ecosystm.

TATA COMMUNICATIONS

Secure Access Service Edge (SASE): Empowering the Distributed Enterprise

AUGUST 2023

DARIAN BIRD
Principal Advisor, Ecosystm

Emergence of the Distributed Enterprise

Organisations are rapidly transforming – enhancing customer experiences with digital services, boosting production efficiency with IoT, and providing mobile and remote access to users.

This requires network and security strategies to become highly distributed, cloud native, and converged.

Modernising networking and security environments opens up a world of possibilities for organisations to create a hyperconnected ecosystem. This ecosystem fosters closer collaboration with customers, employees, and partners, empowered by AI-augmented decision-making processes. At the core of this ecosystem is a seamless flow of data between connected machines, regardless of their location.

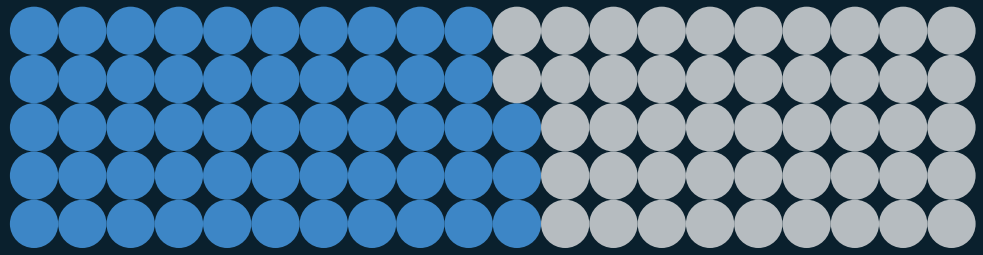

Challenges of Building a
Distributed Enterprise

Cloud Overtaking the Data Centre

Cloud is already a mature deployment model, with organisations trusting it for latency-sensitive collaboration, business critical transactions, and customer-facing services. Traditional networking architectures cannot keep pace with cloud-native organisations that rely more on the cloud than on their data centres.

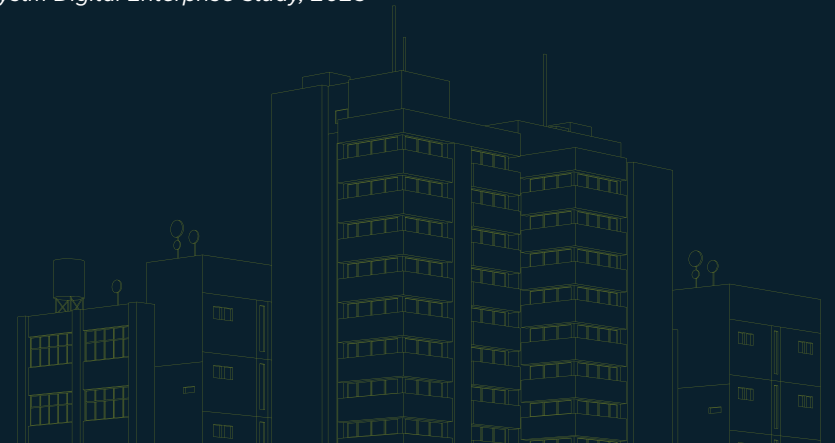
Inefficient and costly backhauling adds latency just as applications are demanding better network performance.

Multi-Cloud is Becoming Increasingly Popular



53%
Adopted Multi-Cloud

N=948
Source: Ecosystm Digital Enterprise Study, 2023



Supporting Hybrid Work

The advancement of collaboration tools, like video conferencing and workflow management, allows knowledge workers to be productive from anywhere. Organisations now recognise that providing a hybrid work environment is vital for talent attraction and retention.

With the WAN edge now extending to home offices and remote locations, traditional security and network architectures are no longer sufficient. Secure access with quality of service can be granted to power users, such as executives or those with external-facing roles with small, low-cost edge devices. Although most home networks rely on a single connectivity path, steering policies and error correction will boost performance.

Security policy enforcement and centralised management will give organisations control over an increasingly distributed environment.

