

SOC 2 Type 1 Audit Report

for

Netspective


2313 Falling Creek Rd
Silver Spring, MD 20904

prepared by

Dathan Scott, CPA
Lead Auditor


X 

Dathan Scott, CPA

 (202) 696-4678

 admin@prowative.com

 www.prowative.com

 17781 Woods Overlook Dr.
Dumfries, VA 22026

Netspective SOC 2 Type 1 Audit Report

Table of Contents

1. Executive Summary
2. Independent Service Auditor's Report
3. Management's Assertion
4. Description of the System
5. Applicable Trust Services Criteria
6. Tests of Controls and Results
7. Other Information Provided by Management
8. Appendices

1. Executive Summary

Purpose of the Report:

This SOC 2 Type 1 audit report provides an in-depth assessment of Netspective's systems and controls. The report offers transparency regarding how the organization manages and secures client data, ensuring compliance with the Trust Services Criteria for Security, Availability, and Confidentiality. This detailed evaluation of Netspective's operational controls aims to provide clients and stakeholders with reasonable assurance that the organization is safeguarding sensitive information and operating in a secure environment.

Service Organization:

- **Name:** Netspective
- **Key Contacts:** Shahid Shah, CEO
- **Business Overview:** Netspective specializes in secure hosting and data management services, focusing on providing high-availability platforms that protect the confidentiality of client data through advanced security measures.

Audit Details:

- **Audit Period:** November 1, 2024, to November 30, 2024
- **Trust Service Categories Covered:**
 - **Security:** Ensuring systems are protected against unauthorized access, disclosure, and misuse.

- **Availability:** Ensuring systems are operational as agreed upon and are available for client use without interruption.
- **Confidentiality:** Safeguarding sensitive information from unauthorized access and disclosure.

Auditor Information:

- **Firm Name:** Prowative, Inc.
- **Lead Auditor:** Dathan Scott, CPA
- **Audit Team Contact Information:** Shuaib Shah, shuaib@prowative.com

2. Independent Service Auditor's Report**Scope and Opinion:**

This examination of Netspective's system focused on its ability to provide secure hosting and data management services. The audit assessed the design and implementation of internal controls as of November 30, 2024, with a focus on the Trust Services Criteria for Security, Availability, and Confidentiality. The scope of our audit included an evaluation of key technical, administrative, and physical controls within Netspective's operations.

Responsibilities:

Netspective management holds primary responsibility for the operation and maintenance of the system, including the development and implementation of controls. As the independent auditor, our responsibility was to assess the design and effectiveness of these controls, ensuring they were appropriately implemented to meet the criteria set out by the AICPA's Trust Services Criteria.

Inherent Limitations:

It is important to note that no system of controls can guarantee absolute security or performance. Our audit did not cover all aspects of operational effectiveness, and we recognize the inherent limitations of control systems, particularly when subject to evolving threats or operational changes.

Opinion:

Based on the procedures performed, we believe that the system and controls described by Netspective meet the criteria for Security, Availability, and Confidentiality as of November 30, 2024. We have no reservations regarding the design of the controls and their capacity to provide reasonable assurance of compliance with these criteria.

3. Management's Assertion

Netspective's management asserts that:

- The system description accurately reflects the design and implementation of Netspective's hosting and data management services as of November 30, 2024.

- The controls in place for the Security, Availability, and Confidentiality categories have been suitably designed and implemented to meet the criteria set forth in the applicable Trust Services Criteria.

4. Description of the System

System Overview:

Netspective offers a range of secure hosting and data management services to its clients, including cloud-based solutions that emphasize high availability, data protection, and strict confidentiality. These services are essential for clients requiring robust systems for handling sensitive information.

- **Infrastructure:**
Netspective operates in Tier-4 data centers, ensuring maximum uptime through redundant power and cooling systems. The data centers are geographically distributed, minimizing the risk of service disruption.
- **Software:**
Netspective uses a combination of custom-built software alongside industry-standard solutions to implement data encryption, access control, and monitoring functions. These solutions are continuously updated to ensure they meet the latest security and privacy standards.
- **Personnel:**
The system is managed by a team of qualified IT and security professionals. These personnel have clearly defined roles and responsibilities for system management, incident detection, response, and escalation processes. Regular training ensures that staff remain proficient in the latest security protocols.
- **Processes:**
Continuous system monitoring and incident management are vital to maintaining service integrity. Netspective conducts frequent risk assessments and ensures that all systems are updated regularly to address emerging vulnerabilities.
- **Data:**
The data processed and stored by Netspective includes personally identifiable information (PII), business-critical transactional data, and other confidential client information. Netspective employs strict data handling protocols to ensure all data is secure.

Scope:

The audit covered the primary hosting platform used to deliver Netspective's data management services, including all associated systems that process, store, or transmit client data. Client-specific configurations were excluded from the scope.

5. Applicable Trust Services Criteria

- **CC1-CC9:**
These criteria focus on the governance structure, risk management processes, access control measures, and other operational controls that ensure data protection and system availability. Specific attention was given to how risks are assessed, monitored, and mitigated across Netspective's systems.
- **C1.0 Confidentiality:**
Netspective's data protection policies ensure that confidential information, including PII, is shielded from unauthorized access, using advanced encryption and access control mechanisms.
- **A1.0 Availability:**
Netspective ensures that its systems are operational and available to clients at all times, supported by robust redundancy measures and disaster recovery planning.

6. Tests of Controls and Results

Control Testing Approach:

Our control testing involved a combination of inspection, observation, and system walkthroughs. Key areas of focus included the verification of technical configurations, review of relevant documentation, and testing of security measures, access restrictions, and monitoring tools.

| Control Objective | Control Activity | Testing Performed | Results | |
|----------------------|---|--|--------------|--|
| CC1-CC9 Compliance | Verified all criteria through system review | Reviewed internal documentation and system configurations | Satisfactory | |
| C1.0 Confidentiality | Encryption policies and restricted access | Verified encryption protocols, observed access control mechanisms | Satisfactory | |
| A1.0 Availability | Redundancy and uptime guarantees | Inspected disaster recovery plans, reviewed uptime metrics and system redundancies | Satisfactory | |

7. Other Information Provided by Management

In addition to the controls evaluated during the audit, Netspective's management has provided forward-looking information about planned upgrades to its hosting platform, future investments in system monitoring, and the implementation of next-generation security tools. While this information was not subject to audit procedures, it demonstrates Netspective's commitment to continually improving its security posture.

Appendices

Appendix A: Glossary of Terms

- **PII:** Personally Identifiable Information
- **SOC:** System and Organization Controls

Appendix B: Management Representation Letter

A signed letter from Netspective's management is included, affirming that all information presented in the report is accurate and that the described controls are in place.

Appendix C: Supplemental Information

This appendix includes additional details about planned system enhancements, certifications recently achieved by Netspective, and a roadmap for future compliance efforts.