



SASE IS A JOURNEY, NOT A SILVER BULLET

SECURITY IS TOP OF MIND FOR EVERY ORGANIZATION...

..and similar to cloud and digital transformation, every business is in a unique state of maturity with their security strategies and practices. A few organizations may feel they have it well handled, most have some services in place but with gaps or challenges they struggle to overcome, while some don't know where to start. Given the innovation within the market and new heights of monetary motivation for cyber criminals, organizations should look at security as an ongoing journey.

CONTENTS

No One is Safe	3
The Challenge of Compliance	3
Defenses Require More	4
Is SASE the Silver Bullet?	4
See SASE as the End Goal	5
Zero-Trust Network Access	6
Shift to OpEx for Infrastructure and Security	6
GTT Enables a SASE Journey that is Right For You	7
GTT Secure Connect, a SASE Framework	7
Visibility into Applications and Network	7
The GTT Infrastructure Difference	7
Learn More	8
About GTT	8
About Fortinet	8

NO ONE IS SAFE

Attackers are intelligent and financially driven to discover new ways to infiltrate networks, steal, and resell your data or exploit it for fraud. Personal Identifiable Information (PII) is particularly valuable due to its close connection to monetizable data like intellectual property or private personal information (PPI). While industries like financial services, healthcare, and government are frequent targets, organizations of all sizes and sectors are at risk, as they often store sensitive data like social security numbers, birth dates, and addresses. Many corporations underestimate the "street value" of their information, neglecting the importance of security. Moreover, attackers seek more than just data; they increasingly siphon processing power and bandwidth to fuel large-scale attacks or resell these resources for profit. No matter the industry or company size, any organization can be targeted. Statistically, it's only a matter of time, given that highly incentive-based bad actors continually refine their tactics using emerging technologies like AI and generative AI for faster, more effective attacks.

Companies face immense pressure to safeguard data, and in the event of a breach, they must respond quickly and transparently. Delayed responses can lead to fines from multiple federal entities, eroded customer trust, reduced productivity due to disrupted operations, and various other consequences.

The CIA triad—confidentiality, integrity, and availability—is an important guiding model in information security. A comprehensive security strategy takes administrative, technical, and physical controls into account to reduce risk and mitigate threats. While this paper focuses on technical controls, organizations should be mindful to address all three areas to contribute to a safe and secure environment.

IMPACT OF POOR PREPARATION

- Loss of jobs
- Insurance premium increases
- Regulatory fines
- Reputational damage
- Legal costs
- Ransom demands
- Recovery costs
- Operational disruption/downtime
- Lost value of customer relationships
- Lost revenue
- Devaluation of brand
- Loss of intellectual property

THE CHALLENGE OF COMPLIANCE

The demand for compliance is becoming more urgent as well as harder to achieve, and it's pushing many businesses to get their security houses in order. High-profile edicts such as GDPR and other industry and regional data protection requirements are maturing, and the fines are becoming more aggressive as government agencies feel the grace period for awareness and meeting compliance is over. The cyber-insurance industry is maturing as well and requiring higher levels of security and compliance rigor to qualify. Likewise, CEOs and board members are seeking similar transparency and reporting as personal accountability is reaching the executives and they want to keep the business safe and out of the news. Even in industries where data privacy is front and center, most businesses do not have the necessary headcount, expertise, or tools to deliver against the consistent updating and increasingly stringent requirements.



**THE CYBERSECURITY
WORKFORCE GAP HAS REACHED
A RECORD HIGH, WITH**

4 MILLION

**PROFESSIONALS NEEDED TO
ADEQUATELY SAFEGUARD
DIGITAL ASSETS.¹**

STRONGER DEFENSES

It's common for SecOps teams to reach for the next tool that will address the latest threat. But technology choices are only a piece of the puzzle. The classic IT trio remains true: you must align your technology, your people, and your processes to establish effective defenses. This includes having the expertise needed to keep up with the threat landscape. When everything you owned resided in your data center and on your network, this was a much easier task. Now, data is everywhere, users are mobile, apps have distributed architectures, and you have multiple technology stacks to manage and secure across data centers, clouds, and at the edge.

