



SYSTEM AND ORGANIZATION CONTROLS
SOC 3 REPORT
MANAGED THREAT PROTECTION SERVICES

For the period: January 1, 2022, to February 28, 2023

Report Date: April 30, 2023



Management's Report of its Assertions on the Effectiveness of its Controls over Managed Threat Protection Services (System) Based on the Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.



TABLE OF CONTENTS

SECTION I ASSERTION OF NETSURION'S MANAGEMENT 3
ATTACHMENT A..... 5
ATTACHMENT B20
SECTION II INDEPENDENT SERVICE AUDITOR'S REPORT22
APPENDIX A: GLOSSARY 25
APPENDIX B: ABBREVIATIONS.....28

{Remainder of the page left blank intentionally}

SECTION I ASSERTION OF NETSURION'S MANAGEMENT

Assertion of Netsurion's Management

April 30, 2023

We are responsible for designing, implementing, operating, and maintaining effective controls within Netsurion's Managed Threat Protection Services (system) throughout the period January 1, 2022, to February 28, 2023, to provide reasonable assurance that Netsurion's service commitments and system requirements relevant to security, availability, confidentiality, processing integrity, and privacy were achieved. Our description of the boundaries of the system is presented in the Attachment A and identifies aspects of the system covered by our assertion.

Netsurion utilizes SOC 2 Type II compliant data center colocation services provided by Data Foundry (acquired by Switch), Houston Data Center (HOU2) and AWS infrastructure for hosting its servers and service environment. The description (Attachment A) indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary along with controls at Netsurion, to achieve Netsurion's service commitments and system requirements based on the applicable trust services criteria. The description presents Netsurion's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Netsurion's controls. The description presented in Attachment A does not extend and disclose the actual controls at the subservice organizations. The subservice organizations are carved out from the scope of the examination.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period January 1, 2022, to February 28, 2023, to provide reasonable assurance that Netsurion's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality, processing integrity, and privacy (applicable trust services criteria) set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA Trust Services Criteria).

Netsurion's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Attachment B.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period January 1, 2022, to February 28, 2023, to provide reasonable assurance that Netsurion's service commitments and system requirements were achieved based on the applicable trust services criteria relevant to Security, Availability, Confidentiality, Processing Integrity, and Privacy set forth in the AICPA's TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy, if subservice organizations applied the complementary subservice organization controls assumed in the design of Netsurion's controls throughout the period January 1, 2022, to February 28, 2023.

--- **Netsurion**

ATTACHMENT A



Description of Netsurion's Managed Threat Protection Services Relevant to Security, Availability, Confidentiality, Processing Integrity, and Privacy.

Company Background

Netsurion® delivers an adaptive managed security solution that integrates our XDR platform with your existing security investments and technology stack, easily scaling to fit your business needs. Netsurion's managed offering includes our 24x7 SOC that operates as your trusted cybersecurity partner, working closely with your IT team to strengthen your cybersecurity posture. Our solution delivers Managed Threat Protection so you can confidently focus on your core business.

Headquartered in Fort Lauderdale, FL with a global team of security analysts and engineers, Netsurion is a leader in Managed Extended Detection & Response (MXDR). Netsurion has been named a winner in three categories in the 2023 Cybersecurity Excellence Awards. Netsurion was awarded Gold, the top tier honor, for Managed Detection and Response (MDR) and for Threat Hunting. Netsurion also received a Silver award for Extended Detection and Response (XDR).

The Cybersecurity Excellence Awards is an annual competition honoring individuals and companies that demonstrate excellence, innovation, and leadership in information security. Further information about Netsurion is available on the website, www.netsurion.com.

Netsurion's Mission

Cybersecurity threats are incredibly pervasive today. Long gone are the days you expect to prevent all attacks or insider threats. The reality is that growing your business requires a secure and agile IT network through vigilant monitoring, actionable threat intelligence, and continual incident response.

Most organizations have not found a practical way to overcome today's cybersecurity challenges so they can get back to the business of growth and innovation. Why? The cybersecurity solution marketplace is extremely fragmented. At last count, there were over a thousand cybersecurity vendors in over a dozen different solution categories. This makes it very hard just to make a smart solution purchase decision, let alone deploy it quickly and drive it correctly.

Netsurion's Managed XDR solution combines our 24x7 SOC and our Open XDR platform in a co-managed service that gives our customers and partners the ultimate flexibility to adapt and grow while maintaining a secure environment.

Overview of Netsurion's Managed Threat Protection Services

We deliver managed Threat Protection Service with Open XDR technology and 24x7 SOC expertise across your entire IT ecosystem.

Netsurion's Open XDR Platform

Netsurion's open XDR platform unifies your existing security telemetry to deliver wider attack surface coverage and deeper threat analytics resulting in greater security visibility. Some of our platform's key capabilities include: SIEM, UEBA, XDR, and Endpoint Protection.

Dedicated Security Team

Netsurion's SOC does the heavy lifting for you of proactive threat hunting, event correlation and analysis, and provides you with guided remediation. We also provide vulnerability management to identify your soft spots before they can be exploited.

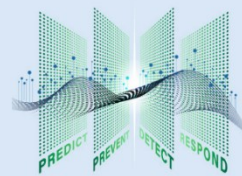
Protect Your Environment Top-to-Bottom

You need to protect your entire IT ecosystem – from cloud infrastructure to on-prem network to endpoints to applications to user behavior. Managed Open XDR from Netsurion covers it all.



Co-Managed SecOps Processes

Netsurion is a force multiplier that allows your IT team to be confident and in control again while also maximizing all of your cybersecurity investments. As an MDR provider, we work with you to create and maintain a co-managed cybersecurity runbook and incident response playbook.



