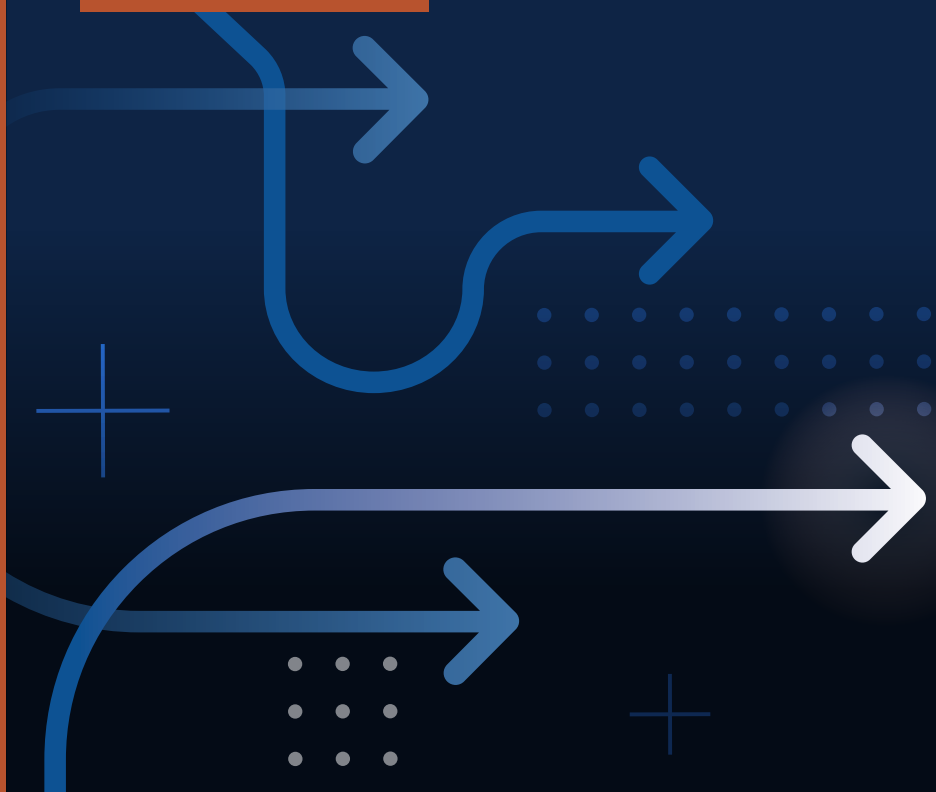


COMMISSIONED BY:

T Mobile

Secure Mobility with T-Mobile 5G

SECURITY & RISK








GigaOm CxO Decision Brief: Secure Mobility with T-Mobile 5G

	Solution Overview	2
01	Solution Value	3
02	Urgency & Risk	4
03	Benefits	7
04	Best Practices	8
05	Organizational Impact	9
06	Solution Timeline	10
07	Analyst's Take	11
08	About the Author.....	12
	About GigaOm	13





Solution Overview

T-Mobile SASE with T-SIMsecure delivers secure, reliable 5G connectivity for remote work, integrating advanced security features directly into the T-Mobile network.



Benefits

The solution enhances cybersecurity and productivity by providing seamless, high-speed, and secure internet access for remote and mobile employees.



Urgency

Immediate adoption of T-Mobile SASE with T-SIMsecure is critical to mitigate rising cybersecurity risks associated with remote work.



Impact

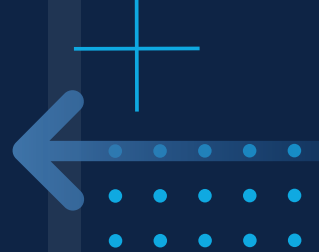
Adopting this solution significantly boosts operational efficiency and cybersecurity, requiring an IT management shift to handle 5G-connected devices.



Risk

Delaying the deployment exposes businesses to increased cybersecurity risks, potential data breaches, and reduced productivity.