SecOps teams are straining under volumes of point products that are hard to manage, don't talk to each other, and can't provide the needed holistic visibility or control. And teams are short on resources to effectively protect the business, its users, its applications, its customers, and its partners. This shortage of security professionals is causing security gaps, burnout, and prevents businesses from being able to scale. Knowing the lack of talent won't be resolved any time soon, it's important to adapt and consider new approaches, including SASE, or secure access service edge, and working with expert managed services providers.

IS SASE THE SILVER BULLET?

The short answer? No. The longer answer is SASE is not a capability you turn on with the flip of a switch. It's an architecture that brings network and security functions together, typically delivered as-a-service, and often includes SD-WAN, secure web gateways, cloud access security brokers, firewall as a service, and zero-trust network access.

THE MARKET FOR SASE WILL GROW AT A

**CAGR OF 29%
THROUGH 2027.²**

SEE SASE AS THE END GOAL

Instead of a silver bullet, approach a SASE framework as a path to creating a stronger security posture over time. Done correctly, your approach to SASE is viewed as a journey that's aligned to your business mission—which is where you need to begin. Here are some drivers that can influence which parts of SASE may be important to you.

BUSINESS PRIORITY	CONSIDERATIONS	SASE COMPONENTS
Reduce complexity to improve total cost of ownership and agility.	- Where are your teams bogged down in tool management? - How has cloud and edge increased your complexity? - How mature is your investment in automation? - Where might managed services simplify operations?	- Cloud-based security functions - Platform approach to reduce niche and point-product tools
Formalizing hybrid workforce strategies to securely support onsite, at-home, or roaming workers plus contractors.	- How will you secure users and the resources they access, regardless of where and what they are connecting from? - Do you have the resources and expertise to architect, deploy, and manage zero trust network access?	Zero-trust network access
Firmly invested in multiple clouds and may continue maintaining an existing data center.	- How do you secure and protect your cloud assets? - How do you keep up with each technology stack? - How do you create consistency across clouds? What is the “tax” you pay for the uniqueness of each cloud? - Are the cloud-native capabilities enough to meet compliance? Protect assets?	- Secure web gateways - Cloud access security brokers (CASB) - Firewall as a service (FWaaS)
Need to securely connect branch or edge sites to data center and cloud resources.	- What do your sites/edges need access to? - How important is performance at the edge? - What connectivity solutions are in place today and what does it take to manage them? Keep them secure?	Software-defined wide area network (SD-WAN)
Can't risk non-compliance.	- What damage can occur from non-compliance? - Do you have the deep, evergreen expertise needed to meet industry and regional requirements? - Is your reporting adequate for all stakeholders?	- Zero trust network access - SD-WAN
Damage from a breach could cause catastrophic damage to customer trust, productivity, revenue.	- How confident are you in keeping up with emerging, evolving threats across a complex landscape? - Where are your weaknesses in detecting, containing, and recovering from attacks?	- FWaaS - SWG - CASB
Address infrastructure and security skills shortages.	- How will you retain resources and keep them trained on the latest and greatest? - How might you augment teams with outside expertise or managed services?	- Professional services - Managed services

ZERO-TRUST NETWORK ACCESS

One of the key components of SASE is zero-trust networking. With traditional network security, if you are allowed to come in through the “front door”, perhaps via VPN, secure remote access (SRA) or through a connected branch, you are assumed authorized and can go anywhere on the network. As boundaries between environments blur, modern networks have needed to shed the concept of a front door. Zero-trust network access, or ZTNA, protects every door to every room, and you’re only allowed to enter when you have the proper authorization. Zero trust represents a fundamental shift that assumes anyone on the network can be an intruder. ZTNA prevents attackers from traversing the virtual or physical network to look for resources to exploit. If someone’s laptop or credentials are stolen, it doesn’t automatically mean your company is at risk to a cyber threat.

BY 2026,

***10% OF LARGE
ENTERPRISES***

***WILL HAVE A COMPREHENSIVE, MATURE, AND
MEASURABLE ZERO TRUST PROGRAM IN PLACE, UP
FROM LESS THAN 1% IN 2023.³***

SHIFT TO OPEX FOR INFRASTRUCTURE AND SECURITY

Data is growing, your IT landscape is expanding, and your bandwidth and infrastructure needs can vary over time. Perhaps you’re starting to outgrow the hardware you purchased for your on-premises firewall. Shifting security functions to the cloud can help unload static, hardware investments (CapEx) and allow for the ability to expand and contract with a more consumption model option (OpEx). When you move a security function to the cloud, everything is virtualized so it’s easy to scale up or down, support mergers and acquisitions quickly, scale back if your user base shrinks, and get the control you need to be efficient and control costs. This is a key benefit of a SASE framework and provides needed flexibility in today’s volatile, digital world.

