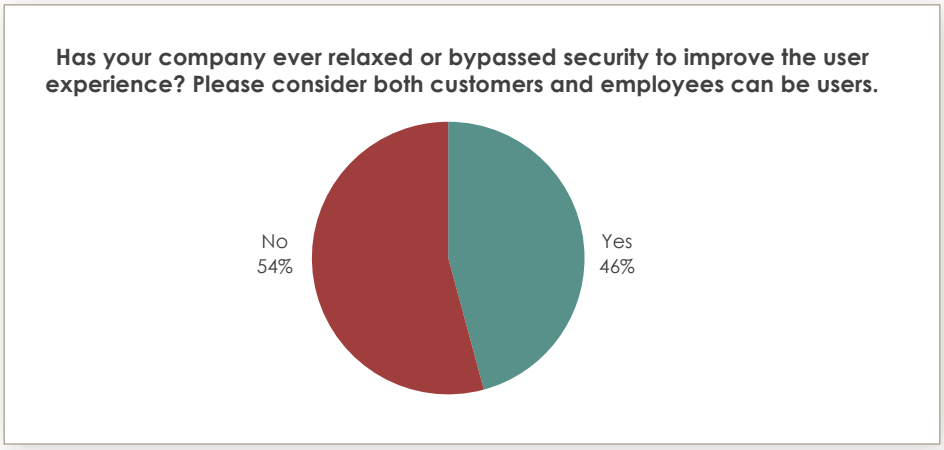
It would be easy to construe the findings of a reckless focus on security as attributed to just the security team, or those on the front-line just doing their job without considering the consequences. But when the data was analyzed and broken out by seniority a critical finding surfaced. Executives led all other roles by a wide margin in stating it is acceptable to sacrifice user experience and productivity to increase security. This suggests decisions about security and its impact on customer satisfaction are happening at the highest levels within the business.



Security More Important than Customer Satisfaction

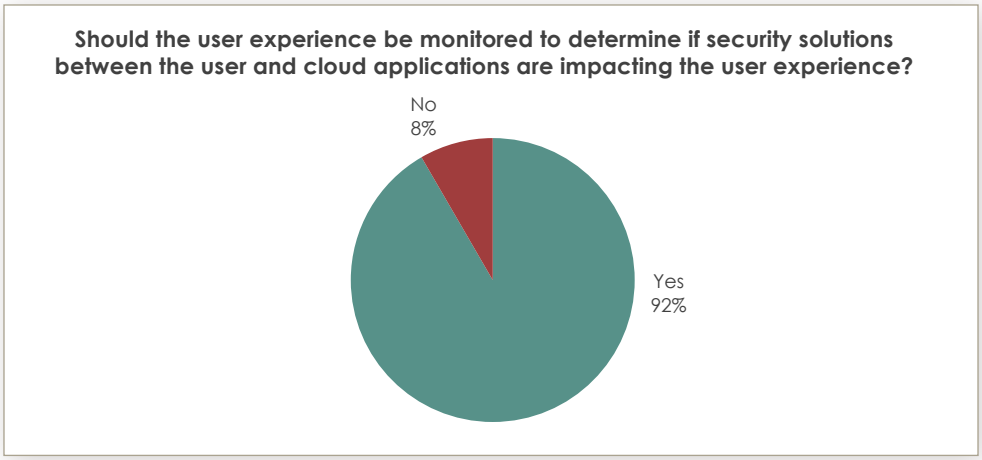
To clarify the preceding findings, participants were asked specifically if it is acceptable to negatively impact customer satisfaction for increased security. 44% said yes. This data continues to reinforce that security is a priority above all else for the business, at the expense of the customer. From a business perspective this seems like an insane tradeoff to literally impede your business for more security. It seems this tradeoff was not lost on those within the company where nearly half (46%) stated their company has actually bypassed security to increase the user experience. It is perplexing that companies are employing this security approach, consciously impacting user experiences, productivity, and customer satisfaction, to then put the security strategy at risk by deciding they may have gone too far.



