SPOTLIGHT
Sponsored by Broadcom

Secure service edge (SSE) is an emerging security technology for enabling secure worker access regardless of location.

Security Transformation: Enabling Remote Work and Modern Business Practices

November 2022

Written by: Christopher Rodriguez, Research Director

Introduction

Data breaches continue to make headlines in 2022 as cybercriminals discover new methods of evading outdated defenses or exploit new threat vectors introduced by emerging technologies. While there is little incentive for cybercriminals to slow their efforts, businesses are equally unlikely to eschew adoption of new technologies given that they offer improvements in efficiency, productivity, and user experience and help accelerate overall business growth. Unfortunately, security considerations are often a secondary concern throughout this process.

According to IDC surveys, digital transformation (DX) strategies have been a top investment priority for businesses in recent years. Organizations adopt transformation to accelerate time to market or to improve customer experiences, among other reasons. In 2020, the importance of DX strategies became apparent to businesses around the world as a sudden shift to work-from-home (WFH) models introduced unexpected logistical challenges. For one in four organizations, DX initiatives were key to navigate these challenges, according to IDC's *Future Enterprise Resiliency and Spending Survey, Wave 11* (December 2021). But many organizations were not prepared — roughly 34% were forced to adopt a digital-first strategy in response to pandemic disruptions. For many others, the disruptions were a wake-up call about the need for digital-first strategies as an investment in future business resiliency. Business leaders have since focused on learning from the challenges of that first migration effort to better operationalize and extend the benefits of remote work and hybrid business models.

However, network security architecture was a complicated maze of functionality and coverage long before the pandemic. Each new technology or threat vector generates the need for a specialized security tool. The result is an unmanageable sprawl of security products, services, consoles, agents, and data silos. This complexity leads to security gaps and wastes resources. The sudden migration to a remote workforce merely amplified familiar challenges, such as gaps in protection, inconsistent policy, unmanaged devices, excessive agent software, shadow IT, and inflexible VPN limitations.

AT A GLANCE

KEY STATS

When asked by IDC which work practices and technology emerging from the pandemic are the most likely to endure, 45% of respondents said that "remote and hybrid work models will be an embedded part of accepted work practices."

41% of organizations said they plan to "improve network bandwidth and security for remote and in-office workers" to enhance collaboration and communication.

Source: IDC's *Future Enterprise Resiliency and Spending Survey, Wave 11,* December 2021, n = 858

The underlying challenge is that the traditional approach to network security is outdated and forces a trade-off between convenience and security. This trade-off is untenable in the modern digital-first era. Enterprise security architecture must be adapted to the modern requirements of an "anywhere-anytime-any device" workplace and other complexities resulting from digital transformation. Notably, IDC finds that this is not a check-the-box exercise. This objective requires complete protection that is powerful, pervasive, and compatible with the modern expectations of a digitally transformed user experience, whether a worker is in the office or not.

Security Modernization Enables Emerging Business Practices

The COVID-19 pandemic propelled the trend toward a democratization of IT. Prior to the pandemic era lockdowns, workers had increasingly demonstrated a willingness to utilize any device — and cloud applications of their choosing — to work anywhere and anytime. As pandemic restrictions loosened through 2021, and workers returned to the office, these newly formed expectations remained. Workers have projects, deadlines, and goals — and they need to be able to work without restriction whether they occupy an office cubicle, a hotel room, or a home office. As a result, the concept of a defensible network perimeter has become antiquated. Rather than attempting to erect a static wall of access controls and defenses at a logical network perimeter, organizations must implement a network security architecture that can adapt to modern computing needs.

Secure service edge (SSE) is a new approach to modernize security for the demands of a digital-first world. SSE emphasizes the convergence of multiple network security technologies as a single cloud-delivered platform. It offers familiar benefits of consolidation such as fewer/simplified vendor relationships to manage across buying cycles, support, and accounting. With fewer interfaces, SSE requires less training time and offers faster time to proficiency. Cloud-delivered security offers the benefits of scalable, pervasive protection anywhere users require access.

Edge Security Enables Business Strategies

Integrated, edge-delivered security helps businesses adopt modern practices such as remote and hybrid work models. The demand for secure workforce access and enablement reached record levels during the pandemic. During this time, over half of organizations also noted an increase in productivity of up to 24%, although many noted greater productivity gains. Suffice to say, remote work is here to stay. IDC research shows that 45% of organizations expect remote and hybrid work models to remain an embedded part of accepted work practices post-pandemic.

