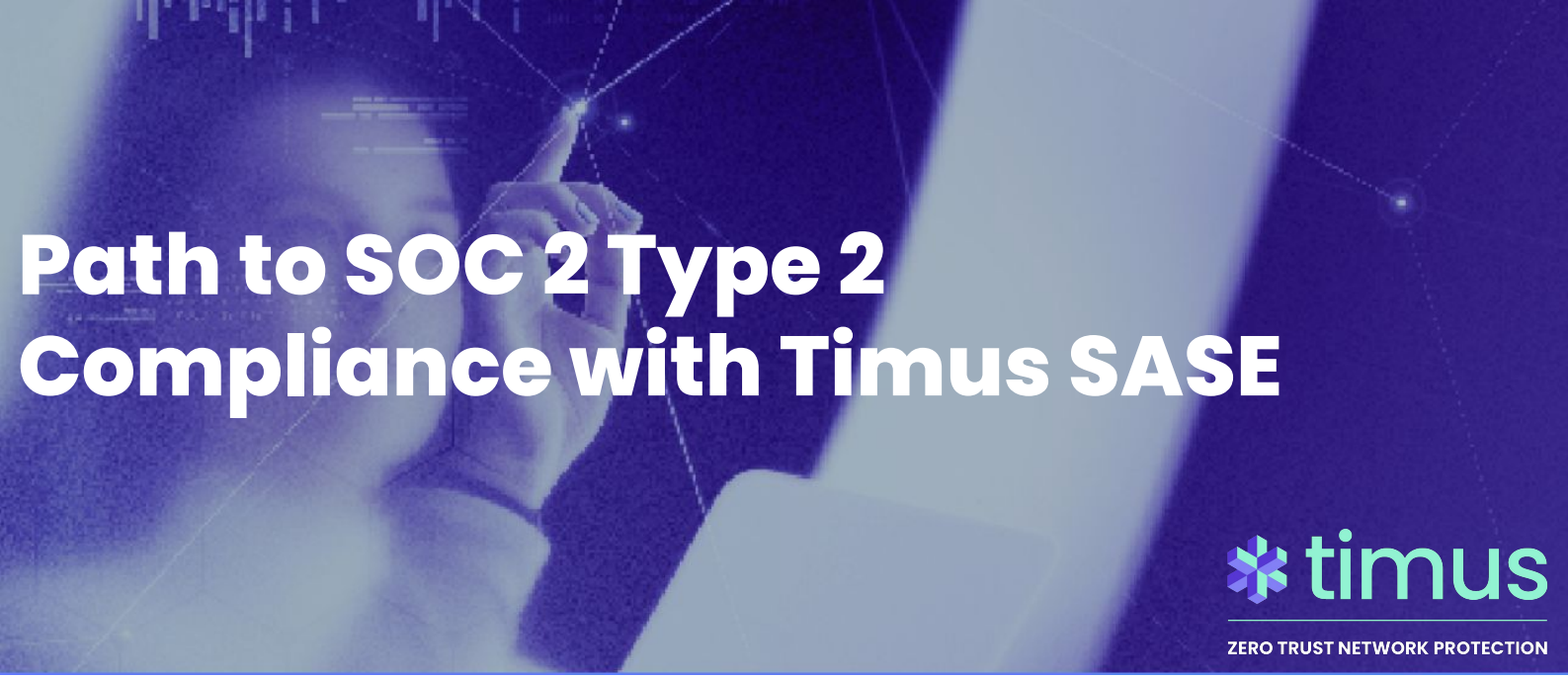


Path to SOC 2 Type 2 Compliance with Timus SASE

timus
ZERO TRUST NETWORK PROTECTION

1. The Significance of SOC 2 Type 2 Compliance

SOC 2 Type 2 is a security framework that specifies how organizations should protect customer data from unauthorized access, security incidents, and other vulnerabilities. At its core, SOC 2 Type 2 was designed to establish trust between service providers and their customers. Achieving SOC 2 Type 2 compliance symbolizes an organization's determination to uphold robust security measures and safeguard sensitive data. Meeting the SOC 2 Type 2 requirements bolsters the efficiency of an organization's security operations, fostering trust among stakeholders.

By leveraging Timus SASE, organizations can enhance their security posture and meet the rigorous demands of SOC 2 Type 2 compliance.