01 Solution Value



This GigaOm CxO Decision Brief commissioned by T-Mobile

T-MOBILE SECURE ACCESS SERVICE EDGE (SASE) with T-SIMsecure addresses the critical need for secure remote connectivity in the modern workplace. With remote work now an integral part of business operations, T-Mobile leverages its nationwide 5G network to provide robust security capabilities and seamless internet access. T-SIMsecure enables comprehensive cybersecurity for devices on the T-Mobile network by integrating advanced security features directly into the authentication process, making it an indispensable tool for businesses aiming to protect their remote workforce.



“T-Mobile leverages its nationwide 5G network to provide robust security capabilities and seamless internet access”

02 Urgency & Risk

THE RISE OF REMOTE WORK has exposed organizations to heightened cybersecurity risks. Immediate deployment of T-Mobile's 5G T-SIMsecure is crucial for businesses with significant remote operations, particularly in finance and healthcare industries where data security is paramount. Delaying adoption could result in vulnerabilities, especially from unsecured public Wi-Fi networks, leading to potential data breaches and financial loss.

Urgency

Immediate deployment of T-Mobile SASE with T-SIMsecure is crucial for businesses with mobile and remote workforces, as it provides security for employee laptops wherever they are working from at any given time. Delaying adoption could increase cybersecurity risks, reduce productivity, and create a competitive disadvantage. The rapid shift towards remote work necessitates secure, reliable connections to corporate data and sanctioned resources through prescribed policies on SASE gateways, bypassing the risks associated with public networks.

Specific Use Cases



Hybrid/remote employees: Employees working from home or shared spaces require secure corporate data and applications access. T-SIMsecure employs zero trust network access (ZTNA) principles to ensure that their devices are protected, maintaining the integrity of sensitive corporate data. This goes beyond the security enhancements made by 5G technology and secures the device traffic to a higher level.



Field technicians: Technicians working in remote locations often lack secure Wi-Fi access. Deploying 5G-connected devices allows them to perform their tasks without exposing critical data to cyber threats.



Mobile workers: Employees who spend significant time on the move or at various off-site locations benefit from the seamless and secure connectivity provided by T-SIMsecure, ensuring continuous protection against cyber threats.

02 Urgency and Risk



“Security is a critical capability not only for organizations directly, but has become a requirement in the organizations they partner with.”

Negative Impacts of Delaying

Delaying the deployment of T-Mobile's 5G T-SIMsecure solution can lead to several negative consequences:

- **Increased cybersecurity risks:** Unsecured devices connecting to public Wi-Fi networks are more susceptible to cyberattacks, leading to potential data breaches and financial losses.
- **Reduced productivity:** Employees may experience connectivity issues, hindering their ability to work efficiently and securely from various locations.
- **Competitive disadvantage:** Security is a critical capability not only for organizations directly, but has become a requirement in the organizations they partner with. Failing to take the proper and available security measures leaves you at a disadvantage when your customer looks for those robust security measures in their partners.

Delaying the implementation of advanced security solutions like T-Mobile's 5G T-SIMsecure may result in missed business opportunities, as potential partners or clients may choose to work with competitors who can demonstrate robust security measures. This can lead to lost revenue, reduced market share, and diminished long-term growth prospects. Adopting these solutions promptly can open doors to new partnerships and business models that rely on secure, flexible connectivity.

02 Urgency & Risk

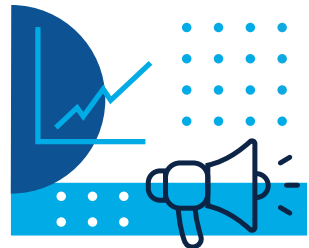
Organizations with Acute Urgency

- **Financial institutions:** With stringent data protection requirements, financial organizations must prioritize the security of their remote workforce to prevent data breaches.
- **Healthcare providers:** Protecting patient data is critical, and healthcare providers must ensure that all remote connections are secure to comply with regulations and maintain patient trust.
- **Legal firms:** Handling sensitive client information necessitates robust security measures to prevent unauthorized access and ensure confidentiality.
- **Energy/mining/oil and gas:** Industries such as these are highly remote by nature, and they often have little to no ability to deploy infrastructure due to environmental, mobility, or geography restrictions. A secure 5G solution can solve many of the issues and challenges faced by workers in foreign countries, at remote outposts, or inspecting miles of infrastructure for faults and defects.