Thwart Attacks End-to-End

Predict and prevent more attacks before they strike. Detect and respond to incidents quickly and completely. Netsurion addresses the entire attack lifecycle - left-of-boom and right-of-boom!

The features and descriptions of the Managed XDR solution are listed below:

Threat Monitoring, Security Orchestration, and Notifications

- 24x7 Monitoring by SOC

The Netsurion Security Operations Center (SOC) operates 24x7x365 and continually monitors security telemetry from the log data streams of customer assets. Alerts, incidents, reports, dashboards, and anomaly detections are generated from these data streams at the Netsurion console to identify Indicators of Compromise (IoCs) and Indicators of Attack (IoAs) that may have occurred in the monitored network.

- Security Information & Event Management (SIEM)

A foundational component to Netsurion's Open XDR platform is SIEM. The platform collects, standardizes, and stores security event logs, and then examines, reports, and acts upon security alerts pulled from the data in real-time.

- Security Orchestration and Automation

Netsurion's Managed XDR solution receives and processes high volumes of system, network, and application telemetry from customer assets. Through automation workflows and guided response, threats are identified, and relevant mitigation steps are developed. In some cases, the necessary mitigation steps can be performed automatically by the platform.

- Priority 1 Alerts

Priority 1 (P-1) alerts are a core function of the Netsurion Managed XDR solution.

For Enterprise Customers –

- P-1 alerts are a set of security or threat related alert conditions that are established at the time of implementation in consultation with Netsurion's implementation team.
- P-1 alerts can be further modified at any time post-implementation.
- Enterprise Customers can deploy P-1 alerts based on their relevant Data Source Integrations (DSIs).

For Essentials Customers

- P-1 alerts are selected by the Netsurion security staff to cover the majority of hardware and software used by SMBs.
- Essentials Customers are provided with a pre-defined set of the most critical and common P-1 alert types for SMBs, selected by Netsurion.

Netsurion's platform constantly analyzes the data received from monitored sources to determine if any security or threat related conditions exist. When threats are detected, the Netsurion SOC analyzes the data and correlates the associated factors with other activity on the impacted customer's systems and network, as well as data available through external threat information resources. P-1 alerts are displayed in the XDR console's incidents dashboard and are visible to both Customers and the SOC when triggered.

Should the P-1 alert be determined to be a true-positive, the SOC will notify the customer within fifteen (15) minutes of that determination and provide all necessary detail to address the concern.

- Priority 2 Alerts

Priority 2 (P-2) alerts are derived from data received from Customer monitored sources. P-2 alerts are comprised of conditions that Netsurion determines may be noteworthy and informational for the Customer, but not likely to be an immediate security issue or threat. These notifications are available for the Customer to review on the console and, for Enterprise customers, are reported on the optional Threat and Incident Review Report.

Support requests are to be submitted via a ticket and are categorized as Urgent, High, or Low by the Customer, Netsurion SOC Manager or Team Leads depending on the nature of the issue being reported.

Managed Endpoint Security

Netsurion Managed Endpoint Security is a managed endpoint threat prevention, response, and analysis service offered by Netsurion® that provides endpoint protection via an easy-to-deploy solution. Netsurion Managed Endpoint Security offers a multi-layer prediction and prevention-first approach, followed by detection and response against known and unknown cyber threats.

Netsurion Endpoint Security Service Components

The service is based on three technical components, one is a lightweight sensor deployed on the endpoint, the second is a hosted console managed by Netsurion, the third is the Netsurion console that may be either hosted at the Netsurion data centers or on Customer premises. It acts as a single-pane-of-glass across all components of the Netsurion service offerings. The 24/7 Netsurion Security Operations Center (SOC) analysts review incidents on the Netsurion console. Sensors are available for Microsoft Windows, macOS, Chrome OS, and Android.

Threats Addressed

- Malware - Prevents Ransomware, Spyware, Trojans, as well as known and unknown threats.
- Static Analysis - Supported File Types - Supports over 100+ file types including executable files, Microsoft Office, PDF, RTF, Flash, JAR, images, fonts, archive files among others.
- File-less Script Based Attacks- Protects against file-less attacks that are script based. This includes PowerShell, MASHTA, JavaScript, VBScript, HTML applications and more.

Service Operating Options

Netsurion Managed Endpoint Security includes two service operating options:

Prevent Threat and Notify – Prevent a process or file (threat) and notify Customer of action taken. Upon Customer confirmation, the SOC may reverse the prevention protocol and update the Customer safelist accordingly. This option provides the Netsurion SOC with the authority to make security decisions but allows customers to retain oversight.

Detect Threat and Notify – Detect threat, notify Customer, and await guidance. When a potential threat is observed, Netsurion SOC will notify Customer and await confirmation on any actions to be taken. This option provides Customers the opportunity to make ad hoc security/safelist decisions. Netsurion SOC will respond as instructed. Action will be taken based on the model of operation in effect.

Alerts

This service offering provides alerts which will be in the Netsurion console and are visible to Customers on the Incidents Dashboard. Critical Alerts will be escalated to the Customer.

Netsurion Managed Endpoint Security will trigger an alert for all detection events visible in the Netsurion console monitored 24/7 by the Netsurion SOC. The SOC will notify the Customer as per the incident call tree instructions. Upon completion of forensic analysis, the Netsurion SOC will update the Customer with guided remediation recommendations. Customers may direct the Netsurion SOC to update their safelist or other configurations.