Preferred Work Location for Knowledge Workers

71%
Both from home and the office

20%
Remotely all the time

9%
From the office all the time

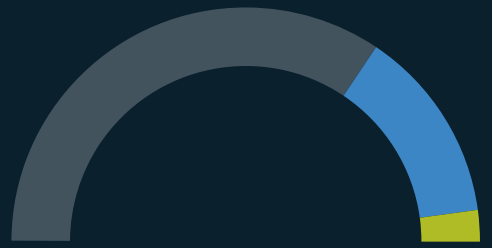
N=1,043
Source: Ecosystm Voice of the Employee Study, 2023

Moving Beyond Perimeter Security

With critical workloads increasingly being migrated to cloud and a distributed workforce accessing the network, organisations face a diversity of attack vectors. Simultaneously, the cost of breaches continues to rise with workforce productivity, customer experience, and the operating environment relying on secure cloud service. Due to this growing complexity, security analysts suffer from alert fatigue, overwhelmed by the volume of false positives and challenged to differentiate critical threats from minor issues.

Organisations are shifting away from traditional WAN architectures to embrace more distributed, heterogenous networks to access cloud services. This is driving the convergence of networking and security to ensure the delivery of applications, wherever they sit, without introducing vulnerabilities.

Organisations Assume Breach



69%
Expect a data breach

26%
Do not expect a data breach

5%
Are unsure

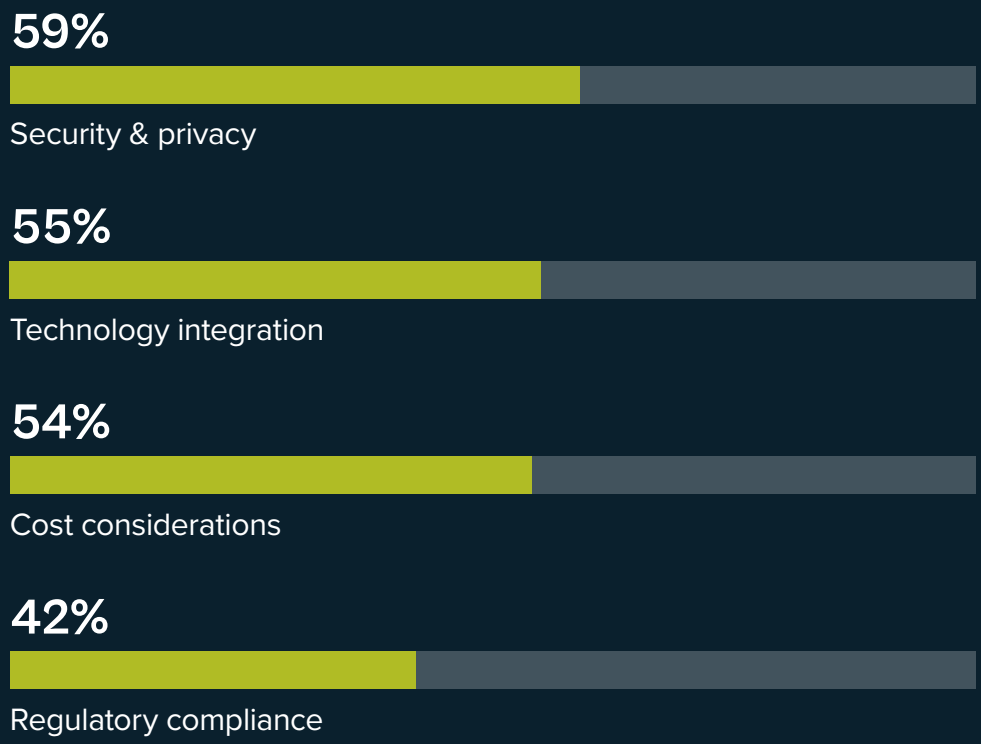
N=948
Source: Ecosystm Digital Enterprise Study, 2023

The Need for Automation to Manage Complexity

With organisations digitising their customer and production environments, the volume and diversity of connected IoT devices have increased. Distributed enterprises now require high performance connectivity across a growing number of locations to support their operations.