Deploying the T-Mobile 5G T-SIMsecure solution is not just a proactive measure, but a necessary step to safeguard remote operations and maintain business continuity in an increasingly digital world.

Risk

The rise of remote work has exposed organizations to heightened cybersecurity risks. Public Wi-Fi, in particular, poses significant dangers due to vulnerabilities such as man-in-the-middle attacks, spoofing, legacy VPNs, employee awareness, and weak passwords. Businesses cannot control the security of external Wi-Fi networks, but they can control how their employees connect.



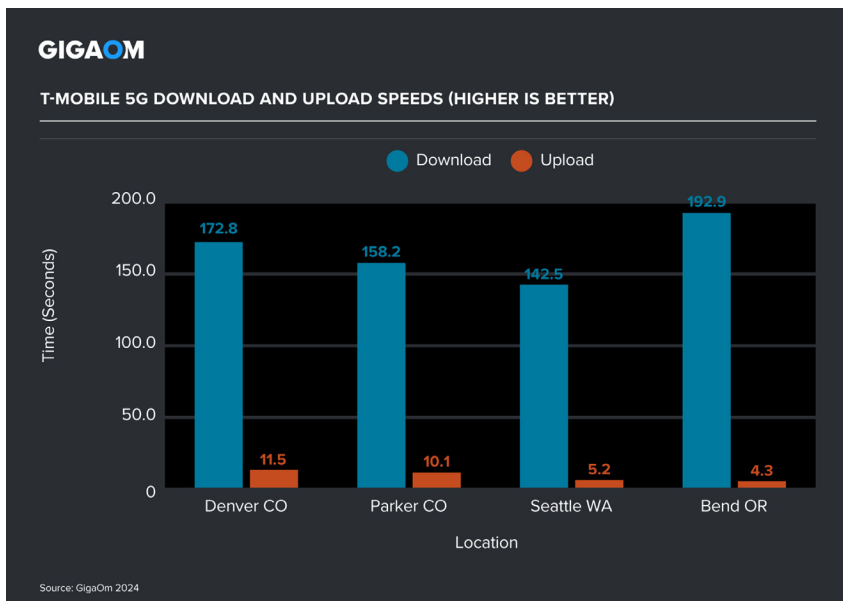
Using public Wi-Fi can lead to data breaches and financial losses. It only takes one employee making one wrong click to cause a breach. Therefore, it is imperative to protect remote workers and their devices as completely as possible.

03 Benefits

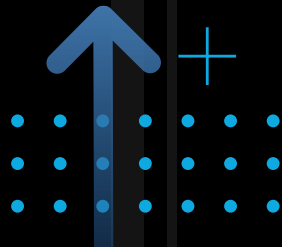
T-MOBILE'S 5G T-SIMSECURE offers several compelling benefits for businesses:

- **Enhanced security:** Built-in security features such as end-to-end encryption and automatic authentication protect against cyber threats.
- **Increased productivity:** Reliable, high-speed internet access anywhere boosts productivity for remote and mobile employees.
- **Cost efficiency:** Potential savings through T-Mobile's device subsidy program and reduced reliance on third-party security software.
- **Future proofing:** Investment in 5G technology ensures long-term competitive advantage and adaptability to evolving work models.

Hands-on testing of laptops optimized for the T-Mobile 5G network showed impressive performance and consistency across locations. With average download speed of 166.6 Mbps across the four locales, and tested latencies at or below 60 ms, the 5G laptops are highly capable for remote work scenarios.

