IDC

SPOTLIGHT

Sponsored by: Tata Communications

Security modernization is required for enterprises to address increasing cybersecurity concerns and related challenges. Integrating key security technologies in a strategy called secure service edge can help.

Best Practices for Successful Secure Service Edge Deployments

September 2023

Written by: Christopher Rodriguez, Research Director, Security and Trust, and Cathy Huang, Research Director, Security Services Worldwide

Cybersecurity Risks Facing the Enterprise

Digital Transformation Offers Undeniable Value

Businesses have invested heavily in digital transformation in recent years, with many now reporting benefits such as increased productivity, revenue, and business agility. Emerging technologies empower businesses to adopt innovative business practices and become more competitive. Flexible work models increase productivity and collaboration. High-performance, low-latency applications drive cloud and compute edge. AI unlocks cutting-edge use cases with tremendous implications for the future of business. Truly, digital businesses are reaping the rewards of their transformation efforts.

The Dark Side of Digital Transformation

Unfortunately, digital transformation efforts have also introduced new vulnerabilities and gaps in perimeter-based defenses. Multicloud and hybrid cloud environments are notoriously difficult to secure, with each cloud provider varying widely in terms of native firewall capabilities available. Third-party firewalls may be deployed as virtual appliances but lack agility and scalability, thereby resulting in complexities and performance issues.

AT A GLANCE

KEY STATS

- 48% of organizations reported notable increases in productivity due to remote and hybrid work (source: IDC's *Future Enterprise Resiliency and Spending Survey, Wave 4,* May 2022; n = 188).
- 28% are prioritizing investments in more efficient networking and access technologies for 2023 such as SSE (source: IDC's *Future Enterprise Resiliency and Spending Survey, Wave 10,* November 2022; n = 824).
- Ransomware damages increased 144% in 2022 to $354,000 per business compared with $145,000 in North America in 2021 (source: IDC's *Future Enterprise Resiliency and Spending Survey, Wave 7,* August 2022; n = 776; December 2021, n = 764).

Digital transformation influences business decisions to gravitate toward cloud and web applications, resulting in corporate data existing in third-party cloud environments outside of IT visibility or control. Similarly, employee preference is expanding the types of devices used to access corporate applications and data. In fact, 76% of organizations offer policies to support the use of BYOD for work purposes. These activities and work models are often outside the control of the IT organization, which further increases the level of risk in the business. Similarly, IT organizations lack visibility into many of the devices on the enterprise network. Often, new IoT devices are manufactured for speed and performance rather than security, which introduces new cybersecurity risks.

Security organizations are struggling to keep pace with the expanding attack surface. Enterprises are already struggling to hire new security personnel in the face of a years-long skills shortage in the labor market. Security teams are further inhibited from adding skilled manpower due to lingering economic uncertainty.

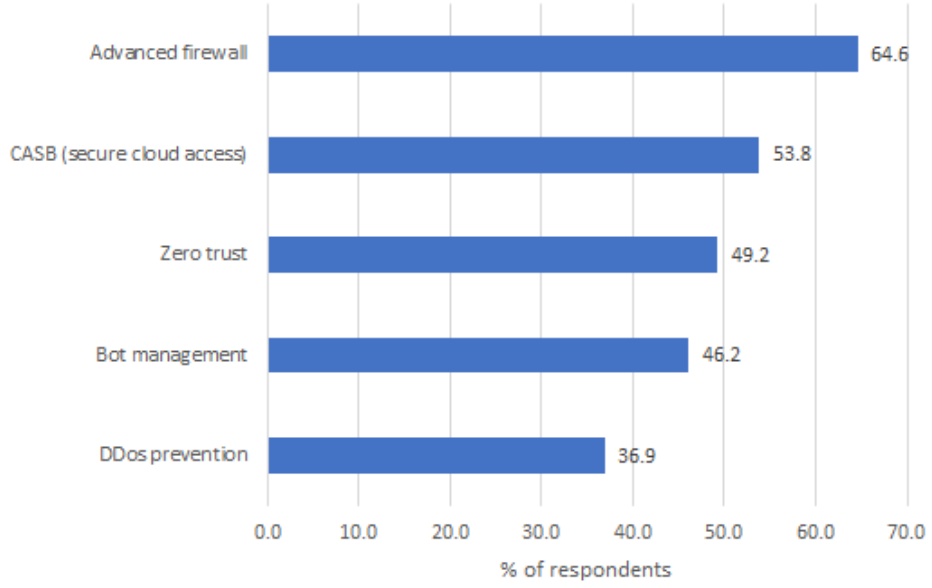
As a result, business risk is mounting rapidly, resulting in costly data breaches. According to IDC, 43% of organizations paid a ransom to regain access to systems or data in 2022 (source: IDC's *Future Enterprise Resiliency and Spending Survey, Wave 7,* August 2022; n = 829). The costs of these damages have risen dramatically around the world, with many organizations reportedly paying hundreds of thousands of dollars in ransom demands. Understandably, 35% of business leaders consider cybersecurity investments as a top strategic priority for the organization's business success (source: IDC's *Future Enterprise Resiliency and Spending Survey, Wave 10,* October 2021; n = 829).