Timus Synopsis:

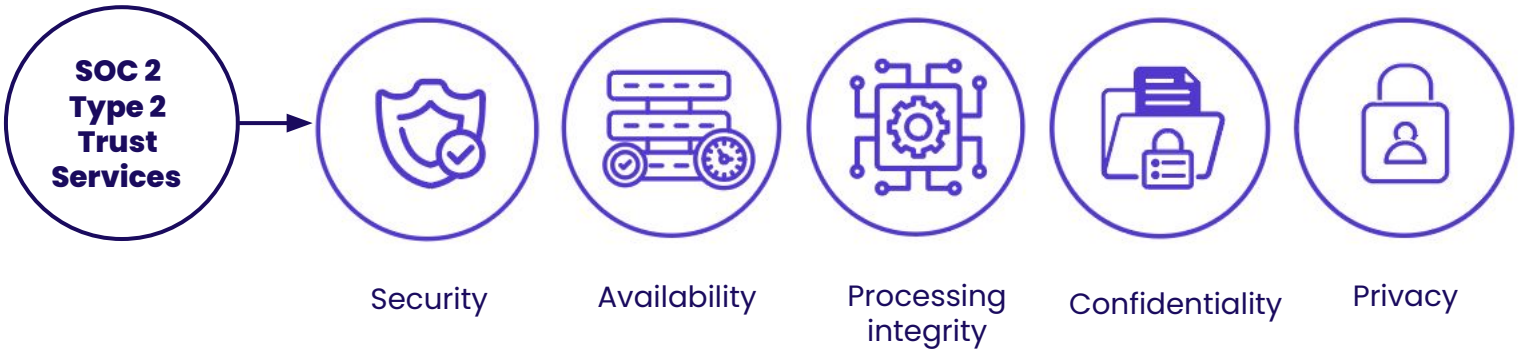
Timus SASE is a comprehensive cloud-based network security solution based on a zero-trust framework, designed to bolster secure connectivity for hybrid workforces. It provides a suite of features to enhance information security, including asset management, vulnerability identification, access control, incident response, and risk assessment.

Timus Networks is SOC 2 Type 2 and ISO 27001 Compliant, and uses AES 256 bit encryption.

© Timus Networks, Inc. 2025 All Rights Reserved.

2. Fulfilling SOC 2 Type 2 Trust Services Criteria

SOC 2 Type 2 compliance is achieved across 5 main trust services criteria: security, availability, processing integrity, confidentiality, and privacy. Timus SASE can help achieve compliance with all.



2.1. Managing Assets

Timus SASE assists organizations in identifying, documenting, and maintaining records of system components, including infrastructure, software, and other information assets.

It facilitates the management of physical endpoint devices, virtual systems, data flows, external information systems, and organizational roles.



© Timus Networks, Inc. 2025. All Rights Reserved.

2.2. Communicating Objectives Related to Confidentiality

Timus SASE enables organizations to effectively communicate their objectives related to confidentiality and the protection of confidential information to external users, vendors, business partners, and other relevant parties.

It facilitates the dissemination of information regarding changes to these objectives, ensuring transparency and maintaining alignment with stakeholders.



2.3. Communicating System Responsibilities

Timus SASE provides a mechanism for communicating system responsibilities to external users involved in designing, developing, implementing, operating, maintaining, and monitoring system controls.

It ensures that these individuals have the necessary information to carry out their responsibilities effectively.

2.4. Analyzing Threats and Vulnerabilities from Vendors, Business Partners, and Other Parties

Timus SASE incorporates a risk assessment process as part of its Zero Trust Network Access screening layer that includes the analysis of potential threats arising from vendors, business partners, customers, and other third parties with access to the organization's information systems.

It helps organizations understand and mitigate risks associated with external entities.



© Timus Networks, Inc. 2025. All Rights Reserved.

2.5. Establishing Relevant Technology Infrastructure Control Activities

Timus assists management in selecting and developing control activities over the technology infrastructure.

It ensures the completeness, accuracy, and availability of technology processing through the implementation of relevant control measures.

2.6. Establishing Relevant Security Management Process Control Activities

Timus supports the establishment of control activities designed to restrict technology access rights to authorized users based on their job responsibilities.

It helps protect the organization's assets from external threats through the implementation of appropriate security management processes.



2.7. Restricting Logical Access

Timus enables organizations to restrict logical access to information assets, including infrastructure, software, and data, through access control software, rule sets, and configuration hardening processes.