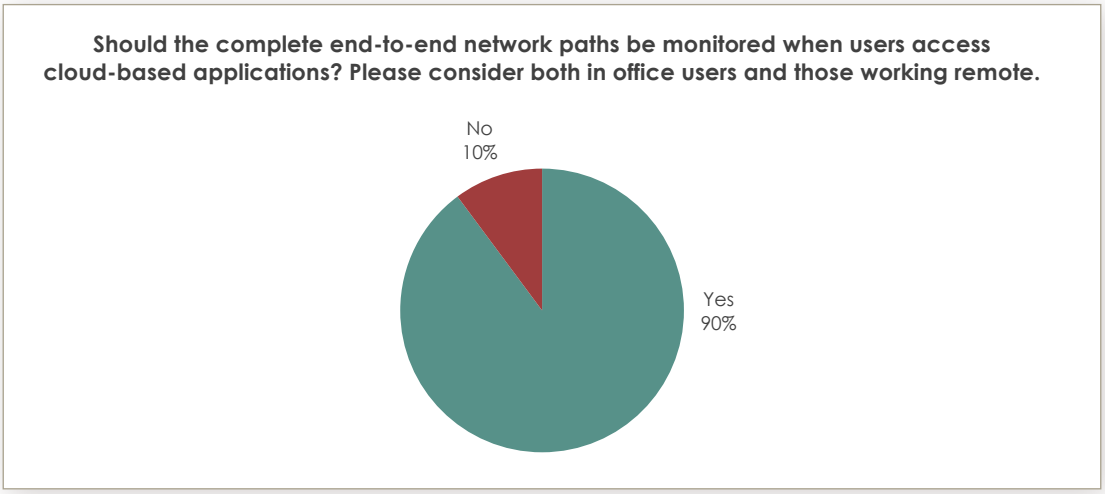


Impact of Security Solutions on the User Experience Must be Monitored

The research then focused on understating the connection between the security solutions and end user experience. In order to understand how a security solution affects users, it needs to be measured. 92% of security and technology professionals agree that user experience needs to be monitored in order to determine the exact effect a security initiative has on the user, productivity, and customer.