Security Modernization Through SSE

Security modernization is required to address these cybersecurity concerns and related challenges, and enterprises are focusing on integration of key security technologies in a strategy called secure service edge (SSE). Forty percent of enterprises cited "network security transformation (e.g., SSE)" as the critical capability required to execute an organization's cybersecurity transformation (source: IDC's *Security ServicesView,* February 2022). SSE solutions integrate critical network security technologies into a unified, cloud-delivered security service. SSE combines key security functions such as zero trust network access (ZTNA), cloud access security broker (CASB), firewall as a service, and others (secure web gateway [SWG] and data leakage prevention [DLP]) (see Figure 1). Remote browser isolation is a feature that can be added on, as well.

FIGURE 1: ***Top SSE Functions***

Q *Which security features are most important to you in an SSE solution?*



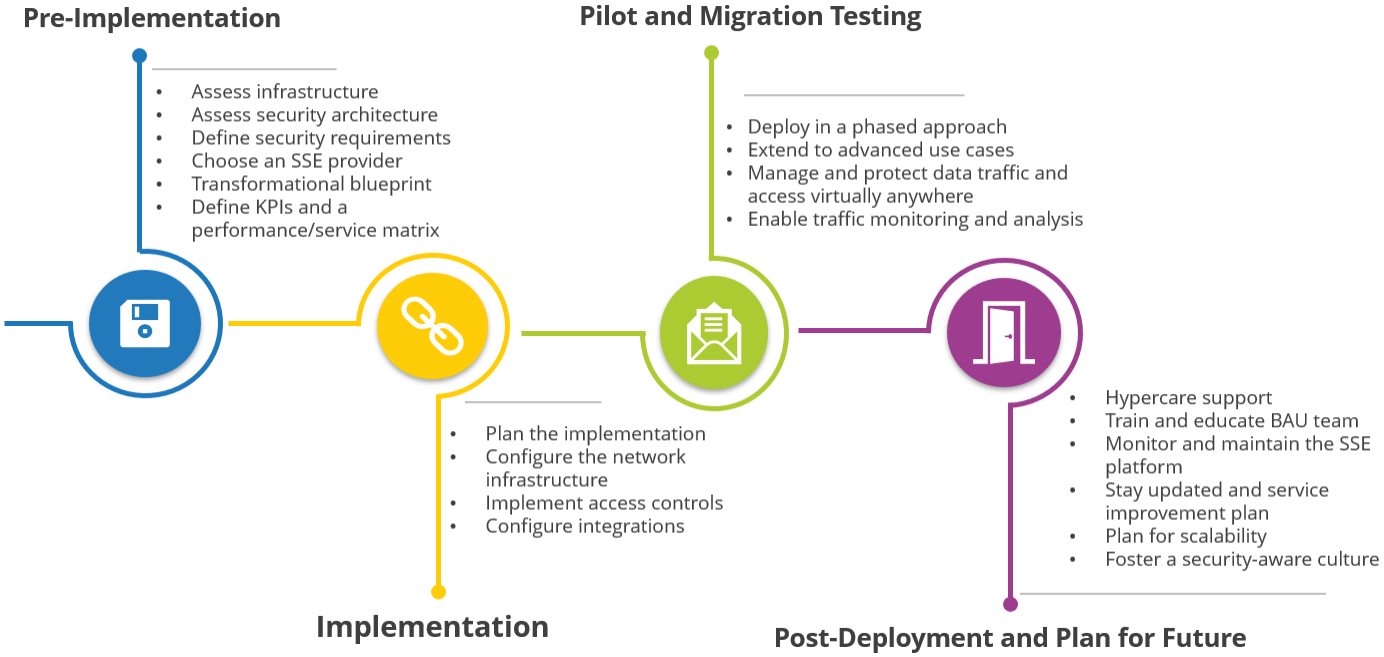
n = 65

Note: Respondents indicated they would use an SSE solution.