The scale and complexity involved in managing networks that support IoT deployments is now beyond human operators. Organisations require automation to improve visibility, regain control, and ease network management.

Leading IoT Deployment Challenges



N=1,466
Source: Ecosystm IoT Study, 2023

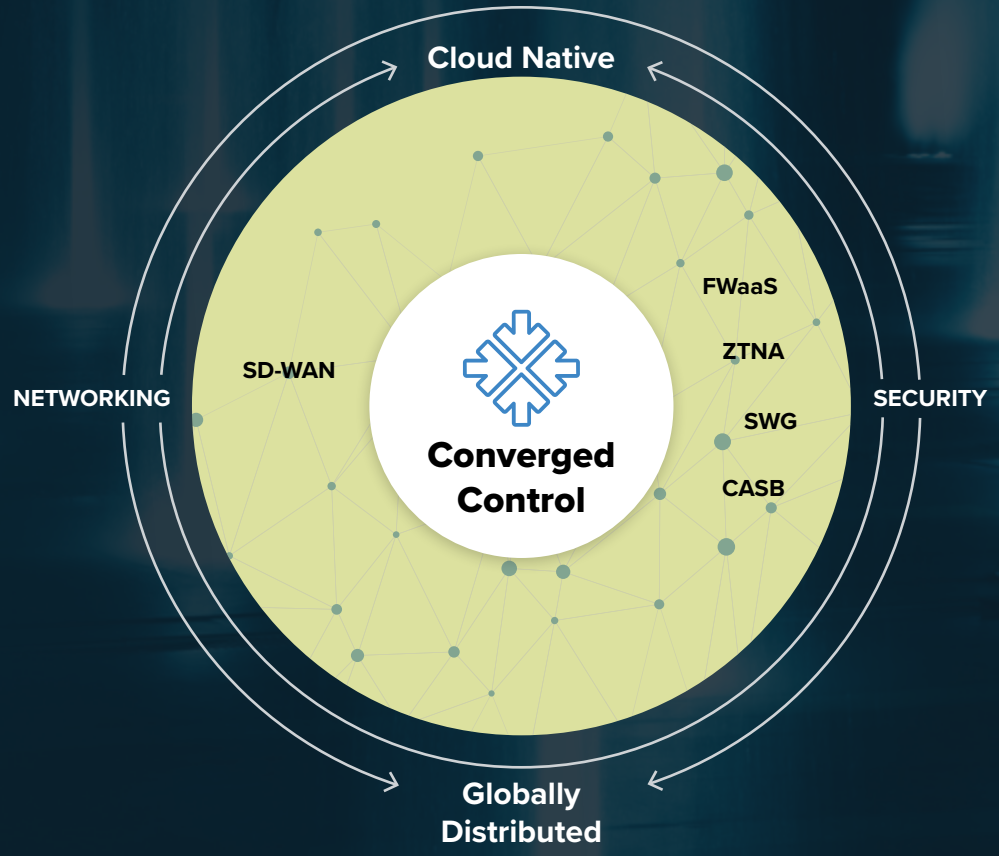
Introducing SASE

SASE: Network and Security Convergence

A Secure Access Service Edge (SASE) represents the convergence of networking and security.

It brings together the modern networking architecture of SD-WAN, with next generation security tools – FWaaS, ZTNA, SWG, and CASB. Delivered as a single service from the cloud, SASE is designed to support distributed enterprises.

SASE Framework



Why SASE?