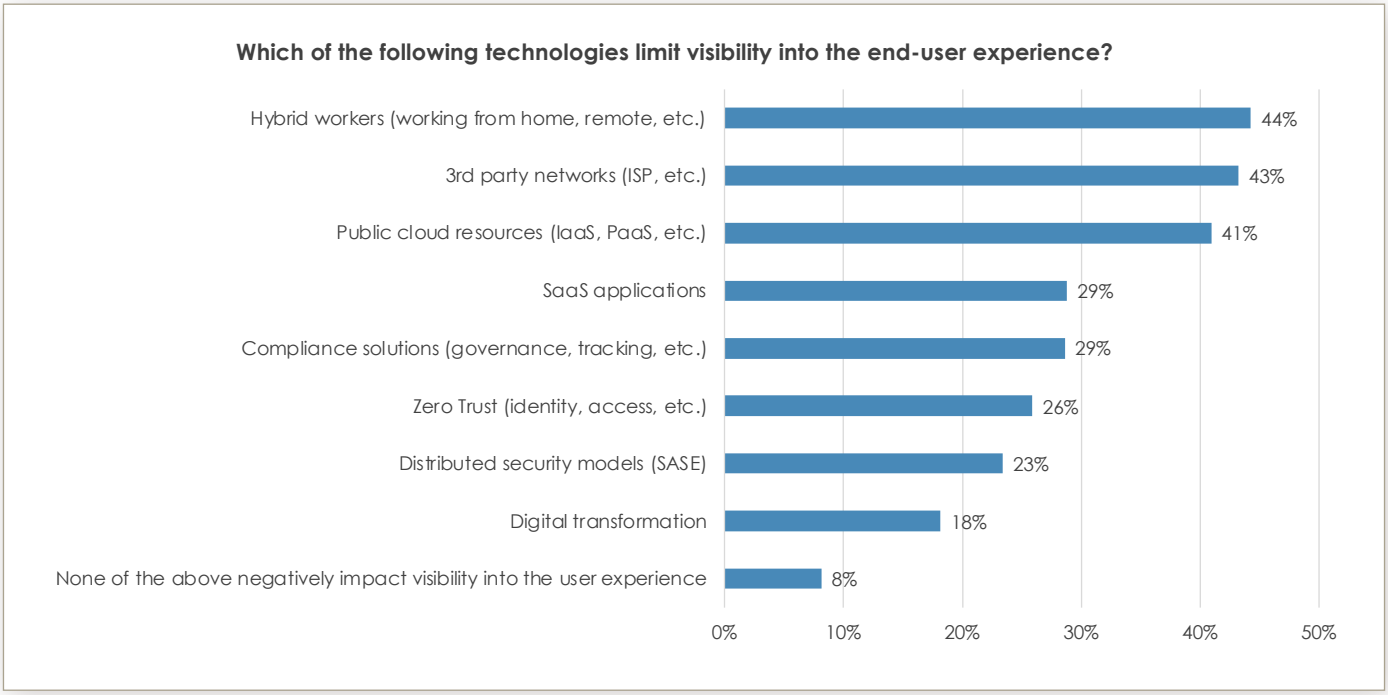


To build a complete view of the user experience, 90% of those surveyed indicated the entire end-to-end path needs to be monitored when using cloud-based applications. This makes sense in the era of hybrid workers but can be more difficult than expected with the use of a VPN, where the connection to the cloud-based application is not direct but actually routes from their location or work network via the VPN and then back out to the internet and ultimately the cloud-based application. The complicated network path adds opportunity for issues of both security risks and impact to the user experience, driving the need for visibility, measurement, and monitoring.



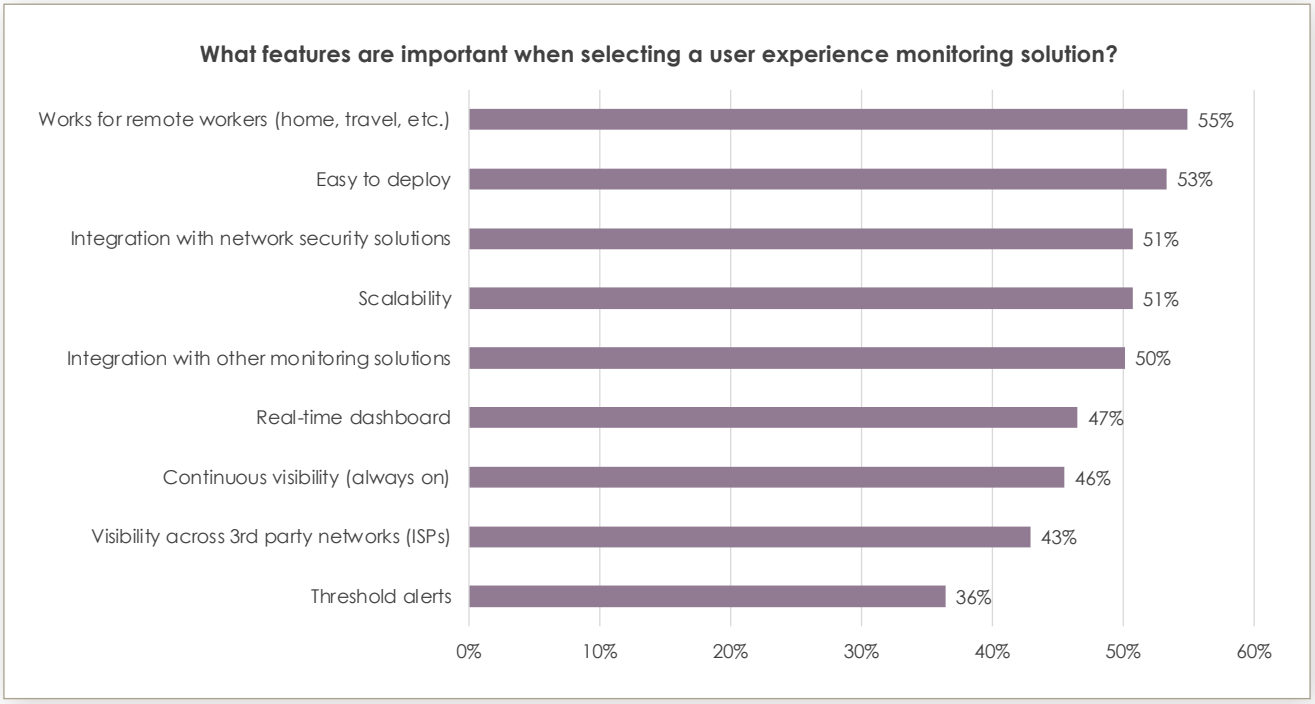
New Technologies Inhibit End-User Experience Visibility

