SPONSORED CONTENT | WHITE PAPER

Market Pulse

Why the SASE approach to network and security is the answer to **combatting sophisticated cyberattacks**

Research reveals only 28% of companies think their security is robust, as data shows IT leaders increasingly perceive the SASE methodology as the right approach.

CIO

SPONSORED BY paloalto NETWORKS | accenture

Market Pulse

An exclusive survey conducted by Foundry on behalf of Palo Alto Networks and Accenture of 207 companies across North America,the UK, Germany, and France has found that boosting IT and data security was their top priority for 2023 - with Secure Access Services Edge (SASE) being their preferred method.

As the nature of how and where we work continues to evolve, an increasing number of organizations are adopting cloud security and networking solutions to be more efficient, improve their customer experience, and deliver a seamless experience.

While remote work implies the enterprise perimeter is now "everywhere," this creates new and expanded vulnerability vectors for potential cyber attacks. At the same time, enterprises also understand that they must embrace Zero Trust principles to protect their networks, applications, and data - but many questions remain regarding how to implement these principles.

Current networking and security approaches are too rigid and siloed to keep up with the rapidly evolving pace of change experienced by today's hybrid organizations and their hybrid workforces. What has served the needs of businesses in the past is now often no longer a fit for the future.

Traditional hub-and-spoke architectures with disparate network and security stacks don't scale well for hybrid work and cloud. Taking application workloads back to increasingly distant corporate data centers creates significant application performance issues unsuitable to modern employee and customer experience expectations. Additionally, inconsistent policies and capabilities that depend on a user's physical location create inherent gaps in security, challenging IT teams' ability to keep up with digital transformation and stay ahead of cyber threats.

Converging networking and security into a cloud-delivered model promises to remedy many of the shortcomings of traditional approaches, helps to improve business productivity and performance while establishing cloud security as a fundamental success driver for enterprises.

Although cloud-based security solutions exist to address digital transformation challenges, the research uncovered that IT leaders found certain aspects of these available solutions in need of clarification, particularly with regard to the differences between various security approaches.

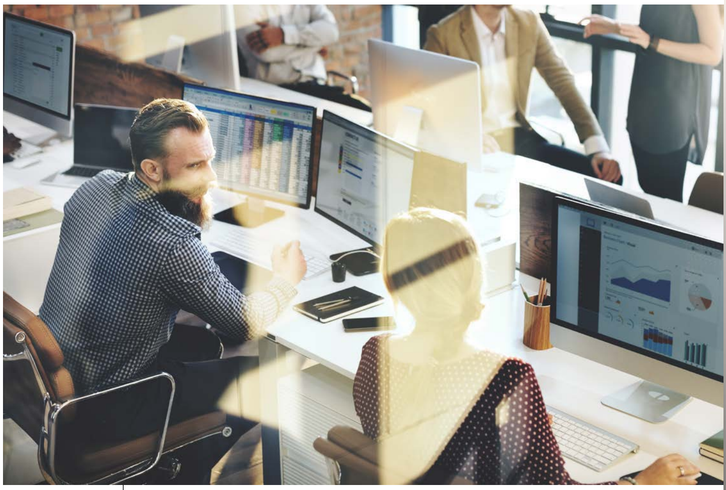


PHOTO BY RAWPIXEL.COM

Security challenges are driving the need for modernized technology

Hybrid work has become what most now refer to as the new normal and a requirement for many organizations. The pandemic forced organizations to adopt new systems and methods of operation almost overnight. Despite this, the research found that just 25% of those surveyed felt like their digital infrastructure had been transformed, indicating a lag between where organizations need to be — and where they actually are.

A growing number of employees today use their personal IT equipment and require access to secured systems while working remotely. Unfortunately, this has created new attack vectors and vulnerabilities in the least controlled areas within legacy access architectures. And this trend has not gone unnoticed by IT leaders, with only 11% of those surveyed feeling their security was "perfect."

Compounding this challenge is cloud networking, which organizations are increasingly using. According to the survey, 92% of businesses use public cloud networks, and 62% use private cloud. Hybrid cloud was used by 55% of users, and multicloud by 44%. As work continues to move outside of our traditional offices and into the comfort of our respective environments, the threat of cyber risk significantly increases.

Martin Glowik, managing director for Accenture Security, says, "Remote work moves workers outside the traditional office network boundaries, re-exposing them to attack vectors traditionally handled by office access networks. They are accessing vital corporate secrets through an increasing variety of unsecured and potentially compromised access vectors such as homes, cafes, airports, etc.”