Source: IDC's U.S. Enterprise Communications Survey, August 2022

While there is no silver bullet for cybersecurity, the SSE approach addresses key security and related business concerns. SSE consolidates several critically important network security technologies into a common security solution, leveraging the same POPs to perform multiple security functions at the edge. This prevents the need for hairpinning traffic back to a datacenter for inspection or to multiple security clouds for one-off inspections, which reduces latency and increases performance. Similarly, a single SSE agent can support ZTNA access, device protection, compliance, and DLP to reduce the extreme resource utilization required to support multiple security agents. The convergence strategy also offers single-pane-of-glass management for centralized control and reporting. The SSE value proposition prominently features the opportunity to reduce or retire the use of security appliances, consolidation of security technologies, and simplified workflows for security teams. As a result, enterprises are increasing spending on SSE and are planning for further adoption in the coming years (see Figure 2).

FIGURE 2: ***Best Practices for SSE Adoption Journey***



Source: IDC, 2023

The key phases of the SSE adoption journey are described in the sections that follow.

Pre-Implementation

- **Assess infrastructure.** Identify key network requirement, pain points, use cases, user groups, and technical needs. This stage involves an assessment of key questions by leveraging the right tools. Particularly for large enterprises, the assessment requires automated tools to find questions like: What applications need to be accessed remotely? What resources are required? What are the uptime and latency requirements, and what is the business criticality of the application?

- **Assess security architecture.** Assess current security architecture and practices for shortcomings, limitations, vulnerabilities, and security gaps. Are VPNs overly permissive, and if so, which applications require ZTNA protection? What are identified security risks? Next, map these requirements to SSE capabilities. Align expectations for security outcomes. Does ZTNA address the limitations of VPN?

- **Define security requirements.** What is the goal of the project? Consolidation or true integration? What is the importance of leveraging AI in security processes? Does the importance of AI vary by use cases (e.g., threat detection versus automatic remediation)? What about business objectives such as improving digital resiliency, modernizing security infrastructure, limiting the number of security vendors, or reducing data silos?

- **Choose an SSE provider.** It is important to carefully evaluate the capabilities of an SSE solution before choosing one and to make sure that the organization has the resources to effectively use it. SSE solutions can be complex to set up and manage, especially for organizations that lack the relevant skills in-house. It is useful to consider a managed SSE services option; an experienced managed SSE services provider has the right technology, process, and expertise to make it all work.

- **Transformational blueprint.** SSE solutions offer a one-stop shop, but an enterprise transformation journey often starts with focus on specific security functions. Replacing legacy security controls and networking tools is a top priority. Consider replacing VPN with ZTNA in phases or specific applications, followed by eventual full VPN retirement. Similarly, businesses are replacing MPLS with SD-WAN.

- **Define KPIs and a performance/service matrix.** Despite spending millions in cybersecurity programs, organizations often struggle with the following asks: What are my security KPIs? Are my security investments working? Why am I still getting breached? Am I secure? Organizations work with security service vendors to define the desired outcomes, such as reducing the risk of a data breach, improving incident response times, maintaining uptime of critical systems, or achieving some level of cybersecurity compliance/maturity.

Implementation

- **Plan the implementation.** List the necessary device installations, updates, and changes required, including agent software deployment and configurations of existing network infrastructure such as routers, firewalls, and proxies. Identify stakeholders, solicit their feedback, and consider their input to ultimately generate buy-in. Create a timeline that minimizes business disruption. Identify which use cases or environments may require specialized devices, and if so, the bandwidth, power consumption, and environmental considerations involved.

- **Configure the network infrastructure.** Configure network devices including routers and firewalls to direct traffic to the security provider's cloud including necessary changes to IP addresses and DNS settings. The SSE solution may require new connector devices or virtual appliances to be installed at network entry points whether across on premises, branch offices, or public cloud environments, depending on the level of ZTNA granularity required. Updating DNS settings allows managed and unmanaged devices to connect to the relevant applications and servers. For remote users and devices, updated IP, DNS, and proxy settings will be required on their end devices. An installed agent will help route traffic to the security cloud as well.

- **Implement access controls.** SSE solutions offer powerful ZTNA policy enforcement and access control capabilities. Legacy VPN policies may be a useful point of reference to understand access needs, but IT organizations should be

sure to avoid replicating the broad permissive access of VPNs. To the extent possible, an understanding of user group access requirements mapped to specific applications and resources is needed. To assist with simplifying adoption of more powerful access controls, SSE solutions feature out-of-the-box policies, wizards, and policy recommendations. With the advent of generative AI, additional automation capabilities will soon be available to simplify the creation of zero trust and CASB policies through declarative statements.