Full visibility into the user experience is becoming more challenging, with the top 3 drivers being hybrid workers (44%), 3rd-party networks and ISPs (43%), and public cloud resources (41%). This provides even more evidence why the end-to-end path for cloud based applications discussed previously is so important. But newer security initiatives such as Zero-Trust (26%) and SASE (23%) also contribute to obscuring the visibility into the user experience and continuing to fuel the tradeoff between increased security and user impact.



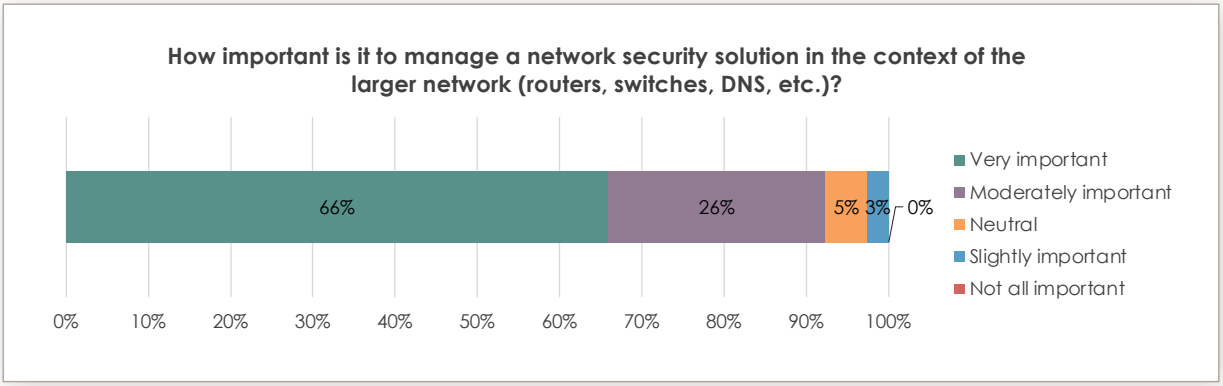
User Experience Monitoring Solutions Require New Capabilities

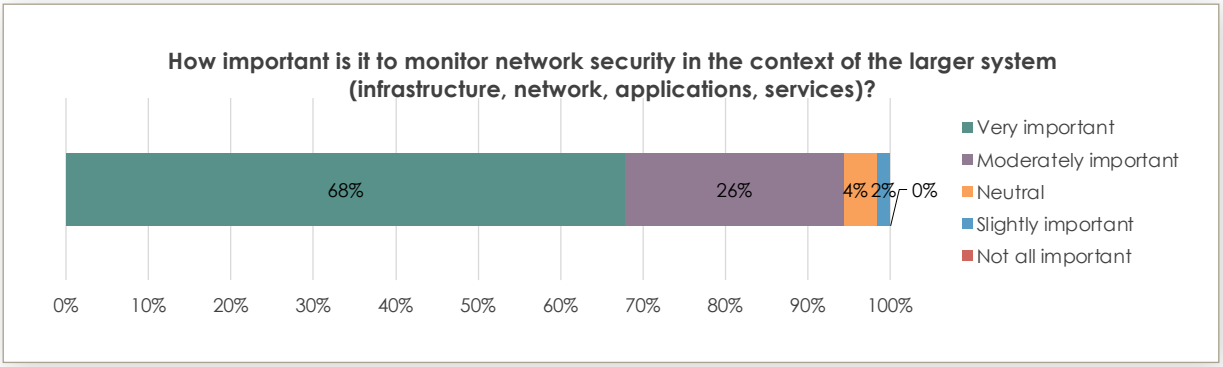
With numerous technologies and hybrid worker trends diminishing user experience visibility, participants were asked what features are required for a modern user experience monitoring solution. Not surprisingly, the ability to monitor users when working remotely (55%) tops the list of needed capabilities. The solution has to be easy to deploy (53%) and integrate with network security solutions (51%) to not create new security vulnerabilities itself. With companies employing thousands or tens of thousands of employees, it is easy to see why scalability (51%) is tied at the 3rd spot. User experience monitoring needs to integrate with other monitoring solutions (50%) and provide that single pane of glass, real-time dashboard (47%). The visibility needs to be continuous (46%) and extend across 3rd party networks (43%) which were reported to be directly obscuring visibility today. At the bottom, but perhaps the most interesting, is the ability to set threshold alerts (36%). While it has been around for decades for servers, networks, applications, and services, it is a newer concept that the user experience should have a threshold, and someone should be alerted when it has been crossed.