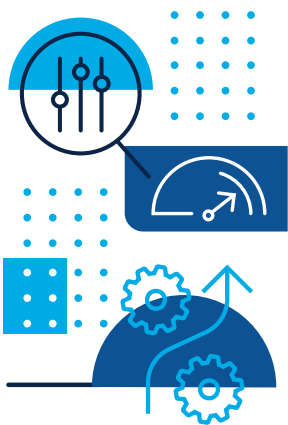


04 Best Practices



TO MAXIMIZE THE BENEFITS of T-Mobile SASE with T-SIMsecure, businesses should follow these best practices:

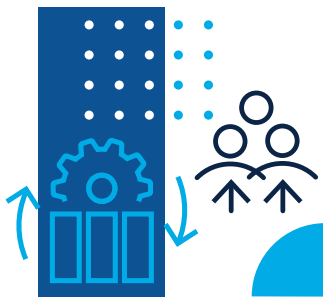
- **Comprehensive training:** Ensure all employees are trained on using 5G-connected devices and security protocols.
- **Regular updates:** Keep all devices updated with the latest security patches and software.
- **Integration with existing security systems:** Seamlessly integrate 5G-connected devices with existing IT and security infrastructure.
- **Usage and performance monitoring:** Regularly monitor device usage and performance to address any issues or threats quickly.



“To maximize the benefits of T-Mobile SASE with T-SIMsecure, businesses should follow these best practices: Comprehensive training, regular updates, integration with existing security systems, and usage and performance monitoring.”

05 Organizational Impact

ADOPTING T-MOBILE'S SASE with T-SIMsecure will significantly enhance overall cybersecurity and operational efficiency. This solution requires a shift in IT management practices, with an increased focus on managing 5G-connected devices and ensuring they adhere to corporate security policies. Training programs need to be implemented to educate staff on new protocols and device usage.



People Impact

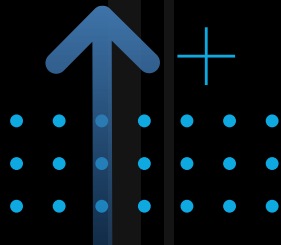
The introduction of 5G T-SIMsecure will necessitate upskilling IT staff to manage and troubleshoot 5G devices. There will be a need for additional support personnel to handle increased security monitoring and device management. Budget considerations will include initial investment in 5G devices and ongoing costs for training and support.

- **Staff training:** Upskill IT staff and end-users on new devices and security protocols.
- **Support structures:** Establish dedicated support teams for managing and securing 5G-connected devices.
- **Budget allocation:** Plan for initial investment and ongoing operational costs.

Investment Outlook

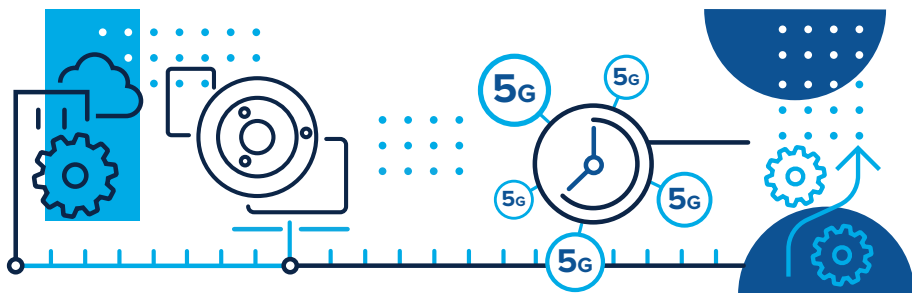
Implementing T-Mobile SASE with T-SIMsecure involves an initial investment in 5G-enabled laptops and access to the full Versa SASE management platform to configure their own rules, which requires customer time and effort. Licensing is typically per device and on a monthly consumption model, with potential subsidies available through T-Mobile's programs. Organizations should plan for long-term budget allocation for device management and refreshes. The return on investment comes through enhanced security, productivity gains, and reduced reliance on third-party security solutions.

06 Solution Timeline



ORGANIZATIONS CAN EXPECT a phased implementation of T-Mobile SASE with T-SIMsecure over 6 to 12 months, depending on the scale of deployment and availability of existing IT resources. The timeline is based on the adoption rate of the organization and their ability to deploy new devices. This timeline includes assessing organizational needs, devising a comprehensive deployment strategy, conducting pilot testing, and rolling out the solution to individual business units. Continuous monitoring and support are essential to address emerging challenges.