However, remote work introduces new considerations. Business leaders noted the following plans for enabling remote work:

- 40.6% of enterprises are looking to enable collaboration and communication among the workforce.
- The top technology priority to enable this collaboration is "improved network bandwidth and security for remote and in-office workers," according to IDC's *Future Enterprise Resiliency and Spending Survey, Wave 11* (December 2021).

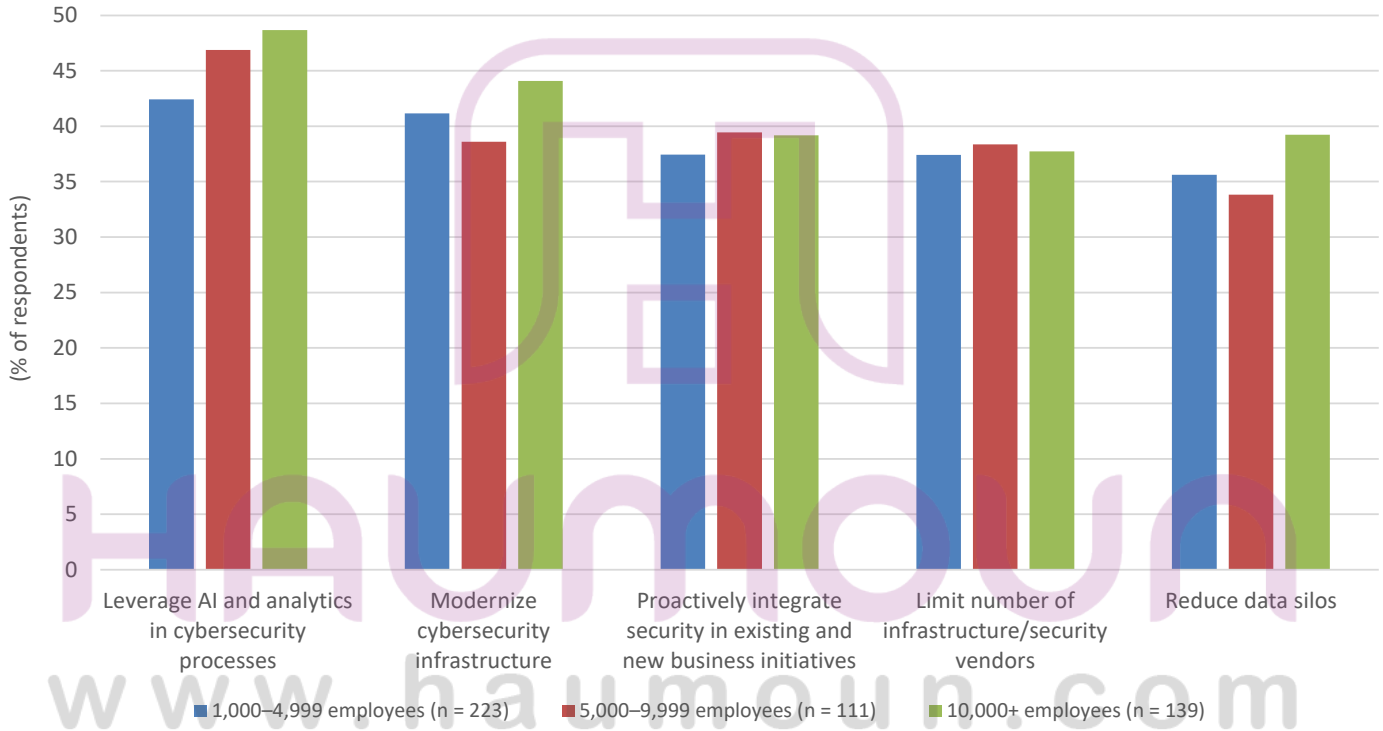
This last item indicates that business leaders are aware of the inseparable need for protection and a positive user experience. SSE solutions provide an inspection point that is as near to the end user as possible for low-latency communications. By comparison, legacy security tools required backhauling traffic to a central inspection point, which introduced latency or errors into the user experience.

Integrated Security for Better Protection

IDC research identified cybersecurity risk as a top priority for enterprise decision makers — 37.7% of enterprises expect "cybersecurity threats/regulations" to have the greatest impact on technology investment plans in coming years, according to IDC's *Future Enterprise Resiliency and Spending Survey, Wave 12* (January 2022). In response, 41.6% of organizations plan to modernize security infrastructure and 44.3% plan to leverage advanced analytics for security (see Figure 1).