Network Security Requires Full System Context

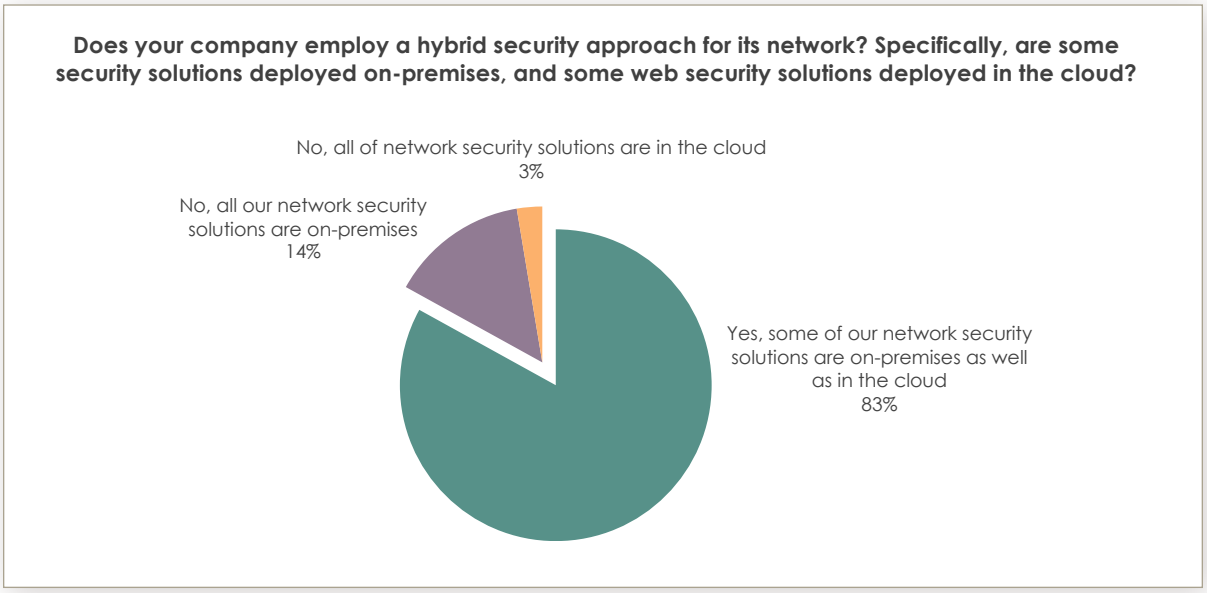
Context was added to the concept of visibility, when participants were asked about network security. 66% responded it is very important that network security solutions have the full context of the larger network. And by a similar margin, 68% also stated it is very important to have the context of the larger system such as other infra-structure, applications, and services. This underscores that network security is not just a point-to-point issue or centered around a single application or service, but must be managed holistically.