Netsurion Managed Endpoint Security Service Deliverables

Netsurion Managed Endpoint Security generates incidents, dashboards, and reports based on detection and prevention events that are available for review on the Netsurion console for partners and customers based on user privilege settings.

Add-On Threat and Incident Review Report – Netsurion Managed Endpoint Security + Netsurion Enterprise

When Netsurion Managed Endpoint Security is delivered for an existing Netsurion Enterprise Customer, the Add-On Threat, and Incident Review Report (TIRR) can be prepared by Netsurion SOC for the Customer to include the Priority 1 (P-1) alerts observed along with customized guided remediation recommendations. The optional TIRR will be shared as per the Customer subscription service frequency.

- **Security Summary Report** – Netsurion Managed Endpoint Security + Netsurion Essentials

When Netsurion Managed Endpoint Security is added by a Netsurion Essentials Customer, this report is configured to reflect activity observed during a 24-hour period with automated remediation recommendations. Customers are expected to review these reports regularly. The Netsurion SOC may provide additional guidance for specific events.

- **Security Summary Report** – Netsurion Managed Endpoint Security Standalone

When Netsurion Managed Endpoint Security is purchased as a standalone subscription, the Summary report is configured to reflect the activity observed during the previous 24-hour period with automated remediation recommendations. Customers are expected to review these reports regularly.

Netsurion Vulnerability Management

Netsurion Vulnerability Management is a vulnerability management service offered by Netsurion® that provides vulnerability assessment, prioritization, and remediation recommendations via an easy-to-deploy solution. It is an add-on to our Managed Open XDR portfolio of Netsurion Essentials and Netsurion Enterprise.

Service Components

The service is based on three technical components, one is a lightweight scanner node/agent deployed on the site/endpoint, the second is a management console hosted and managed by Netsurion, and the third is the Netsurion console that may be either hosted at Netsurion data centers or on Customer premises. The solution acts as a single-pane-of-glass across all components of the Netsurion service offering.

Scan Types

Netsurion Vulnerability Management supports various types of scans including device discovery, basic vulnerability scan, file content search, configuration assessment, and compliance scans. Netsurion Vulnerability Management Scans and Audits.

Service Deliverables

Netsurion Vulnerability Management generates dashboards and reports based on results that are available for review on the Netsurion console for partners and customers based on user privilege settings. Reports will be posted in the console within 24 hours of scan/audit completion. Customers and Partners are strongly encouraged to review these reports regularly for remediation recommendations and to take proactive steps to mitigate risks.

Vulnerability Summary Report

The Vulnerability Summary Report provides a summary of the assessment, a distribution of vulnerabilities, and the top 10 vulnerabilities found across the targets. This report provides an overview of big-picture results from the assessment and provides details of the following:

- Summary of the assessment
- Vulnerabilities by severity
- Hosts by vulnerability
- Vulnerabilities by class
- Top 10 vulnerabilities
- Top 10 services

Vulnerability Detail Report

The Vulnerability Detail Report starts by providing a summary of the assessment, distribution of vulnerabilities, and top 10 vulnerabilities found across the targets. It then provides complete details of scanned hosts and vulnerabilities including the severity, class, impact, resolution, and technical details. The detailed report provides the following in addition to the summary report:

- List of scanned hosts with number of vulnerabilities detected on each of them
- List of all vulnerabilities detected on each host
- Details of each vulnerability including the severity, class, CVE, CVSS score, impact, resolution, and technical details

Vulnerability Trend Report

The Vulnerability Trend Report provides insights into the status of vulnerabilities compared with the previous scans. This report provides distribution of vulnerabilities as “new”, “pre-existing”, “reintroduced”, and “removed” status.

Add-On Threat and Incident Review Report – Netsurion Vulnerability Management + Netsurion Enterprise

When Netsurion Vulnerability Management service is delivered for an existing Netsurion Enterprise Customer, in addition to above reports, the Add-On Threat and Incident Review Report (TIRR) can be prepared by the Netsurion SOC for the Customer to include the critical insights along with guided remediation recommendations. The optional TIRR will be shared as per the Customer subscription service frequency.

Boundaries of the System

The boundaries of the system are the specific aspects of the Netsurion’s infrastructure, software, people, procedures, and data necessary to provide its services and that directly support the services provided to customers. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to customers are not included within the boundaries of the system.

System Components

The system is comprised of the following components:

Infrastructure including the physical structures, information technology (IT) and other hardware.

Software includes key assets in providing Managed Threat Protection Services.

People

Netsurion is responsible for the management and supervision of personnel involved in providing services delivered to its clients. Netsurion’s staff is organized in the following functional areas.

- Leadership
- Sales and Marketing
- Managed Threat Protection Team (SOC)
- Research and Development Teams
- Finance
- Human resource,
- Infrastructure Team (IT)
- Finance and Operations Team
- Information Security and Compliance Team (ISC)

Procedures

Netsurion has developed the Information Security Management System (ISMS) policies and procedures. The ISMS policies and procedures are reviewed and changes, if any, are authorized by the Information Security Steering Committee (ISSC). Policy documents cover the following key areas:

- Organization’s Information Security,
- Acceptable Use,
- Antivirus and Patch Management,

- Backup and Recovery,
- Change Management,
- Asset Management,
- Human Resources and Training,
- Risk Management,
- Incident Management,
- Information Classification,
- Information Exchange,
- Internet Use,
- Logical Access,
- Network Security,
- Organization Chart,
- Physical Security,
- Vulnerability Management, and
- Recurring Control Review Procedure

Standard Operating Procedures are defined across which are primarily used internally to guide Netsurion employees to support day-to-day operations. All the teams of Netsurion are expected to adhere to Netsurion policies and procedures that define how the services should be delivered, these are located within the organization's SharePoint/intranet portal and accessible to an authorized user.