CLOUD NATIVE

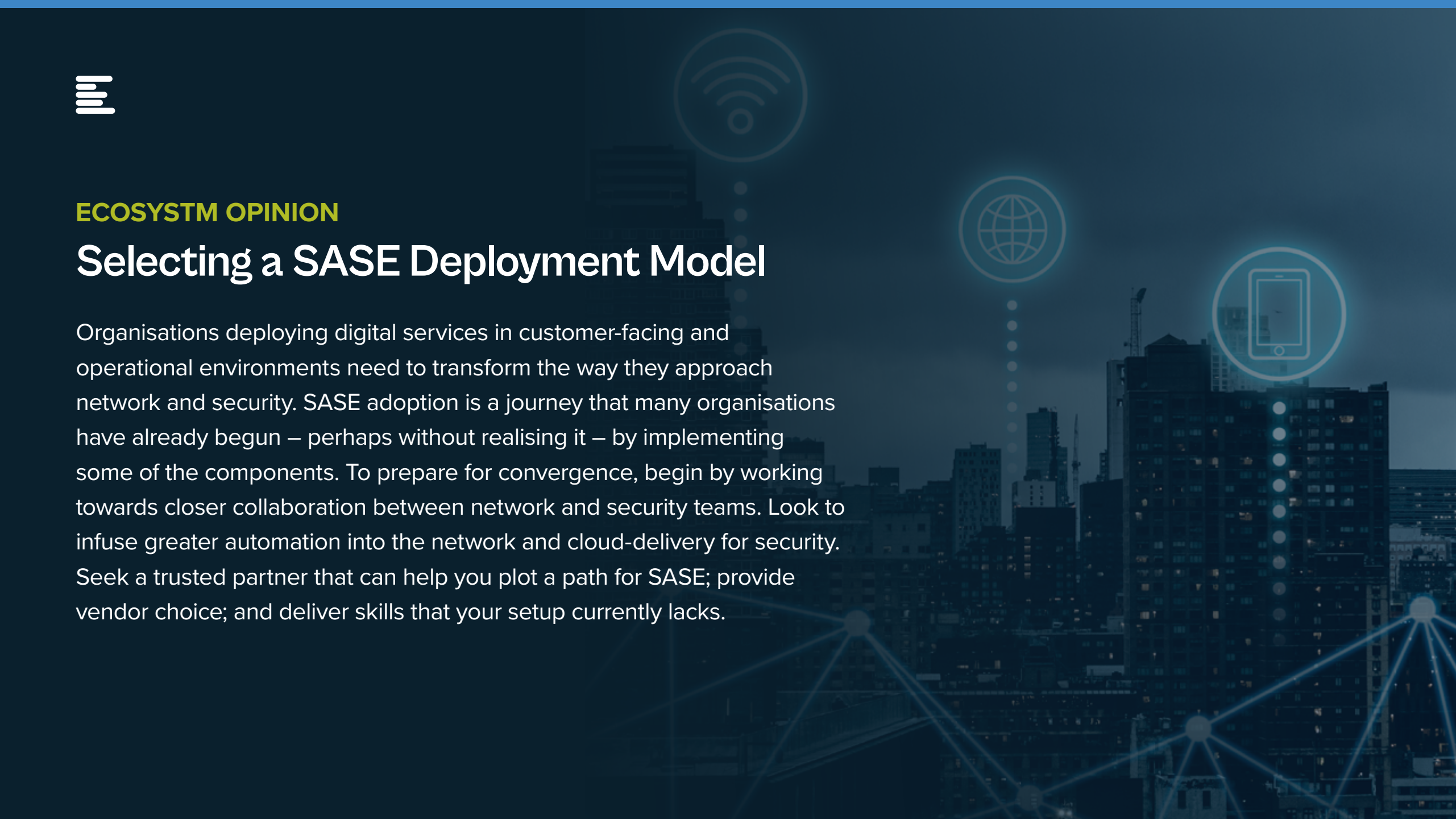
SASE is delivered as-a-service with the benefits of being cloud-elastic, managed, and highly available. Organisations already host critical applications in the cloud and their customers access services in branches, at home, and on mobile devices. Rather than relying on perimeter protection, SASE provides security from the cloud to wherever it is needed.

GLOBALLY DISTRIBUTED

Distributed enterprises have branches, offices, machines, and customers across a diversity of locations. SASE providers match this architecture with global networks that reach the edge wherever it is. They deploy PoPs adjacent to cloud data centres, securely connected by private backbones with multiple paths to maximise performance and resiliency.