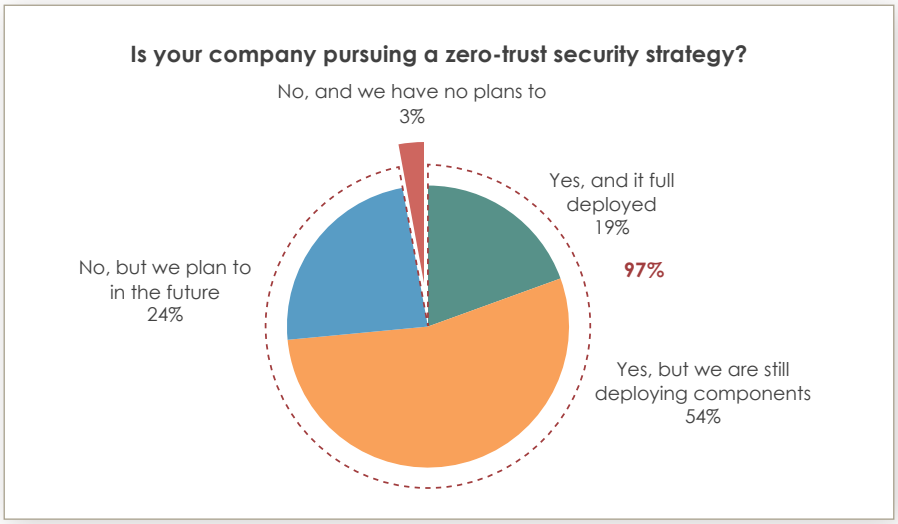
Most Companies Employ a Hybrid Network Security Approach

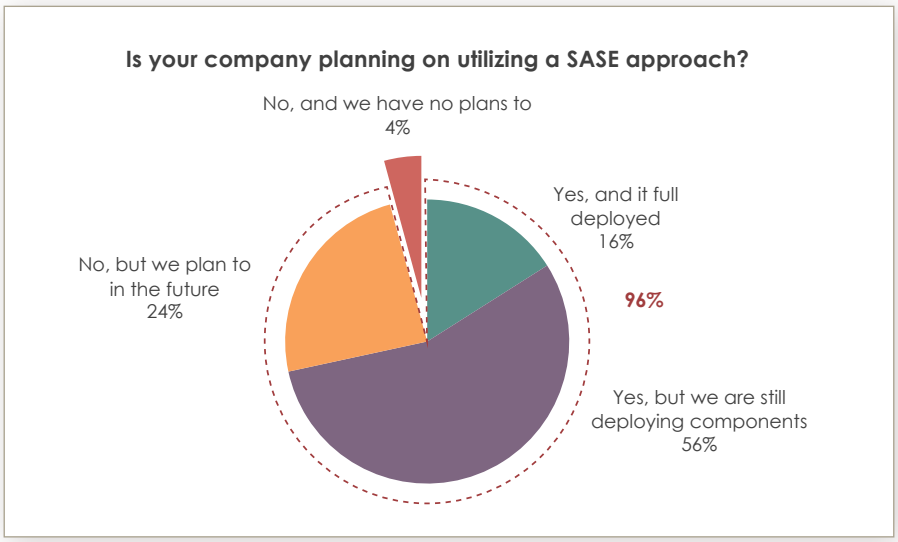
The cloud has been a boon for developers and hosting applications and recently a critical option to enable hybrid-workers. However, the research sought to understand if companies were actually leveraging security solutions that were hosted in the cloud to form a hybrid network security strategy. 83% of companies today are already utilizing a hybrid network security approach, collectively utilizing both on-premises and cloud-based solutions. Only 14% of companies remain reliant on an on-premises network security philosophy.