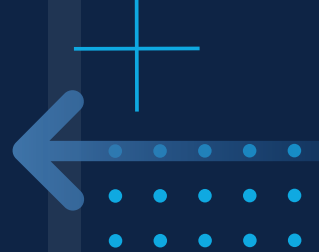
We recommend assessing your organizational needs and devising a comprehensive deployment strategy tailored to your specific business requirements. Follow that by conducting pilot testing with a select group of users who have the most mobility needs and will have the greatest benefit to a secure mobility solution. This will help to identify potential issues and refine full deployment plans. When you begin your deployment, roll out the solution to individual business units, focusing on benefit and geography, ensuring continuous monitoring and support to address emerging challenges.



Future Considerations

Over the next three years, organizations should anticipate advancements in 5G technology and enhancements to T-Mobile's security features. They should regularly review and update security protocols to align with evolving threats and leverage new functionalities introduced by T-Mobile.

07 Analyst's Take



T-MOBILE'S SASE WITH T-SIMSECURE offers a robust solution for businesses navigating the complexities of remote work and cybersecurity. Its unique integration of 5G technology with advanced security features addresses a critical need in today's market. The long-term benefits of enhanced security, increased productivity, and future-proofing make it worthwhile for organizations.



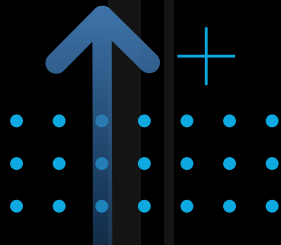
“The long-term benefits of enhanced security, increased productivity, and future-proofing make it worthwhile for organizations.”

Report Methodology



THIS GIGAOM CXO DECISION BRIEF ANALYZES a specific technology and related solution to provide executive decision-makers with the information they need to drive successful IT strategies that align with the business. The report is focused on large impact zones that are often overlooked in technical research, yielding enhanced insight and mitigating risk. We work closely with vendors to identify the value and benefits of specific solutions, and to lay out best practices that enable organizations to drive a successful decision process.

08 About Howard Holton



HOWARD HOLTON IS AN ANALYST AT GIGAOM. He has worked in IT for three decades, the last half in executive leadership, as a CIO and CTO. He has been an engineer, an architect, and a leader in telecom, health care, automotive, retail, legal, and technology.

In the last decade, Howard focused on cloud technology and economics, data analytics, and digital transformation. As CTO of Hitachi Vantara, he spent his time developing digital transformation, IT, and data strategies for Fortune 1000 companies and global governments.

His years at Rheem Manufacturing, Hitachi Vantara, and others provided the experience that helped him develop a mind for leadership—the successful execution of vision and culture to inspire. Successful leadership is all about maximizing your team’s potential, as Howard has demonstrated over the course of his career.

Howard is also a technologist at heart; passionate about how data science and new technologies can be used to accelerate time-to-market and better serve the customer, now and in the future. Howard has been a trusted advisor and agent of change to a number of organizations, bringing vision and successful execution to internal and external customers alike.



About GigaOm

GigaOm provides technical, operational, and business advice for IT's strategic digital enterprise and business initiatives. Enterprise business leaders, CIOs, and technology organizations partner with GigaOm for practical, actionable, strategic, and visionary advice for modernizing and transforming their business. GigaOm's advice empowers enterprises to successfully compete in an increasingly complicated business atmosphere that requires a solid understanding of constantly changing customer demands.

GigaOm works directly with enterprises both inside and outside of the IT organization to apply proven research and methodologies designed to avoid pitfalls and roadblocks while balancing risk and innovation. Research methodologies include but are not limited to adoption and benchmarking surveys, use cases, interviews, ROI/TCO, market landscapes, strategic trends, and technical benchmarks. Our analysts possess 20+ years of experience advising a spectrum of clients from early adopters to mainstream enterprises.