CONVERGED

SASE unifies the network and security functions, enabling centralised management and increased visibility. By using APIs, unification can be achieved in either a single or multi-vendor system allowing organisations to leverage already installed systems. Convergence makes single pass inspection for security and routing possible, and reduces latency and processing costs.



ECOSYSTM OPINION

Selecting a SASE Deployment Model

Organisations deploying digital services in customer-facing and operational environments need to transform the way they approach network and security. SASE adoption is a journey that many organisations have already begun – perhaps without realising it – by implementing some of the components. To prepare for convergence, begin by working towards closer collaboration between network and security teams. Look to infuse greater automation into the network and cloud-delivery for security. Seek a trusted partner that can help you plot a path for SASE; provide vendor choice; and deliver skills that your setup currently lacks.

The SASE market is still taking shape with networking and security vendors rounding out their portfolios and telecom providers enhancing their offerings.

Consider the following options when selecting a deployment model.

SINGLE or MULTI-VENDOR?

Many organisations maintain heterogenous networks and security stacks that lack cohesion. Very few providers can deliver the full SASE suite and the concept of rip and replace of a full infrastructure is unappealing anyway. Find a partner that can integrate your current system and migrate it over time, to cloud. Trusted partners offer vendor choice and help to avoid lock in.

DIY or MANAGED?

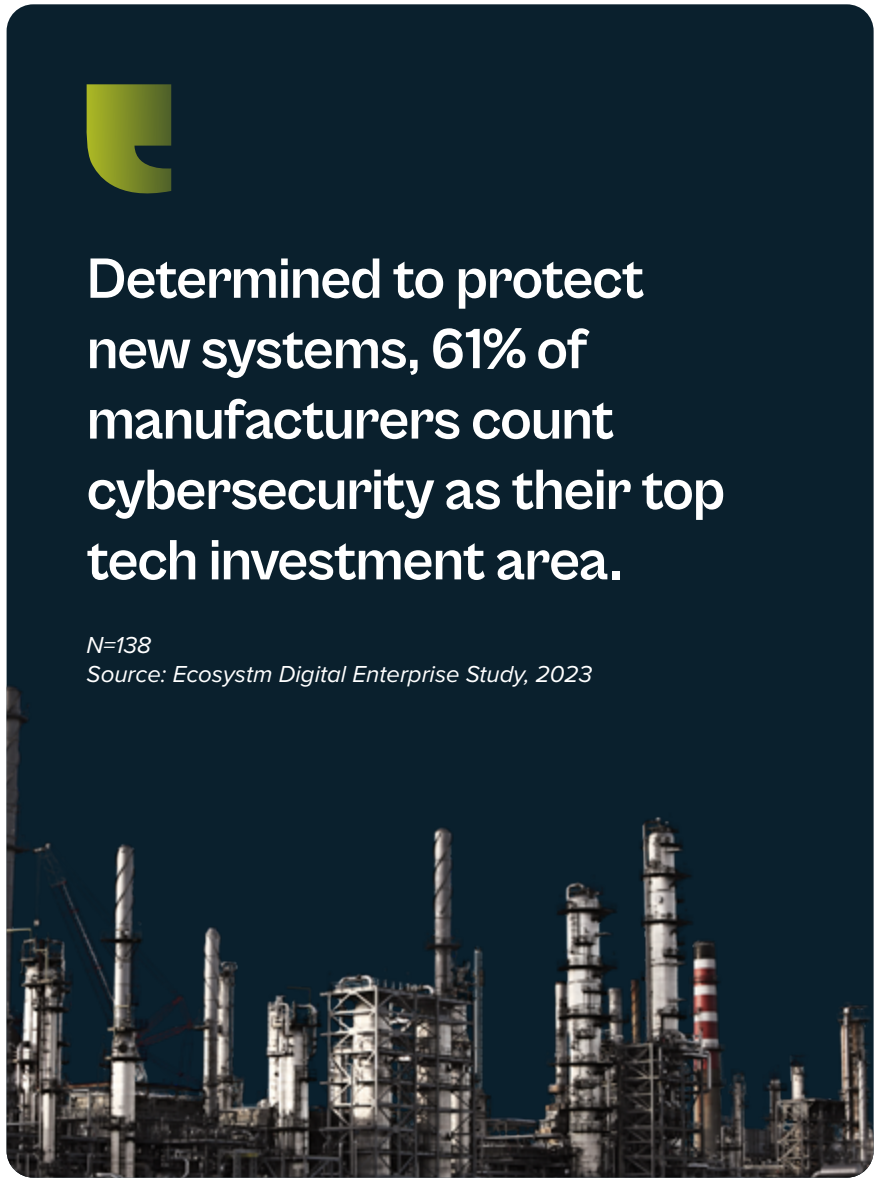
Early SD-WAN adopters employed a DIY approach with the aim of reducing costs. SASE focuses on greater benefits, including centralised management and global infrastructure. Managed services providers ensure faster deployment, provide specialised knowledge, and allow network and security teams to focus on higher value projects.