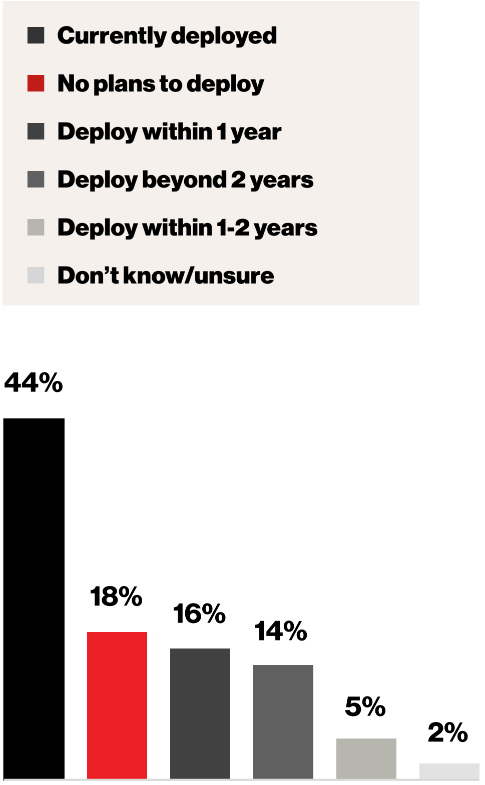
An ever-evolving threat landscape

Cybercriminals constantly find new, more sophisticated ways to infiltrate networks, ranging from malware and phishing attacks to ransomware and data breaches. In fact, the number of cyber attacks soared by 38% last year[1], costing businesses worldwide $8.4 trillion in 2022[2]. This concern plays a significant role in the financial sector, with 74% of financial institutions saying they had experienced at least one ransomware attack over the past year.[3]

The survey showed IT leaders across all industry sectors are aware of these threats, with 53% planning to increase spending on SASE in the coming year. It’s important to note that SASE was amongst the most widely deployed solutions (44%), underlining its growing popularity among security experts.

Even with increased awareness and a plan to increase spend and combat these threats, market complexity remains a concern for many IT leaders. For example, organizations lack an understanding of the benefits of an integrated solution over best of breed. Only 14% of respondents thought these benefits were highly differentiated or distinct. Organizations need better clarity on the security solutions available to them to make informed decisions that produce better business outcomes and keep them one step ahead of cybercriminals.

Figure 1 | SASE plans



SOURCE: FOUNDRY

These findings paint a picture of businesses that are all too aware of the present threats, yet are unclear on how to address them.

Traditional security architectures continue to be a problem

Legacy architectures struggle to meet the demands of businesses and remote workers as digital transformation, hybrid workplace, and hybrid cloud transformation continue to evolve. Moreover, various working locations (home or office) can be subject to different policies and security capabilities, depending on which security features, such as firewalls, are installed in that specific location.

Additionally, traditional security systems also introduce significant latency, delivering an unpleasant user experience while being less operationally efficient.

In a 2022 survey conducted by Censuswide[4], 49.4% of UK respondents said that their organization relies on primary backup and recovery infrastructure designed in, or before, 2010. Of that group, 27% claimed to be using technology designed either between 2000-2005 or in the 1990s.

These old systems are becoming progressively harder to change and no longer provide adequate support for expanding business operations.

To address this, security policies should be applied to all users consistently, with consistent verification across data center, cloud and software as a service (SaaS) application estates.

Driving optimal performance with SASE

Increased use of SaaS applications, hybrid work, and cloud adoption has changed how employees leverage networking and security solutions, creating greater threat vectors, performance latency, and inconsistent user experience. For this reason, organizations are adopting SASE to streamline and secure their digital infrastructure.

SASE combines best-of-breed networking and security like cloud access security broker (CASB), firewall as a service (FWaaS), Cloud SWG and Zero Trust into a unified solution built for agile, cloud-enabled organizations while helping ensure an exceptional experience for users. A SASE architecture identifies users and devices, applies policy-based security, and delivers secure access to the appropriate application or data. This approach allows organizations to apply secure access no matter where their users, applications, or devices are located.

According to Yogesh Ranade, senior director of product management at Palo Alto Networks, “With next generation firewall [NGFW], the access has to be from on premises. SASE provides a global footprint where users can access public and private resources from any location yet get the same level of security. SASE has similar — or better — capabilities to NGFW but is cloud-delivered. Prisma SASE provides the same cloud-based protection for mobile users and remote branch offices.”

In fact, participants of the survey stated that the top two reasons for adopting SASE were optimized performance (18%) and increased effectiveness of IT staff (15%). This supports the notion that security optimization across an evolving digital work landscape improves business efficiency and overall organizational productivity.