Data

Netsurion has defined and documented the Asset Management Policy to ensure that information receives an appropriate level of protection in accordance with its importance to the organization.

Netsurion's data is classified as:

- Restricted
- Confidential
- Internal Use Only
- Public

Relevant Aspects of Control Environment, Risk Assessment, Information and Communication, Monitoring Activities, and Control Activities

Control Environment

Integrity and Ethical Values

Ethical values and integrity are cornerstones of Netsurion's corporate culture. These values are emphasized in the Company Handbook. As part of the process, new employees (permanent and contingent) are required to sign a statement indicating that they have read, understood, and will follow the Company Handbook and the organization's policies and procedures.

Organization Structure & Assignment of Authority and Responsibility

Netsurion employs a management team consisting of C-Level leadership in all functional areas. This group reports to the COO / President and, in turn, the CEO. Each functional area is predominantly structured in a hierarchical manner with layers of management employed as appropriate based on organization size, specialization, and duties. Organizational charts are in place to communicate areas of authority, responsibility, and the lines of reporting to personnel.

Commitment to Competence

Netsurion's management defines competence as skills that are required to deliver the assigned tasks that define employee roles and responsibilities. Commitment to competence includes management's consideration of competence levels for particular jobs and how those levels translate into required skills and knowledge. Netsurion has written job descriptions specifying the responsibilities for job positions. Job descriptions are periodically reviewed and updated as necessary. Technical training is provided to employees to expand the knowledge base and improve performance.

Information Security

Netsurion has a formal information security protection program based on ISO 27001: 2013 framework and periodically certifies its compliance with the standards. The information security policy is formally documented, actively monitored, reviewed, and updated to ensure its objectives continue to be met.

An organizational structure is defined for information security which details the reporting lines, authorities, and responsibilities for business operations. The roles and responsibilities of the members of the information security organization are defined. Information Security Policy and information security-related procedural documents for processes are made available to the employees.

Training and Awareness

An information security education and awareness program has been established that includes policy training and periodic security updates to Netsurion's personnel. New hires and existing employees are required to undergo Information Security Awareness Training via a training portal.

Information security related policies and procedures are communicated to the employees during the induction training and are made accessible to employees via SharePoint. Personnel using mobile computing devices/teleworking are trained on the risks, the controls implemented, and their responsibilities.

Netsurion has developed, implemented, and maintained a comprehensive privacy protection awareness and training program to educate relevant personnel on their responsibilities of protecting PII and organizational procedures. Also, modules related to privacy protection and awareness are also covered during the Information Security training conducted for all employees.

The training focused on the technology domain, soft-skills, and behaviour are conducted periodically for employees as part of the learning and capabilities development initiatives of the organization.

Human Resources Policies and Procedures

Netsurion maintains written Human Resources Policies and Procedures. The policies and procedures describe Netsurion's practices related to hiring, learning and development, performance reviews and advancement, code of conduct, disciplinary action, and termination. Employee candidates' ability to meet job requirements is evaluated as part of the hiring evaluation process.

Competency metric exists that defines the competency requirement for every role, the recruitments are carried out based on this. Netsurion requires employees to provide their acceptance on the offer letter that includes employment terms and conditions.

In addition, new joiners are required to sign a 'Non-Disclosure Agreement' at the time of joining. Third party background verification check is conducted for all employees joining Netsurion. All employees are required to authorize a background check by signing a consent form.

Quarterly and Annual performance evaluation is conducted via performance management portal where employees are evaluated based on the performance criteria and organizational values. Netsurion has documented Anti-Harassment Policy to maintain a workplace free of harassment. Awareness training is conducted periodically.

Information and Communication

Netsurion utilizes various methods of communication to help ensure employees understand their roles and responsibilities and the entity's controls. Netsurion's knowledgebase is hosted on their intranet portal to disseminate information to employees. Netsurion has established various communication channels to communicate with external stakeholders. Netsurion provides periodic reporting on operations and other relevant reports as agreed with the clients.

Risk Assessment and Risk Treatment

Risk Assessment and Treatment Procedure is documented to assess risks of information assets and services as per the context stated in the Information Security policy and Service Management Manual. Risk assessment is performed at least annually by ISC Team but may be performed more often in case of any changes to the technical or business landscape or other changes that introduces new risk to the organization to identify and manage risk across Netsurion. Privacy risk assessment is performed on an annual basis by the ISC Team to identify, assess, and mitigate privacy risks.

Monitoring Activities

Netsurion performs periodic Information Security Management System (ISMS)/Service Management System (SMS) reviews and results are reviewed with management. This involves monitoring ongoing effectiveness and improvement of the control environment by reviewing security issues, audit results, and monitoring status, and by planning and tracking necessary corrective actions.

Netsurion undergoes ISO 27001, ISO 20000 independent audits at least annually, to monitor and verify compliance with security and service management system requirements. The findings are recorded, reviewed, prioritized, and remediation plans are developed. Netsurion conducts a PCI DSS audit to ensure that the controls relevant to PCI DSS requirements are effective in the organization to support its PCI DSS certified clients.

Internal audits are performed twice a year as per the Internal Audit Policy & Procedure and effectiveness is documented in the form of the Internal Audit Summary and discussed during the management review meetings. Audit Findings are recorded in the GRC Tool, and remediation is tracked in the tool by the ISC Team.

Control Activities

Access Administration

Access to the customer's information by Netsurion employees is protected by authentication and authorization mechanisms. User authentication is required to gain access to production and sub-production instances.