SASE and Zero-Trust Being Aggressively Adopted

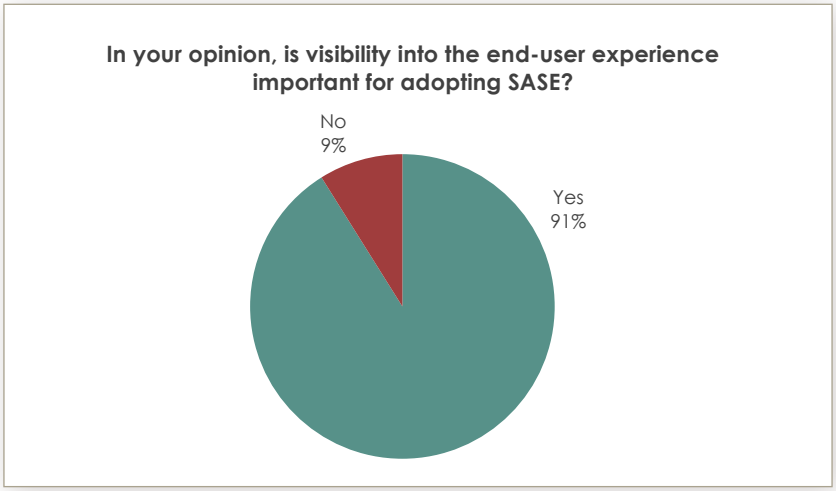
Earlier in the report it was discussed that Zero-Trust and SASE are inhibiting visibility into the user experience. In an attempt to understand how pervasive those strategies are, participants were asked where their company is on the adoption curve. 97% of companies are planning on deploying Zero-Trust, with 19% fully deployed and another 54% already underway. Similar findings occurred for SASE where 96% plan to utilize that approach with 16% fully deployed and 56% more still rolling out components. This aggressive adoption indicates growing user experience visibility issues.





SASE Adoption Requires Visibility into the User Experience

This research indicates that currently security and end-user experience don't go hand in hand and typically are not managed by the same team. However, when security professionals and executives were asked, 91% stated that having visibility into the user-experience is key for successfully adopting SASE. This directly indicates security professionals know SASE impacting users is occurring and would like more information to better understand how.



Conclusion

The reality today is that companies and their executives are consciously making tradeoffs against user experiences, productivity, and even customer satisfaction for increased security. But the data suggests they go too far to the extent that they disable some security controls to regain productivity and improve user experiences. This indicates a disconnect in information and the inability to truly understand how a new security solution, initiative, or approach will affect the users, and thus the business.

Hybrid-workers, 3rd party networks, and public cloud resources provide even more barriers to understanding the user experiences. Add in new security initiatives such as SASE and Zero-Trust that are being rapidly adopted but further obscure the view into the user experience, and this means the situation is getting worse.

What executives really need is empirical data to make an informed decision, to understand how exactly a security solution impacts the user experience and productivity. Then the business impact can be weighed against security risk and rational business decisions can be made. Security professionals need this information to perhaps find a configuration or implementation that doesn't impact the user experience and relieves executives from these difficult tradeoffs.

The end user experience needs to be constantly monitored to measure the impact of new deployments, changes, or issues. A baseline or threshold should be set, and as the research participants indicated, perhaps a user experience monitoring system with an alert function would be a good thing to help everyone know when their security solutions have gone a bit too far and put the business at risk.

Survey Methodology

Security and technology professionals at enterprise companies representing all seniority levels were invited to participate in a survey on their company's security practices. Participants were selected at random from an independent market resource. The survey was administered electronically, and participants were offered a token compensation for their participation.

A total of **503 qualified participants** completed the survey. All participants had enterprise security responsibilities from numerous industries. Participants were from 5 continents, providing a global perspective.

About Dimensional Research

Dimensional Research provides practical marketing research to help technology companies make their customers more successful. Our researchers are experts in the people, processes, and technology of corporate IT and understand how IT organizations operate. We partner with our clients to deliver actionable information that reduces risks, increases customer satisfaction, and grows the business.

For more information, visit www.dimensionalresearch.com.

About Broadcom

Broadcom Software is a world leader in business-critical software, delivering category-leading solutions with unmatched scale.

The Broadcom Software portfolio includes intelligent software solutions in infrastructure and security. Solutions from our CA Technologies and Symantec portfolios, and recently acquired AppNeta help companies worldwide transform their businesses.

Specifically, the portfolio spans AIOps, AppNeta, Cyber Security, Value Stream Management, DevOps, Mainframe, and Payment Security.

For more information, go to https://software.broadcom.com.