FIGURE 1: ***Key Investment Priorities to Improve Security and Trust by Organization Size***

Q Specific to security in 2020 and 2021, in which of the following areas has your organization invested or does your organization plan to invest to improve organizational trust?



Source: IDC's Future of Trust Survey, February 2021

Unfortunately, pandemic-era approaches to secure remote access relied on legacy tooling that lacked scale or flexibility. By using an assortment of point products, security teams had to divide their attention and proficiency across dozens of consoles, greatly increasing risk of incompatible rules, gaps, and human error. SSE helps address these challenges through single-pane-of-glass management for efficient use of limited IT personnel. Decreasing IT's administrative workload allows the IT team to shift time and resources to new and advanced projects, reducing time spent on low-level access requests and policy.

SSE further improves security posture through consistent policies and protection and complete security observability. Key solution elements include:

- **Universal policy enforcement.** Policy should adapt to contextual risk factors such as time of day or device type by design. However, security policy must be centrally managed and universally applied to ensure a consistent user experience regardless of location or device. The approach ensures that users receive a secure but seamless experience whether in the office, at home, or on the road.

- **Consistency of protection.** Consistent threat detection across all environments is required for a minimum acceptable security posture. Standardizing on an SSE provider eliminates the possibility of differing threat detection capabilities or configurations across vendors, platforms, or environments.
- **Comprehensive observability.** Advanced persistent threats require correlation of multiple indicators of compromise to detect. SSE's broad network visibility provides a wealth of security signals and telemetry for analytics-based detection tools. Elimination of security silos reduces time to detection of fast-spreading, destructive threats such as ransomware as well as insidious insider threats and data theft.

Security Trends in the Digital Transformation Age

The Risks Inherent in New Business-Enabling Technologies

The digital transformation era has introduced a plethora of new technologies and unlocked new business practices. However, these same innovations also introduce previously unimagined threat vectors. For example, edge computing and cloud-native technologies architecture all offer quantifiable benefits such as smaller capital investments, elastic scalability, robust reliability, and low-latency communications. While advantageous, cloud and edge computing require applications, data, and workloads to leave the confines of in-house datacenters and corporate networks. A new environment requires security teams to adapt existing security tools, which they have done with varying degrees of success. It also introduces new vulnerabilities and creates security blind spots for monitoring tools. The WFH trend has raised similar concerns. Legacy approaches to security may result in differing policies and protections for users depending on their location or device type, which increases organizational risk.

The WFH trend is not new. However, the pandemic forced large portions of the workforce to transition to a WFH model seemingly overnight. While most organizations had basic capabilities for remote work, others reported limitations with legacy VPN approaches including licensing challenges, scalability, or the need to install agents. For some workers, fixing VPN-related technical challenges required a brief, unwelcome return to the office or involved a costly work stoppage while awaiting delivery of a new device. Although provided with work devices and applications designed to support workers in their homes, many users found the need to utilize personal devices or cloud applications of their preference. These user-led technologies are colloquially referred to as "shadow IT," a trend that represents a further loss of security visibility and control over user activity and data that increases business risk.

Escalation of External Threats

The cybersecurity risk landscape has expanded in recent years as social engineering efforts by cybercriminals took advantage of pandemic-related fears and confusion. IDC research shows that most ransomware attacks were enabled by unintentional user actions, including drive-by downloads, impersonation, or phishing attacks. On the other hand, criminal organizations such as LAPSUS$ targeted disaffected employees, recruiting insider threats to share credentials or to answer MFA requests on behalf of attackers.

Furthermore, IDC research revealed that destructive ransomware campaigns proved to be more difficult to detect and pernicious than ever in 2022:

- The average ransom paid in North America jumped from $184,000 in July 2021 to $354,000 in August 2022.

- Worldwide, the number of organizations that reported "no successful ransomware attacks" fell by 42 percentage points from July 2021 to August 2022.
- 18% of ransom payers paid six-figure sums; many of these breaches resulted from user error.

Considering Symantec, a Division of Broadcom

Symantec SASE is based on Broadcom's expansive cybersecurity portfolio, which has grown over the years through key acquisitions and organic development. For Symantec SASE, Broadcom has combined multiple key network security technologies into a single cloud platform, offering depth and breadth of capabilities across key security functions.