Access Control Policy is formally documented, reviewed, and approved at least on an annual basis. User registration and de-registration formally address establishing, activating, modifying, reviewing, disabling, and removing accounts. Logical access to Netsurion's systems is restricted through Active Directory based domain policies. Netsurion maintains administrative safeguards for the protection of confidentiality and integrity of customer data.

Password Management

There is a defined password policy configured on the domain controller specifying minimum password length, maximum password age, password complexity requirement, and account lockout.

The organization's password requirements are documented in Access Control Policy published, communicated, and made available to all employees via SharePoint. In-scope system components require a unique username and password before authenticating users.

Before deploying any new devices in a network environment, the organization changes all default passwords for applications, operating systems, routers, firewalls, wireless access points, and other systems to have values consistent with administration-level accounts.

Network Security

Firewalls with IPS modules are implemented and configured to protect the network from external threats and vulnerabilities. The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.

Access to the internet is controlled and monitored through content filtering settings configured in the firewall. All production application servers are hosted behind a WAF to prevent common attack traffic. The IT team is notified of suspicious activity through alerts received from FortiAnalyzer. Alerts are addressed promptly based on the severity. Firewall rules are reviewed bi-annually.

There is no direct connection between the internal network and the internet, all connections to the internet from the internal network are through firewalls. All the connections to the client network are allowed only after reviewing the requirements by the infrastructure team. Connection to the client network is always encrypted and wherever possible Netsurion insists on two factor authentication.

Remote access to Netsurion's network by authorized employees is through VPN connection. Multi-factor authentication is implemented for remote connectivity. Access to AWS instances for ports other than 80 and 443 are allowed only from Netsurion's corporate network.

Endpoint Protection

There exists a documented Antivirus Policy for antivirus management and monitoring. Netsurion Endpoint Security is installed on all workstations and Carbon black on production servers that are in the Netsurion's domain. On a monthly basis, the asset list is compared with the reports to verify whether the Endpoint Security solution is installed on all Netsurion assets.

Netsurion Open XDR agent is installed in all windows systems to detect new/zero-day vulnerabilities. On a monthly basis, the asset list is compared with the Netsurion's Open XDR report to verify whether the Netsurion Open XDR is installed on the systems.

Software Installation

End users in SOC Team do not have permissions to install software on the workstations. Software installation requests are submitted to the IT Team via ticketing tool/ email and carried out based on the approval from the respective manager and/ or ISC Team.

Encryption and USB Management

Full disk encryption is enabled in all user workstations. USB access is disabled for all users in the SOC Team. USB access is requested via email/ticketing tool and approved on the business justification. Approved list of devices and users are maintained by the ISC Team.

Security Configuration

The Infrastructure Team is responsible for security configuration as per the industry standard. Information Security Compliance team conducts configuration audits to verify if the servers, workstations, and network devices are configured as per the standard.

Inventory of Assets

Netsurion maintains an inventory of hardware and software used in the Netsurion network. A list of authorized software is maintained. Netsurion ensures outdated softwares are removed and existing software are fully patched.

Vulnerability Assessment and Penetration Testing

Netsurion conducts a periodic vulnerability assessment to identify potential vulnerabilities, then validate and prioritize them based on scores, such as CVSS for all CVE vulnerabilities, and create a prioritized remediation. In addition, Internal and External PT is conducted once in 6 months. ASV scans (external) are performed on a quarterly basis for assets in PCI DSS assessment scope.

SOC Monitoring

SOC monitors changes in critical systems, network devices and workstations. Security logs are monitored 24/7 by Netsurion's SOC Team. The Critical Observation Report (COR) is published by the SOC team daily to the management and respective teams describing the changes.

The report consists of the below critical activities:

- Threats
- Managed Services like EDR
- Privileged User Monitoring
- Changes to Identity and Access Policies
- Application Activity Monitoring

Change Management

Changes to Netsurion's infrastructure and system is controlled by a defined Change Management Policy. The policy is reviewed at least annually or when significant changes occur. Formally documented change management procedures are in place to govern the modification and maintenance of production systems and address security and availability requirements. Changes are categorized as Standard, Normal, Emergency and Major Changes.

All the changes are made as per the change management policy which comprises of:

- Documentation and Review of Change
- Prioritization of change
- Impact Analysis
- Approvals of changes
- Change Schedule and Plan
- Change Testing
- Change Implementation
- Change Monitoring and Verification
- Change Rollback

The Change Advisory Board (CAB) is responsible to ensure that changes with respect to the production environment or application are authorized and approved on a timely basis. A ticketing system is utilized to track and document changes throughout the change management process

Patch Management

Netsurion has implemented a patch management process to ensure that security updates are patched regularly on servers, network devices and workstations.

Netsurion Open XDR product update/ patch management process is documented which provides detailed information about the process that is defined and followed by the SOC Teams in the Netsurion Open XDR Patch Management.

The Infrastructure Team ensures that all patches are tested before applying to the production environment. On a monthly basis, the ISC Team verifies the application of patches by comparing the patch reports with the asset list.

Information Security Incident Management

An incident management framework has been established and communicated to all employees with defined processes, roles and responsibilities for the detection, escalation, and response of security incidents. Incident Management framework includes the steps of the incident management process and the factors that relate to the whole system.

Business Continuity

Business Continuity Plan is developed to ensure the continuation of the business during and following any critical incident that results in disruption to the normal operation capability. Disaster scenarios, response, and recovery strategies are documented in the Business Continuity Plan.

The plan describes, at a high level, the purpose, objectives, scope, critical dependencies, RTO/RPO, and roles/responsibilities. The mission of Netsurion's BCP Team is to help ensure timely recovery of critical business operations of Netsurion after a business interruption and return to normalcy.