- **Configure integrations.** Integration with existing identity and security systems are a given for some aspects of SSE. For example, Azure AD and MFA SSE provide insight into user identity and validation that is a critical factor for deciding and enforcing ZTNA policies. In addition, SSE solutions provide an excellent source for network telemetry. By capturing and collecting relevant packet data in a SIEM, security analytics can have more insight with which to identify sophisticated and elusive threats. Many SSE solutions are now bolstered by powerful XDR tools and data lake capabilities.

Pilot and Migration Testing

- **Deploy in a phased approach.** A full SSE deployment can consolidate the many enterprise networking and security tools and reduce security silos. But it can take time. Many organizations find success beginning with a focused ZTNA project or a pilot project, before expanding into a broader rollout. This will effectively mitigate risks with regard to implementation and development. Very often, SWG is a useful starting point as security organizations can establish a standard set of protections and risk mitigation policies that can be enforced across all user groups. CASB and DLP are logical next steps.

- **Extend to advanced use cases.** Advanced security functions such as sandboxing or deception may represent a third phase for deployment. SSE may also take longer to extend to use cases or environments such as IoT/OT. However, 27% of organizations expressed a need to support all assets including IoT/OT as a key security feature (source: IDC's *Security SOC Tools Survey,* November 2021; n = 377). In addition, IDC notes that while ZTNA is a useful solution for specific access needs, a full zero trust transformation may involve SSE-adjacent solutions such as microsegmentation.

- **Manage and protect data traffic and access virtually anywhere.** The goal of SSE is to extend to a full deployment across all devices and use cases. Comprehensive, flexible SSE solutions can support all users regardless of workforce location. However, integrations with MDM and UEM tooling may be required to account for all device types.

- **Enable traffic monitoring and analysis.** SSE has important tie-ins to SIEM, XDR, and other security analytics tools that may represent a broader security initiative beyond SSE adoption. Security analytics tools are important to detect advanced threats. However, practical decisions must be made between the need to capture more packet information versus storage investments. Beyond security considerations, SSE telemetry can also provide insight into performance and reliability of connections. Some SSE providers now offer digital experience monitoring (DEM) tools for insight and troubleshooting into user experience for application access, hosted in cloud and hybrid environments.

Post-Deployment and Plan for Future

- **Hypercare support.** Hypercare support is used to provide extended support after implementation and rollout, with the objective of continuous improvement post deployment. It is to ensure the overall workflow and integrations

with other platforms is working as expected. The hypercare support is also to ensure that all critical issues are recognized and documented for further resolution and remedy.

- **Train and educate business as usual (BAU) team.** The training will help the BAU team to be aware of any new security controls and processes to prevent the team from accidentally bypassing security controls that could lead to a security breach. Regular training will allow the BAU team to be familiarized with the incident response and escalation procedures so it can be more effective in detecting and preventing security breaches. It also helps to define runbooks to achieve efficiency and left shift in security operation
- **Monitor and maintain the SSE platform.** The monitoring of the SSE platform is not only for performance reasons but also security reasons. Like any other IT platform, the SSE platform has potential for the introduction of security vulnerabilities or any software bugs. By monitoring the platform, it is possible to identify any vulnerabilities or software issues early on and address them before they cause serious problems for users.
- **Stay updated and service improvement plan.** To have a service improvement plan (SIP) is to have a document that outlines the steps that will be taken to improve the performance, reliability, and security of a service. A comprehensive managed SASE offering often includes continuous management of the SASE platform and 24 x 7 monitoring. It is critical to have a SIP to track progress and measure the effectiveness of the SASE service.
- **Plan for scalability.** The nature of the digital transformation era involves more powerful applications, many more devices, and demanding user expectations. To the extent possible, a fully cloud-delivered SSE solution is ideal for scalability and future proofing. Physical devices may be necessary for certain use cases — in which case, scalability is a key factor to accommodate future traffic demands.
- **Foster a security-aware culture:** Security breaches often tie back to user actions, including many cases of accidental data leakages due to insider threats or unpatched systems. Strong security controls are only half the battle. Leading SSE solutions provide direct feedback to end users to explain the reasoning behind policy enforcement decisions.

Recommendations for the SSE Buyer

The following recommendations are offered to assist in increasing the likelihood of project success, minimizing wasted time and resources, and reducing business risk overall:

- **Identify priority pockets of transformation.** Start with modern applications that are best suited for ZTNA access. After a few quick SSE transformation projects, momentum will build, and lessons learned can be applied to other transformation areas.
- **Conduct a thorough risk assessment.** A comprehensive cybersecurity risk assessment helps meet the needs of a digital enterprise and deliver a transformation road map around SSE-centric enterprise architecture. Every organization has varying levels of risk appetite, and that directly drives the security outcomes and related metrics organizations should drive for their cybersecurity program and investment. A one-size-fits-all security solution may not be effective for all organizations. Instead, security solutions and programs need to be right-sized and aligned with their specific business needs and objectives.