GTT ENABLES A SASE JOURNEY THAT IS RIGHT FOR YOU

GTT offers the flexibility you need for your SASE journey. We support a multi-vendor, best-of-breed or single vendor approach, including the configuration, deployment, and management of security services powered by Fortinet, with a tiered managed services support model. GTT has the industry, technology, and security expertise to understand your requirements and risk and recommend the right SASE framework for your business—this includes working with your existing solutions, and even managing them in some cases, so you can maximize investments and create a less disruptive path to improved security and operations.

GTT SECURE CONNECT, A SASE FRAMEWORK

GTT Secure Connect protects enterprises with the people, processes, and tailored designed solutions that meet the customer's needs, requirements, and compliance demands to defend against the ever-growing threat landscape. It allows you to maximize investment, reduce risk, and control your security posture with GTT's expanded Secure Connect portfolio providing flexibility and choice with a trusted partner who can manage your network and security saving time, simplifying business operations, and delivering the best experience for your organization.

GTT Secure Connect integrates multi-vendor solutions for SD-WAN and secure service edge (SSE) functionality, including SD-WAN, CASB, ZTNA, SWG and FWaaS into a single, networking and cloud-based cybersecurity solution.

Rapidly onboard applications in a secure environment.	Support business compliance requirements.	Proactively protect users and applications, even when not connected to the internet.	Improve TCO with an asset light solution built for customers looking to build a zero-trust network.
Choose the right managed service tier.	Minimize latency and maximize uptime running on an industry leading Tier 1 IP backbone.	End-to-end local support backed by global expertise.	Eliminate security concerns around commingled data and a shared management plane with private deployment design.

VISIBILITY INTO APPLICATIONS AND NETWORK

GTT leverages Fortinet FortiAnalyzer and other Fortinet logging capabilities to manage the network. For example, seeing the top ten active applications on your network and their top users according to browsing time or bandwidth can provide important insights into app abuse or visits to inappropriate or unauthorized web sites. With improved visibility, you have the knowledge to determine what you need to control. GTT customers get this and more with access to reports and a tiered managed services solution providing empowerment to make changes or access GTT's team of experts.

THE GTT INFRASTRUCTURE DIFFERENCE

It's common for cloud security services to be hosted in a rented virtualized space provided by cloud providers such as AWS or Azure. This causes concern for some organizations as this space is typically multi-tenanted and your traffic can be inspected in the same place as other organizations using the service. If a consumer of the service is threatened, say by a DDoS attack, you may feel the effects of the constrained bandwidth, even if you're not the target. There is also concern with unauthorized access to data if it commingles.

By contrast, GTT builds a customer dedicated, private cloud security network. Leveraging its Tier 1 IP network and more than 450 points of presence (POPs) around the world, the network is designed and deployed to meet your business objectives and focused only your company's mission. There is zero possibility of commingling data with other organizations. GTT network customers get the added benefit of keeping all traffic with a single network provider, further enhancing performance and control.



ABOUT GTT

GTT is a managed network and security services provider to global organizations. Our services are uniquely enabled by our top-ranked, global, Tier 1 IP backbone, which spans more than 260 cities on six continents.

ABOUT FORTINET

For over 20 years, Fortinet has been a driving force in the evolution of cybersecurity and the convergence of networking and security. Our security solutions are among the most deployed, most patented, and most validated in the industry. Learn more about our solutions at fortinet.com.

LEARN MORE

GTT is ready to help you on your SASE journey to improve security and compliance. To learn more, please visit gtt.net.

Sources:

1. ISC2, 2023 ISC2 Cybersecurity Workforce Study, Oct 2023
2. Gartner, Forecast Analysis: Secure Access Service Edge, Worldwide, Oct 2023
3. Gartner, Hype Cycle for Zero Trust Networking, July 2023