The Business Continuity Plan is reviewed annually or when there is a material change to the situation. The Business Continuity Plan is tested at least twice a year. After BCP tests are performed, outputs of the tests are captured, analyzed, and discussed to determine the scope of the next steps for continuous improvement

Backup, Replication, and Restoration

Netsurion has a documented Backup and Restoration procedure to ensure adequate back-up for recovering essential business information and systems. Netsurion performs automated backup and replication of critical servers hosted in Data Foundry using a comprehensive backup and replication solution.

Third Party Security Policy

Netsurion has established a Third-Party Security Policy. Third-party risks are assessed before signing any contract with third parties and during the annual risk assessment process. Service Contracts along with confidentiality agreements are signed with vendors or third-party providers.

Capacity Management

Netsurion has developed and implemented a capacity management process to manage capacity demand. Capacity Planning is done by process owners and process managers and reviewed during the Technology Steering Committee Meetings. Resource & Capacity Management Information System reports are maintained that provide a concise view of the various parameters that are important to the availability of resources for continuous operations. Infrastructure team monitors the critical servers continuously for the resource utilization.

Physical and Environmental Safeguards

Physical Access to Netsurion's premises is controlled through the access control system, close circuit television cameras and security desk. Close circuit television cameras are installed at key locations.

Environmental protections have been installed in Netsurion's premises and monitored at regular intervals including the following:

- Cooling systems
- Power backup in the event of power failure
- Redundant communications lines
- Smoke detectors
- Fire Extinguishers

Privacy

Netsurion has certified its compliance with the EU-US Privacy Shield Framework as set forth by the US Department of Commerce regarding the processing of certain Personal Information from the European Union member countries and the United Kingdom. Netsurion has adopted this Privacy Shield Policy as part of its overall Privacy Notice to establish and maintain an adequate level of privacy protection.

Netsurion's privacy policy is published on its corporate website in clear and conspicuous language (<https://www.netsurion.com/privacy-notice>). Netsurion uses personal information only for the sole purpose of providing the services as specified in the contractual agreement and privacy policy.

Netsurion has developed, implemented, and maintained a comprehensive privacy protection awareness and training program to educate relevant personnel on their responsibilities of protecting PII and organizational procedures. Also, modules related to privacy protection and awareness are also covered during the Information Security training conducted for all employees. Netsurion performs ongoing procedures for monitoring the effectiveness of controls over personal information and for taking timely corrective actions when necessary.

Subservice Organizations (Carved-Out)

Netsurion utilizes SOC 2 Type II compliant data center colocation services provided by Data Foundry (acquired by Switch), Houston Data Center (HOU2) and AWS infrastructure for hosting its servers and service environment.

The following key controls are expected to be implemented by Subservice Organization however they have not been included in the scope of this examination.

i. Data Foundry

Complementary Subservice Organization Controls

Physical Security: External

- 24x7x365 manned security at gated entry, data center entrances and loading docks
- Mantraps and dual-factor authentication (biometric) access control
- Mantraps at all exterior doors, including loading dock
- Color camera digital surveillance system and security camera with digital video recording and storage

Physical Security: Internal

- Color camera digital surveillance system and security cameras with digital video recording and storage
- Escorted access

- Digital video recording upon every door opening
- Cabinet and cage security options include individual locks and biometric scanners.

Availability (internet, power etc.)

- Dual underground utility feeds
- UPS with N+1 redundancy to supply power in case of utility power failure.
- In the event of extended power outage, onsite diesel generators are in place to generate power until power is restored (Scalable 2.25 MW N+1 diesel generator pre-wired for additional capacity/8,400 gallons, 48 hours of fuel per generator).
- Transformers owned and maintained by Data Foundry
- Closed transition ATS
- Line ups per power train
- STS-switched and dual-input PDUs for fault tolerance
- Power monitoring to the circuit level
- Houston data center consists of carrier neutral with access to multiple providers with 100% uptime

Environmental Safeguards

- 3-layer plan for fire prevention and suppression
- Full HSSD sensors
- Dual interlock, dry-pipe, pre-action sprinkler system
- Multiple redundant Computer Room Air Conditioner (CRAC) and Computer Room Air Handlers to maintain constant temperature and humidity levels in the Data Center.
- Temperature, humidity, fire suppression and smoke detection and action system implementation & monitoring.
- Solid grounding
- Lightning protection system

Disaster Recovery Facility available at Data Foundry Austin.

ii. Amazon Web Services (AWS)

AWS has achieved many compliance certifications including SOC 2 Type II to provide customers assurance that its platform meets customer security requirements and industry standards.

<https://aws.amazon.com/compliance/programs/>.

The type of controls assumed in the design of Netsurion's controls are as follows:

- The system is protected against unauthorized access (both physical and logical).
- The system is available for operation and use and in the capacities, as committed or agreed.
- Policies and procedures exist related to security and availability and are implemented and followed.

Monitoring of Subservice Organizations

Netsurion obtains and reviews the SOC 2 report of Data Foundry and AWS on an annual basis for completeness, accuracy, and relevance to Netsurion's business needs. Reviews include an assessment of complementary user entity controls, subservice organizations, and mapping of the controls to key risks. If there are exceptions, Netsurion reviews the severity and impact of the exceptions, and if needed, follow-up with the subservice organizations.

ATTACHMENT B

Principal Service Commitments and System Requirements

Netsurion makes service commitments to its customers and has established system requirements as part of the Managed Threat Protection Services. Netsurion is responsible for its service commitments and system requirements and designing, implementing, and operating effective controls within the system to provide reasonable assurance that Netsurion's service commitments and system requirements are achieved.