- **Ensure performance optimization:** Performance cannot be sacrificed for the needs of security. When security solutions pose an obstacle, users may look for workarounds or other ways to circumvent security controls. When successful, these users and their devices and data will be at risk. SSE performance is a growing consideration for enterprises and an overlooked factor for successful SSE adoption.
- **Regularly review and optimize (including monitoring performance metrics).** Companies no longer need to wait a year or more to know what their security posture is. The capability of regularly reviewing and fine-tuning the SSE platform offers a continuous view of the security and risk posture. Moreover, the unified threat visibility is particularly important when SSE components are from different vendors. A managed SASE offering in particular helps to keep companies aware and on top of the performance and business metrics.
- **Carefully choose a security provider to avoid financial burdens and management hassles.** The vendor should offer a comprehensive managed SSE offering including continuous management of the SSE platform, 24 x 7 monitoring and threat detection, and other important cybersecurity capabilities, as well as other necessary SSE-related advisory and assessment services. Advisory services, protection services, monitoring services, and many more services help customers develop robust security strategies and offer ongoing assistance as they embrace SSE.

Considering Tata Communications

Tata Communications is an India-headquartered global communications, connectivity, and security services provider. It owns one of the largest wholly owned subsea fibre networks, underpinning the internet backbone and carrying roughly 30% of the global internet routes. Tata Communications has the intent and vision to be a premier provider of cybersecurity services and a one-stop partner for managing cyber-risks globally.

Tata Communications' portfolio of cybersecurity spans advanced network security, cloud security, threat management, security assessment, and consulting services. Moreover, it offers fully managed SD-WAN and full SASE from Zscaler, Netskope, and Palo Alto Networks. In addition, Tata Communications has its own hosted SSE that is a network-agnostic solution with advanced threat protection. Its SSE is designed to protect against various cyberthreats, together with its DDoS mitigation services (i.e., securing Layers 3 and 4 and application Layer 7), contributing to an overall robust defense posture for its clients. Tata Communication provides a single-pass architecture that secures private apps, users, and internet traffic from web, cloud, and network-based threats. Moreover, Tata Communications SSE can accelerate cloud migration by enforcing consistent security while moving on-premises assets to the cloud. The solution automates policy enforcement for migrating workloads. Essentially, the solution delivers the benefits of developing a consistent security posture across multiclouds, while providing simpler and stronger security efficacy.

Very often, the vendor provides holistic threat management and remediation capabilities for its managed SSE clients. Tata Communications has good range of skills to help clients managing multiple security solutions in addition to the SSE solution. Moreover, it has integrated customer's ticketing tool to Tata Communication's portal for service management. As a result, the client enjoys improved user experience and security posture. It has significantly simplified security estate and management by leveraging a single service provider for all network security and managed services requirements.

Challenges

The traditional MPLS-heavy, hub-and-spoke network architecture fails to meet the growing demands of a digital-first enterprise. At the same time, the security team struggles with complexities, tool sprawl, and low efficacy. Tata

Communications could help educate the market with clearly differentiated messages around the managed third-party SSE vendor partnerships it has as well as how it offers its own branded SSE solution at the same time.

Conclusion

IDC believes the SSE market offers an important option for needed security modernization efforts. To the extent that Tata Communications can address the challenges described in this paper, the company has a significant opportunity for success.

About the Analysts

Christopher Rodriguez, *Research Director, Security and Trust*

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 infrastructure. IDC's Security and Trust research services to which Chris contributes include Active Application Security and Fraud, where he covers web application firewall, DDoS mitigation, bot management, and API security.

Cathy Huang, *Research Director, Security Services Worldwide*

Cathy Huang is a research director in IDC's Security and Trust research practice focused on managed security services, security consulting, and integration services within the security services program. In addition, she collaborates with other team members to look at services that help organizations adopt emerging technologies like edge, 5G, and IoT, as well as key focus areas such as cloud security, cyber-resilience, and cyber-transformation.

MESSAGE FROM THE SPONSOR

"By weaving security into every connection, we simplify architecture, fortify control, and amplify visibility through our integrated platform which acts as your fortress converging multiple safeguards forging a unified shield against web and cloud threats. Additionally, our continuous monitoring and accelerated response minimizes lateral threat movement. With our proven track record of resolving critical incidents in under 33 minutes, you can be confident that your data is safe."

Badri Narayanan Parthasarathy, Vice President — MSS Products & Engineering

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