It ensures that only authorized users have access to sensitive information and resources

2.8. Considers Network Segmentation

Timus promotes the use of network segmentation, zero trust architectures, and other techniques to isolate unrelated portions of the organization's information technology based on the risk mitigation strategy.

It helps prevent lateral movement and restricts unauthorized access within the network.

© Timus Networks, Inc. 2025. All Rights Reserved.

2.9. Manages Points of Access

Timus SASE assists organizations in identifying, inventorying, and managing points of access by external entities.

It helps track the types of data flowing through these access points and ensures appropriate management of individuals and systems using them.

2.10. Restricts Access to Information Assets

Timus SASE supports the establishment of access control rules and configuration standards for information assets.

It utilizes various measures such as data classification, separate data structures, port restrictions, access protocol restrictions, user identification, and digital certificates to restrict access to protected information.

2.11. Restricts Access to and Use of Confidential Information for Identified Purposes

Timus SASE helps organizations restrict logical access to and use of confidential information to identified purposes only.

It ensures that access to sensitive data is limited to authorized personnel and prevents unauthorized use.

2.12. Restricts Access to and the Use of Personal Information

Timus SASE enables organizations to control access to and use of personal information.

It ensures that only authorized personnel with a legitimate need can access and utilize personal information, aligning with privacy objectives.



© Timus Networks, Inc. 2025. All Rights Reserved.

2.13. Uses Access Control Structures

Timus SSE promotes the use of access control structures, such as role-based access controls, to restrict access to protected information assets.

It helps limit privileges, support segregation of incompatible functions, and enforce least privilege principles.

2.14. Reviews Access Roles and Rules

Timus SASE facilitates the periodic review of access roles and rules to identify unnecessary and inappropriate individuals, system/service accounts, and access privileges.

It ensures that access rights are aligned with business requirements and modified as necessary.

2.15. Restricts Access

Timus SASE enables organizations to restrict activities that can occur through communication channels, such as any web sites or networks.

It helps prevent unauthorized activities and potential security breaches.

2.16. Mitigates Ongoing Security Incidents

Timus SASE assists organizations in establishing procedures to mitigate the effects of ongoing security incidents.

Its real-time alert system helps contain and remediate security incidents promptly to minimize their impact.

2.17. Remediates Identified Vulnerabilities

Timus SASE facilitates the development and execution of remediation activities to address identified vulnerabilities.

It helps organizations close security gaps and strengthen their overall security posture.



© Timus Networks, Inc. 2025. All Rights Reserved.

2.18. Assesses Vendor and Business Partner Risks

Timus SSE enables organizations to inventory, tier, and assess threats arising from relationships with vendors and business partners.

It helps identify potential risks, including security vulnerabilities, operational disruption, and failure to meet regulatory requirements.

2.19. Informs Data Subjects If Access Is Denied

Timus SASE supports organizations in informing data subjects when their access to personal information is denied.

It ensures timely communication, providing transparency and compliance with applicable laws and regulations.



2.20. Responds to Data Controller Requests

Timus SASE helps organizations establish a process to respond to data controllers' update requests, including updates to personal information and denial of requests.

It ensures compliance with service agreements and supports privacy objectives.

2.21. Communicates Denial of Access Requests

Timus SASE facilitates the communication of denial of access requests to data subjects.

It provides written explanations for denial, outlines the legal basis for denial, and informs individuals of their rights to challenge such denial.

© Timus Networks, Inc. 2025. All Rights Reserved.



3. Conclusion

Timus SASE offers a comprehensive suite of features that align with SOC 2 Type 2 compliance requirements. By leveraging Timus SASE, organizations can effectively manage assets, communicate objectives, identify vulnerabilities, analyze threats, establish control activities, restrict access, mitigate incidents, remediate vulnerabilities, assess vendor and business partner risks, and respond to data controller requests.

Incorporating Timus SASE into an organization's security infrastructure strengthens its security posture, promotes transparency, and ensures compliance with SOC 2 Type 2, and other stringent security criteria.

timus

timusnetworks.com

About Timus

Timus Networks simplifies network security and access for SMBs and mid-market enterprises helping to significantly reduce business risks and bolster compliance. Our premier product, Timus SASE, transforms complex setups involving multiple tools into a single, unified solution that secures networks and safeguards users, regardless of their location or device.

Developed by firewall experts with decades of cybersecurity experience, Timus SASE is purpose-built for the MSP/MSSP Channel. It offers simplicity and rapid deployment, with installation in under 30 minutes.