The principal service commitments are communicated via customer contracts/service level agreement, description of service offering provided online, Information Security Management System (ISMS policy), Service Management System (SMS policy).

Netsurion has made commitments to customers with regards to service levels objectives. This involves meeting or exceeding the established SLOs, ensuring that the quality of service provided is consistent and reliable, and addressing any issues or problems that arise promptly and effectively. In order to ensure that SLOs are met, and commitments are fulfilled, Netsurion has implemented processes and procedures that monitor and measure the performance of their services and take corrective action when necessary.

Netsurion has made commitments related to protecting the information and systems and complying with relevant laws and regulations. These commitments are addressed through measures including encryption, authentication mechanisms, physical security, and other relevant security controls.

Netsurion's management establishes operational requirements that support the achievement of service commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated to Netsurion's system policies and procedures, system design documentation, and contracts with customers.

Information Security Management System policy (ISMS policy) is a document with high-level requirements for establishing an Information Security Management System in Netsurion and demonstrate compliance to ISO27001:2013.

It also guides the Information Security Steering Committee, Information Security Officer, Information Security Coordinators, Internal/External consultants, and ISMS users in understanding, implementing, maintaining, and reviewing the required security controls. It also clearly defines the authorities and responsibilities and defines overall direction and policies regarding Information Security. It also assesses and addresses the information risks concerning operational activities, infrastructure, and projects the objective of the ISMS is to support the corporate mission regardless of geographic location. Netsurion is committed to providing secure networks and systems that protect the confidentiality, integrity, and availability of information and data that the organization uses and/or is entrusted with.

Service Management System (SMS Policy) is to provide the highest level of service to Netsurion's customers and ensure that Netsurion continually improves the delivery of services to customers.

Netsurion, therefore, aims to provide the best-in-class service delivery that ensures customer satisfaction on one hand and compliance to industry best practices on the other hand. The existence of SMS Policy is a testimony to management's commitment to continually improve the service management and its commitment to ISO 20000-1:2018 requirements.

SECTION II INDEPENDENT SERVICE AUDITOR'S REPORT

Independent Service Auditor's Report

To Management of Netsurion

Scope

We have examined Netsurion LLC (also referred to as "Netsurion" or "service organization") accompanying assertion titled "Assertion of Netsurion's Management" (assertion) that the controls within Netsurion's Managed Threat Protection Services (system) were effective throughout the period January 1, 2022 to February 28, 2023 to provide reasonable assurance that Netsurion's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality, processing integrity, and privacy (applicable trust services criteria) set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Confidentiality, Processing Integrity, and Privacy (AICPA, Trust Services Criteria).

Netsurion utilizes data center colocation services provided by Data Foundry (acquired by Switch), Houston Data Center (HOU2) and AWS infrastructure for hosting its servers and service environment. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with the controls at Netsurion, to achieve Netsurion's service commitments and system requirements based on the applicable trust services criteria. Our examination did not extend to the controls implemented by subservice organizations.

Service Organization Responsibilities

Netsurion is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Netsurion's service commitments and system requirements were achieved. Netsurion has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Netsurion is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.



Our examination was conducted in accordance with the attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

USA OFFICE

1201 N Orange Street
Suite #7424 Wilmington DE 19801-1186

CONTACT US AT

 +1 (302) 691-9076
 +1 (312) 767-2027

FIND US AT

www.attinkom.com
info@attinkom.com

Our examination included:

- Obtaining an understanding of the system and the service organization service commitments and system requirements.
- Assessing the risks that controls were not effective to achieve Netsurion's service commitments and system requirements based on the applicable trust services criteria.
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Netsurion's service commitments and system requirements based on the applicable trust services criteria.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within Netsurion's Managed Threat Protection Services (system) were effective throughout the period January 1, 2022 to February 28, 2023, to provide reasonable assurance that Netsurion's service commitments and system requirements were achieved based on the applicable trust service criteria, is fairly stated, in all material respects, if subservice organization controls assumed in the design of Netsurion's controls operated effectively throughout the period January 1, 2022 to February 28, 2023.

Sincerely Yours,

Attinkom LLC

April 30, 2023



USA OFFICE

1201 N Orange Street
Suite #7424 Wilmington DE 19801-1186

CONTACT US AT

+1 (302) 691-9076
+1 (312) 767-2027

FIND US AT

www.attinkom.com
info@attinkom.com

APPENDIX A: GLOSSARY

applicable trust services criteria. The criteria codified in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022), in AICPA Trust Services Criteria, used to evaluate controls relevant to the trust services category or categories included within the scope of a particular examination.

authentication. The process of verifying the identity or other attributes claimed by or assumed of an entity (user, process, or device) or to verify the source and integrity of data.

authorization. The process of granting access privileges to a user, program, or process by a person who has the authority to grant such access.

boundaries of the system (or system boundaries). The boundaries of a system are the specific aspects of a service organization's infrastructure, software, people, procedures, and data necessary to provide its services. When systems for multiple services share aspects, infrastructure, software, people, procedures, and data, the systems will overlap, but the boundaries of each system will differ. In a SOC 2 engagement that addresses the confidentiality and privacy criteria, the system boundaries cover, at a minimum, all the system components as they relate to the life cycle of the confidential and personal information within well-defined processes and informal ad hoc procedures.