Symantec SASE integrates the following technologies that are considered core SSE capabilities:

- **Secure web gateway (SWG):** Symantec Web Protection provides comprehensive web security with both on-premises and cloud coverage. This service protects user devices and data from online threats, phishing, malware, and data theft whether the user is in the office or on the road.
- **Zero trust network access (ZTNA):** ZTNA ensures a minimum necessary level of access while minimizing risk exposure based on environmental contextual factors. In accordance with "zero trust" strategy, access may be adjusted based on user location or device, but local users are never assumed to be more trustworthy than remote users.
- **Cloud access security broker:** CloudSOC provides zero trust access to cloud applications, including data protection and access control. CloudSOC allows IT organizations to regain insight and control over user activities in SaaS environments, including sanctioned and unsanctioned applications.

In addition, the Broadcom portfolio includes numerous integration points with solutions that are considered optional or extended SSE capabilities:

- **Data loss prevention (DLP):** DLP scans documents and communications to block unapproved transfers of sensitive data outside of the organization, whether intentional or accidental.
- **Browser isolation:** Browser isolation executes web transactions in a dedicated cloud environment where malicious content cannot reach end-user devices.
- **Endpoint protection:** Symantec Endpoint Protection blocks malware and intrusions on end-user devices.

Business Benefits of Symantec SASE Consolidation

There are key advantages to the Symantec SASE approach. First, Broadcom has made significant strides in combining (reducing) the number of endpoint agents required across its portfolio. Symantec Endpoint Protection can steer traffic to the SSE cloud service for inspection. This provides numerous benefits such as fewer agents to manage. Fewer endpoint agents reduce potential points of failure and administrative overhead. Users gain a consistent access experience whether they are remote or local and regardless of device (corporate issued or personal), which improves user experience and productivity. Fewer SKUs to manage simplifies both the buying process and the accounting process. The goal is a common endpoint agent offering for inline DLP, endpoint security, and SSE that would consume fewer resources and deliver better device performance and user experience.

Security Advantages of Symantec SASE

IDC notes key improvements in security efficacy offered by the Symantec SASE approach. As a cloud service, Symantec SASE is designed for ubiquitous and performant access. By ensuring a seamless user experience, the solution prevents the need for users to attempt risky workarounds, access shadow IT, or disable security controls.

As part of the broader portfolio, Symantec SASE can provide vital telemetry about users' cloud and web activities into extended detection and response (XDR) and security information event management (SIEM) platforms for more complete security analysis. Similarly, the Symantec SASE integration with the Symantec Endpoint Protection agent provides endpoint health visibility for policy decisions that can further reduce business risk.

Challenges

Broadcom follows an enterprise-first market strategy that prioritizes large enterprises. The enterprise market focus impacts the product road map and requires a reliance on an updated partner ecosystem. Positively, Broadcom notes that it recently completed a redesign of its partner ecosystem. Theoretically, a narrowed customer focus may limit threat intelligence insights, as small and medium-sized businesses may face cybersecurity threats before enterprises. However, Broadcom notes ongoing intelligence sharing with Norton consumer security solutions as a means to retain a complete view of attack trends.

Further, concerns about vendor lock-in remain. IDC notes that this is not specific to or limited to Broadcom, as the SSE concept is rooted in the advantages of a consolidated approach compared with the potential benefits of point products. Ongoing market education and deployment flexibility will be key for Broadcom and other SSE vendors going forward.

Conclusion

Remote work and hybrid work are here to stay, but they will require key adjustments to the network security architecture. IDC believes enterprise security buyers will increasingly emphasize productivity, collaboration, and user experience in coming years. The SSE landscape is complex and continues to unfold but is already delivering on the key promises of integration for enhanced security efficacy and efficiency.

Enterprise security buyers will increasingly emphasize productivity, collaboration, and user experience.

About the Analyst

Christopher Rodriguez, *Research Director*

Christopher Rodriguez is a Research Director in IDC's Security and Trust research practice focused on the products designed to protect critical enterprise applications and network infrastructure.

MESSAGE FROM THE SPONSOR

Symantec Enterprise Cloud: Data-Centric Hybrid Security

Symantec Enterprise Cloud delivers data-centric hybrid security for the largest and most demanding organizations in the world. It ensures that enterprises meet legal, regulatory, and corporate data compliance requirements. It empowers today's modern workforce to securely access sensitive company assets from anywhere. And Symantec Enterprise Cloud unifies intelligence across control points, enabling organizations to detect, block, and remediate the newest generation of threats throughout their infrastructure. From remote devices to on-premises data centers to cloud-deployed applications, Symantec Enterprise Cloud solves the critical cybersecurity challenges facing the world's biggest multinational corporations.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com