Additionally, SASE helps organizations streamline and secure their digital infrastructure with consistent security capabilities implemented across their entire ecosystem.

Glowik also asserts “SASE provides a holistic new architecture that utilizes advances in architectural security capabilities to provide a higher, integrated level of security. SASE moves security out of the traditional data center and office domains and pushes next-generation security functions to the edge of the new cloud and SaaS edges.”

As SASE continues to evolve, it is becoming the preferred security solution for organizations looking to solve their IT challenges.

Ranade adds, “IT leaders now realize that SASE is more than just a consumption model for networking and security services. It’s an architectural approach that enables organizations to seamlessly and securely enable the future of work.”

Not all SASE solutions are created equal

Some SASE solutions, such as Palo Alto Networks Prisma SASE, have artificial intelligence (AI) and machine learning (ML) based threat detection, enabling organizations to combat new threats and zero-day vulnerabilities efficiently and effectively. By implementing AI-based problem detection and predictive analytics, organizations can automate complex IT operations, increase productivity, and provide consistent Zero Trust security outcomes everywhere.

According to Glowik, “Prisma SASE drives Zero Trust principles by con-

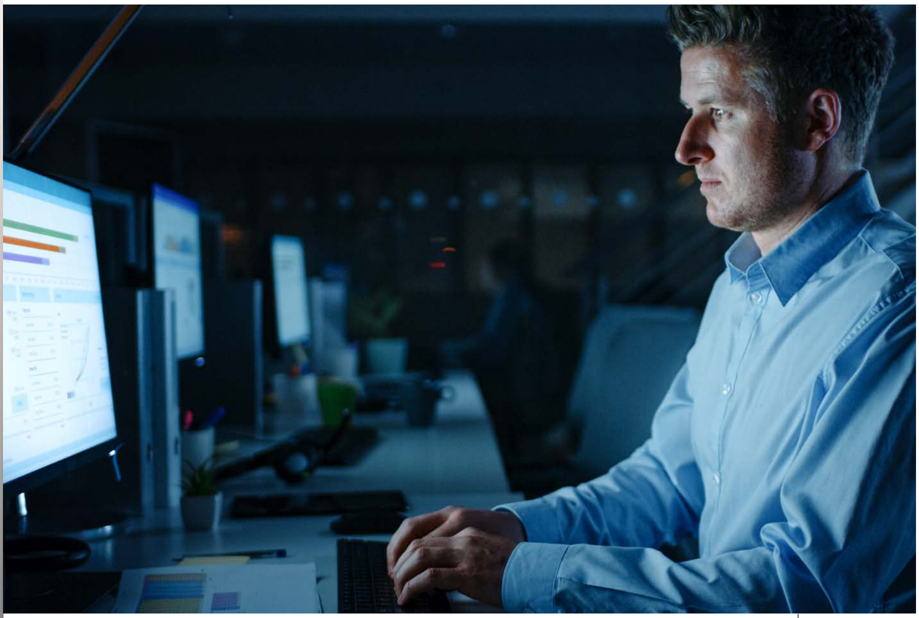


PHOTO BY GORODENKOFF

Market Pulse

tinuously assessing identity and authorizations versus real-time risk profiles. It can assess the validity of the identity, state of the end device, and sensitivity of applications and data being accessed to realize the promise of Zero Trust architectures."

Ranade adds, "Organizations need a solution that safeguards their workforce wherever they are. Most SASE solutions available today are disjointed and incomplete. A solution like Prima SASE gives organizations unique benefits, including superior ZTNA 2.0 security, unified security products, and exceptional user experiences. With a ZTNA 2.0 integrated solution, organizations gain least-privileged access with continuous trust verification, and deep, ongoing security inspection to protect users, devices, apps, and data everywhere — all from a single platform."

International differences in a SASE adoption

The survey discovered several differences in the SASE adoption rate between North American and European organizations. We asked participants about median deployment timeline statistics. When asked, "Does your organization currently have an integrated SASE?" or "When does your organization plan to deploy SASE?" European participants responded that they would do so within the next six months, whereas participants in North America answered that they had already done so. Furthermore, 58% of European businesses expect to increase investment in SASE this year, compared to 49% in North America, which have SASE in place. In general, this disparity could be partly explained due to differences in SASE maturity between the two regions.

Why an integrated SASE solution works best

In the past, organizations frequently resorted to best-of-breed point solutions to solve their security networking challenges. To better understand, best of breed implies taking a piecemeal approach to security by onboarding specialized technologies to address specific disparate security challenges. While this technique may have worked for some organizations, it is not the most efficient for many and leads to an overly complex environment.