Industry Use Cases of SASE

Manufacturing

In an increasingly complex world, manufacturers use cloud services to manage critical functions, such as product development, supply chain, and quality control. At the same time, production lines are becoming automated, necessitating connectivity on the factory floor.

SASE can support manufacturers that are building hyperconnected ecosystems with low latency, secure access even in remote facilities. The foundation of instantly accessing resource locations, sharing sensitive product designs, and facilitating collaboration between different sites lies within the network. By unifying network and security management, using micro-segmentation, and adopting ZTNA, SASE can help manufacturers avoid costly production stoppages.



Retail

Resiliency for retailers no longer only includes uptime and security of their transactional systems but also for data-intensive services delivered at the branch, warehouse, and online. Stores require connectivity for inventory management, loyalty programs, and ecommerce systems to function. Customers also require guest access to experience digital services in-store.

Many retailers operate a diversity of branches, with varying levels of size, connectivity, and IT staffing. The centralised management of SASE can ensure security and guarantee QoS even in BYOD environments and remote locations. Retailers can also quickly onboard new branches with any transport type by deploying zero-touch appliances.

Mobile applications are now the top tech investment focus for 45% of retailers.

N=146
Source: Ecosystm Digital Enterprise Study, 2023

Healthcare

With healthcare providers extending their services to a multitude of settings, clinicians require secure access to critical data, such as diagnostic images, regardless of their location. Patient engagement is also being enhanced with self-service access to health records, prescriptions, and scheduling.

Automated steering and visibility are essential to prioritise critical functions across complex provider and remote environments. Applying role-based controls with zero-trust security principles is crucial to prevent ransomware attacks and achieve compliance, while permitting access to clinicians, patients, and devices.

The need to seamlessly connect the edge to the cloud has made detecting ransomware the top cybersecurity focus for 59% of healthcare providers.

N=79
Source: Ecosystm Digital Enterprise Study, 2023

Banking & Financial Services

SaaS offerings – especially from innovative Fintech providers – are allowing Financial Services organisations to rapidly add new digital services, like personalised engagement, point-of-sale lending, and robo-advisory. They are also gaining efficiencies by increasingly migrating applications to the cloud, such as CRM, collaboration, and backup.

With SASE, organisations can access cloud services without backhauling to the central data centre, maximising application performance, even in rural branches. It can also ensure compliance and secure access to sensitive data with policy enforcement based on role and identity. With 24/7 uptime vital for applications like ATM services and contact centres, SASE can also improve resiliency with redundant connectivity.

Essential Guidance

SD-WAN Optimisation

The first step to SASE is to optimise your SD-WAN by integrating AIOps and leveraging features such as data deduplication and dynamic forward error correction.

Avoid Vendor Lock-In

As contracts come up for renewal, consider reducing the number of vendors in the network and security stack. Most importantly, ensure any long-term contracts are flexible and avoid vendor lock-in.

Network-Security Convergence

SASE is founded on the convergence of network and security functions. Begin by breaking down any barriers between the two teams to ensure planning is conducted from the perspective of both.