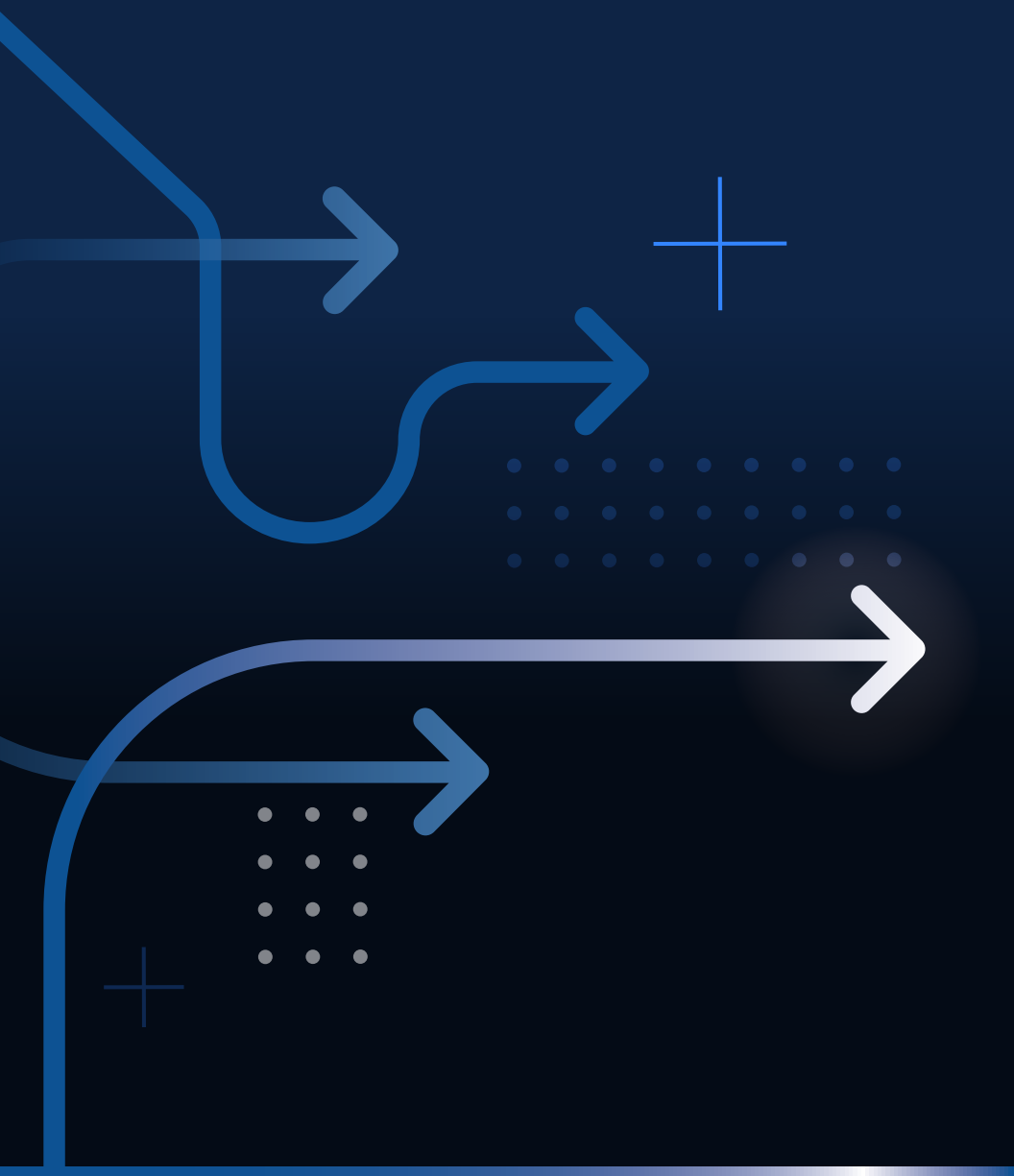
GigaOm's perspective is that of the unbiased enterprise practitioner. Through this perspective, GigaOm connects with engaged and loyal subscribers on a deep and meaningful level.



Copyright

© Knowingly, Inc. 2024 "CxO Decision Brief: Secure Mobility with T-Mobile 5G" is a trademark of Knowingly, Inc.

For permission to reproduce this report, please contact sales@gigaom.com.



GIGAOM

GigaOm democratizes access to strategic, engineering-led technology research. We enable businesses to innovate at the speed of the market by helping them to grasp new technologies, upskill teams, and anticipate opportunities and challenges. The GigaOm platform changes the game, by unlocking deep technical insight and making it accessible to all.