Because of this, an integrated SASE solution is the most effective, as it offers a single-vendor platform approach that addresses the entire attack surface. This ensures a more consistent policy while providing organizations with a comprehensive understanding of what's happening in the network. With an integrated SASE solution, organizations have one platform to manage and monitor all security capabilities, a single policy to secure all traffic, a single application programming interface gateway for automation, and a single place to manage identity and access management and role-based access control.

As perceived benefits of an integrated approach, IT decision-makers cited greater agility (42%), lower cost (41%), reduced complexity (39%), threat prioritization (39%), and improved security (37%). More evidence that IT leaders are embracing integration as their preferred option. Glowik notes, "Adopting SASE is just one step in effecting network transformation to meet the modern cloud, SaaS, IOT [internet of things], and other emerging technology and workload evolutions. Ensuring that new access architectures are operationalized to meet today's requirements and integrated into other security systems of record while also evolving the platform for future needs is critical to realizing the expected value and managing risks."

In addition to the countless advantages organizations receive from an integrated SASE solution is the reduced cybersecurity skills gap obtained through the single-pane management and automation built into Prisma SASE. This enables organizations to concentrate on their workforce while prioritizing fewer critical threat events rather than allocating efforts to maintain brittle legacy integrations.

How best to adopt SASE

Organizations considering SASE can benefit significantly by planning their rollout and leveraging the professional services of experienced cybersecurity experts.

In the context of SASE deployment methodology, every organization is unique. While some companies fully embrace SASE and proactively embark on their journey with a "do it yourself" model, others prefer using a managed service provider (MSP). Engaging an MSP in the journey toward SASE can offer benefits in planning, implementing, and operating these solutions. In fact, more than half of survey respondents (52%) considered engaging an MSP for rolling out SASE. But fewer than half (44%) said they would want their internet service provider to also be their SASE MSP.

"While SASE is easy to deploy, to realize the benefits and operationalize new network capabilities, strategic planning and experienced operationalization is required" says Glowik. "Through managed services models, the burden of operationalization and evolution, as corporate needs evolve, can be met on a scalable basis. Managed services change the cost structure from a significant up-front outlay to a consumption model that scales with business needs," he adds.

Ranade also says, "Companies need to understand the use cases, access methods, key applications (public and private), security posture or requirements, and traffic flows. Then they need to map the features or functionality required from the SASE platform. They can get design and deployment assistance through Palo Alto Networks professional services."

SASE is the way ahead

SASE creates a concrete step toward achieving the benefits of Zero Trust. The survey ultimately demonstrated why SASE is increasingly at the forefront of the agenda for security leaders as the methodology evolves from an early-stage concept to a cornerstone of modern security strategy. Today, organizations have either adopted SASE or are planning to deploy it in a relatively short time frame.

An integrated SASE solution represents an opportunity to free organizations from the complexities and limitations of legacy hardware-based, data center-centric architectures. By removing the barriers to digital transformation, SASE increases the rate at which organizations can empower their hybrid workforces. SASE allows you to move on to cloud initiatives and transform branch offices, enabling you to respond to rapid change.

As an added benefit, SASE provides a concrete opportunity to improve the effectiveness of a hybrid workforce, cut costs, and improve efficiency, presenting a return on investment of up to 270%, according to Forrester Research.[5]

In summary, getting the most from SASE requires the right expertise and an integrated solution provided by a single vendor. By harnessing industry-leading networking and security capabilities, enterprises can leverage the advantage of a solution that offers the superiority of ZTNA 2.0, simplified operations, and an exceptional user experience. Together, Accenture and Palo Alto Networks provide an easy footpath for customers as they embark on their SASE digital transformation journey. ◆

[1] Digit News "New Data Reveals 77% Increase in UK Cyber-attacks in 2022," January 2023, https://www.digit.fyi/38-increase-in-2022-global-cyber-attacks/

[2] Statistica, "Estimate cost from cybersecurity Worldwide 2017-2028," June 2023, https://www.statista.com/statistics/1280009/cost-cybercrime-worldwide/

[3] Financial Times, "The financial system is alarmingly vulnerable to cyber attack," February 2023, https://www.ft.com/content/03507666-aad7-4dc3-a836-658750b880ce

[4] Cyber Magazine, "Reliance on legacy technology is damaging businesses," September 2022, https://cybermagazine.com/articles/reliance-on-legacy-technology-tech-undermining-how-organisa

[5] Palo Alto Blog, "What is the ROI of SASE?" August 2022, https://www.paloaltonetworks.com/blog/sase/what-is-the-roi-of-sase/

Discover **what makes a comprehensive, integrated SASE solution the right approach for your organization.**

CIO

© 2023 IDG Communications, Inc.