Cloud-Enabled Security

Modernise your security stack by migrating legacy functions to the cloud (e.g. FWaaS) and begin adding cloud-native tools like CASB.

Universal Business Consideration

The cloud-native deployment of SASE makes it accessible to organisations of all sizes, including SMEs. The ability to pay monthly, consolidate billing, reduce physical assets, and entrust networking and security to a manged provider is attractive for organisations with limited IT resources.

Engaging a Trusted Partner

Adopting a SASE approach requires new skills, new technology, and a rethink in team dynamics. Currently, no single vendor can provide a comprehensive SASE solution, so integration is still necessary. Identify a trusted partner that can help plan and even manage the transition.

Tata Communications End-to-End SASE Offering

Tata Communications Managed SASE

Hybrid SASE

- Best-of-breed offerings with select technology players (SD-WAN and SSE)
- TC^{x}, customer lifecycle management platform, provides a single pane of glass visibility and self-service
- Unified customer experience with integrated delivery and operations

Hosted SASE

- Unified SASE PoPs deployed within Tata Communications Global Tier 1 IP network
- End-to-end control and visibility over the enterprise traffic
- Consistent experience for users with single pane of management and visibility

Add-on Security Service

- Advanced Threat Management: Detect & Prevent Advanced Threats with Cloud SOC
- Anti-DDoS: Protect against Global Large-scale DDoS Attacks

DAY 0: DEFINE | DAY 1: DELIVER | DAY 2: OPERATE & OPTIMISE

TATA COMMUNICATIONS TC^{x} DIGITAL EXPERIENCE PLATFORM

CASE STUDY

Secure Network Transformation in a Bank With Remote Locations

BACKGROUND

A regional bank in India operating across 35 sites, with multiple disparate network providers

CHALLENGES

- Diverse providers with no visibility across multiple locations. All locations with separate MPLS and local Internet connections
- Concern about achieving the promised benefits from network transformation with SD-WAN
- Compliance with banking regulation, needed URL filtering and other security features in a flexible consumption model

SOLUTION

- IZO™ SDWAN Validate – an expert-led proof of concept (PoC) experience to demonstrate key SD-WAN and security use cases
- Converged SWG and ZTNA, via secure regional cloud gateways
- Unified TC^{x} portal facilitating end-to-end customer journey by providing visibility across multiple services including ordering, billing, ticketing, reporting, along with self-service features

OUTCOMES

Seamless PoC Process

Converged SD-WAN with Security

Unified Platform with Self-Service

About Ecosystm

Ecosystm is a Digital Research and Advisory Company with its global headquarters in Singapore. We bring together tech buyers, tech vendors and analysts onto one integrated platform to enable the best decisionmaking in the evolving digital economy. Ecosystm has moved away from the highly inefficient business models of traditional research firms and instead focuses on research democratisation, with an emphasis on accessibility, transparency, and autonomy. Ecosystm's broad portfolio of advisory services is provided by a team of Analysts from a variety of backgrounds that include career analysts, CIOs and business leaders, and domain experts with decades of experience in their field. Visit **ecosystm.io**

About Tata Communications

A part of the Tata Group, Tata Communications is a global digital ecosystem enabler powering today's fast-growing digital economy in more than 190 countries and territories. Leading with trust, it enables digital transformation of enterprises globally with collaboration and connected solutions, core and next gen connectivity, cloud hosting and security solutions and media services. 300 of the Fortune 500 companies are its customers and the company connects businesses to 80% of the world's cloud giants. For more information, please visit **www.tatacommunications.com**

This ebook is sponsored by Tata Communications. It is based on the analyst's subject matter expertise in the area of coverage in addition to specific research based on interactions with technology buyers from multiple industries and technology vendors, industry events, and secondary research. The data findings mentioned in all Ecosystm reports are drawn from live and ongoing studies, based on participant inputs that include decision-makers from IT and other Lines of Business, from small, medium and large enterprises. For more information about Ecosystm studies visit www.ecosystm.io