carve-out method. Method of addressing the services provided by a subservice organization in which the components of the subservice organization's system used to provide the services to the service organization are excluded from the description of the service organization's system and from the scope of the examination. However, the description identifies (a) the nature of the services performed by the subservice organization; (b) the types of controls expected to be performed at the subservice organization that are necessary, in combination with controls at the service organization, to provide reasonable assurance that the service organization's service commitments and system requirements were achieved; and (c) the controls at the service organization used to monitor the effectiveness of the subservice organization's controls.

complementary subservice organization controls (CSOCs). Controls that service organization management assumed, in the design of the service organization's system, would be implemented by the subservice organization and that are necessary, in combination with controls at the service organization, to provide reasonable assurance that the service organization's service commitments and system requirements are achieved.

commitments. Declarations made by management to customers regarding the performance of one or more systems that provide services or products. Commitments can be communicated in written individualized agreements, standardized contracts, service level agreements, or published statements (for example, a security practices statement). A commitment may relate to one or more trust services categories. Commitments may be made on many different aspects of the service being provided, or the product, production, manufacturing, or distribution specifications.

criteria. The benchmarks used to measure or evaluate subject matter.

environmental protections and safeguards. Controls and other activities implemented by the entity to detect, prevent, and manage the risk of casualty damage to the physical elements of the information system (for example, protections from fire, flood, wind, earthquake, power surge, or power outage).

information and systems. Refers to information in electronic form (electronic information) during its infrastructure. The collection of physical or virtual resources that supports an overall IT environment, including the server, storage, and network elements.

APPENDIX A: GLOSSARY

internal control. A process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance.

personal information. Information that is or can be about or related to an identifiable individual.

policies. Management or board member statements of what should be done to effect control. Such statements may be documented, explicitly stated in communications, or implied through actions and decisions. Policies serve as the bases for procedures.

practitioner. A CPA who performs an examination of controls within an entity's system relevant to security, availability, processing integrity, confidentiality, or privacy.

privacy notice. A written communication by entities that collect personal information, to the individuals about whom personal information is collected, about the entity's (a) policies regarding the nature of the information that they will collect and how that information will be used, retained, disclosed, and disposed of or anonymized and (b) commitment to adhere to those policies. A privacy notice also includes information about such matters as the purpose of collecting the information, the choices that individuals have related to their personal information, the security of such information, and how individuals can contact the entity with inquiries, complaints, and disputes related to their personal information. When a user entity collects personal information from individuals, it typically provides a privacy notice to those individuals.

risk. The possibility that an event will occur and adversely affect the achievement of objectives.

security incident. A security event that requires action on the part of an entity in order to protect information assets and resources.

system. Refers to the infrastructure, software, people, processes, and data that are designed, implemented, and operated to work together to achieve one or more specific business objectives in accordance with management specified requirements.

system components. Refers to the individual elements of a system. System components can be classified into the following five categories: infrastructure, software, people, processes, and data.

SOC 3 Engagement. An examination engagement to report on management's assertion about whether controls within the system were effective to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the trust services criteria relevant to one or more of the trust services categories (applicable trust services criteria.)

subservice organization. A vendor used by a service organization that performs controls that are necessary, in combination with controls at the service organization, to provide reasonable assurance that the service organization's service commitments and system requirements were achieved.

system requirements. Specifications about how the system should function to (a) meet the service organization's service commitments to user entities and others (such as user entities' customers); (b) meet the service organization's commitments to vendors and business partners; (c) comply with relevant laws and regulations and guidelines of industry groups, such as business or trade associations; and (d) achieve other objectives of the service organization that are relevant to the trust services categories addressed by the description. Requirements are often specified in the service organization's system policies and procedures, system design documentation, contracts with customers, and government regulations.

APPENDIX A: GLOSSARY

trust services. A set of professional attestation and advisory services based on a core set of criteria (trust services criteria) related to security, availability, processing integrity, confidentiality, or privacy.

unauthorized access. Access to information or system components that (a) has not been approved by a person designated to do so by management and (b) compromises segregation of duties, confidentiality commitments, or otherwise increases risks to the information or system components beyond the levels approved by management (that is, access is inappropriate). user entity. An entity that uses the services provided by a service organization.

user entity. An entity that uses the services provided by a service organization.

vendor. An individual or business (and its employees) engaged to provide services to the service organization. Depending on the services a vendor provides (for example, if it operates certain controls on behalf of the service organization that are necessary, in combination with the service organization's controls, to provide reasonable assurance that the service organization's service commitments and system requirements were achieved), a vendor might also be a subservice organization.

{Remainder of the page left blank intentionally}

APPENDIX B: ABBREVIATIONS

Abbreviation	Expanded Form
AICPA	American Institute of Certified Public Accountants
ATS	Automatic Transfer Switch
CAB	Change Advisory Board
CEO	Chief Executive Officer
COO	Chief Operating Officer
COR	Critical Observation Report
CPA	Certified Public Accountant
CRAC	Computer Room Air Conditioner
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DC	Description Criteria
FL	Florida
GRC	Governance Risk Compliance
HSSD	High Sensitivity Smoke Detection
IP	Internal Protocol
IPS	Intrusion Prevention System
ISC	Information Security and Compliance
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Infrastructure Team
LLC	Limited Liability Company
NDA	Non-Disclosure Agreement
PCI DSS	Payment Card Industry Data Security Standard
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SIEM	Security Information Event Management
SLO	Service Level Objectives
SMS	Service Management System
SOC	Security Operations Center
UEBA	User Entity and Behavior Analytics
USB	Universal Serial Bus
VPN	Virtual Private Network
WAF	Web Application Firewall
XDR	Extended Detection and Response

**Netsurion**®



END OF REPORT



A decorative geometric pattern in the bottom-left corner consisting of overlapping squares in shades of green and blue, arranged in a grid-like fashion.