Netsurion®
Powering Secure and Agile Networks

SYSTEM AND ORGANIZATION CONTROLS REPORT (SOC 3)

Secure Edge Networking and Managed Threat Protection Services

Relevant to Security, Availability, Confidentiality, Processing Integrity, and Privacy

For the period January 1, 2020 to December 31, 2020

Shaheen Jhariya, CPA, CCSFP in association with DNV

Table of Contents

SECTION I ASSERTION OF NETSURION'S MANAGEMENT

Netsurion
Powering Secure and Agile Networks

ASSERTION OF NETSURION'S MANAGEMENT

We are responsible for designing, implementing, operating, and maintaining effective controls within Netsurion's Secure Edge Networking and Managed Threat Protection Services (system) throughout the period January 1, 2020 to December, 31, 2020, 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 2 compliant data center colocation services provided by Data Foundry, Houston Data Center (HOU2) for hosting its application and servers and AWS infrastructure for hosting its service environment. The description (Attachment A) indicates that complementary subservice organizations 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 organizations 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, 2020, to December 31, 2020, 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, 2020, to December 31, 2020, 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 organizations controls assumed in the design of Netsurion's controls throughout the period January 1, 2020, to December 31, 2020.

-Netsurion

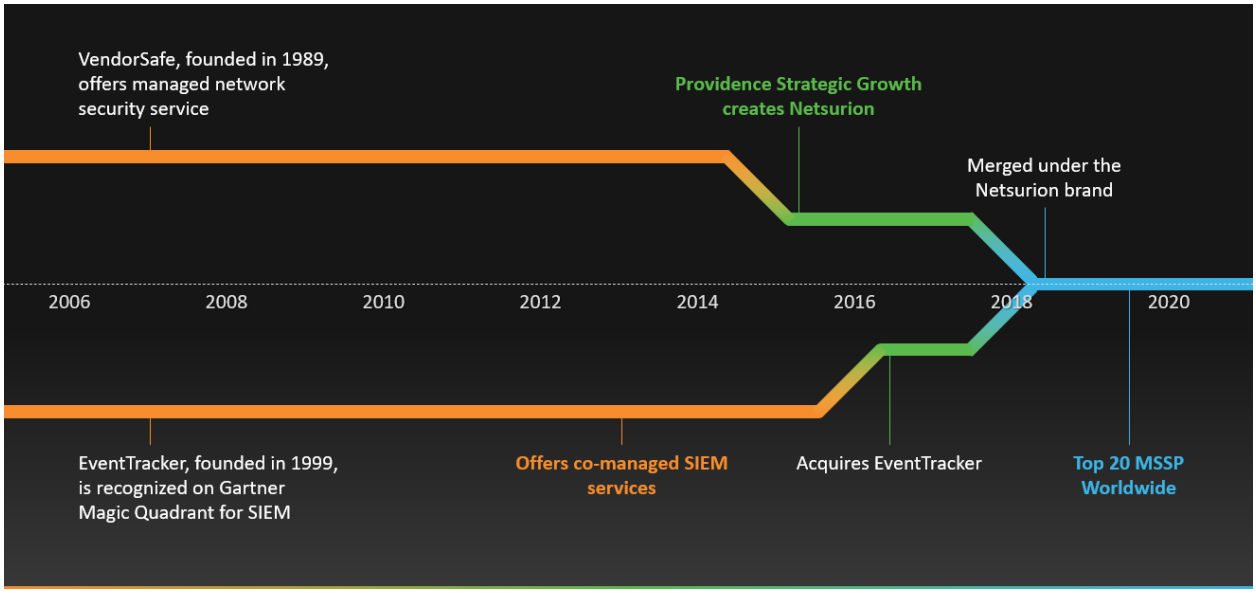
ATTACHMENT A

ATTACHMENT A

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

Company Overview

Netsurion is a managed security service provider (MSSP) with a legacy dating back to 1989 with the founding of managed network security service provider, VendorSafe Technologies, and 1999 with the founding of SIEM software, EventTracker. Merged together, Netsurion has become known as a Top 20 MSSP worldwide according to industry media leader, MSSP Alert. In 2021, Netsurion was awarded Gold for Best Cybersecurity Company by Cybersecurity Excellence Awards.



Mission

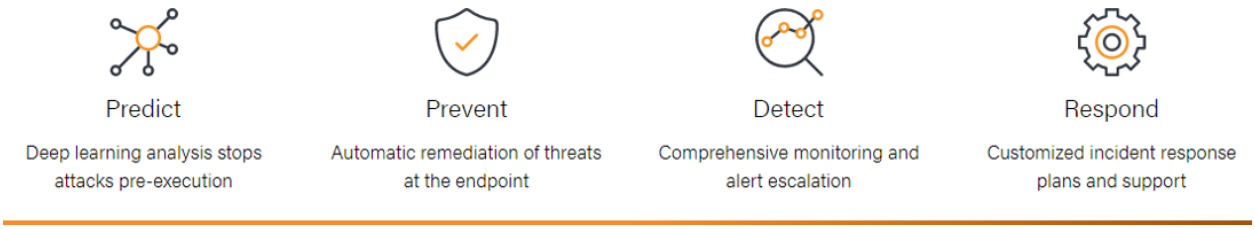
Netsurion's mission is not to deliver technology for the sake of technology. Rather, it's focused on delivering business results – value for the typical business that has limited cybersecurity resources.

Netsurion is not just a software provider, not just a hardware vendor, and not a typical managed security service provider. Netsurion delivers cybersecurity as a managed service with unmatched scalability and simplicity.

Netsurion's managed platform approach of combining purpose-built technology and its team of cybersecurity experts gives customers and partners the ultimate flexibility to adapt and grow while maintaining a secure environment. As trusted advisors, Netsurion believes all businesses, regardless of size and budget, deserve reliable high-quality cybersecurity services with tangible security benefits that exceed expectations.

Managed Threat Protection

Netsurion® Managed Threat Protection is a complete managed security service and platform to predict, prevent, detect, and respond to threats across your entire business. Whether you need a targeted supplement to your existing capabilities and staff or a complete outsourced solution, the service is uniquely customizable to your needs. In 2021, Netsurion® Managed Threat Protection was awarded Gold for Best Managed Security Service and Silver for Best Managed Detection & Response.



Netsurion's Threat Protection Platform – EventTracker

EventTracker, Netsurion's flagship managed security platform, is architected to scale with organizations of any size and any stage of maturity. Whether you need a targeted supplement to your existing capabilities and staff or a complete outsourced solution, the EventTracker platform is uniquely customizable to your needs. EventTracker's "snap-in" architecture lets you enable capabilities such as endpoint protection, SIEM, vulnerability management, threat hunting and more all within one centrally managed console. All of this technology is combined with our ISO/IEC 27001:2013, ISO/IEC 20000-1:2018, PCI DSS (SAQ) certified security operations center (SOC) staffed by experts protecting your business 24/7. This certification emphasizes Netsurion's strong commitment to providing the highest levels of security to enterprises.

EventTracker Enterprise

EventTracker Enterprise Services are enterprise-grade services, deliver enterprise-grade threat lifecycle management through the EventTracker platform that unifies machine learning, behavior analytics, and security orchestration coupled with a 24/7 SOC and managed services. It's difficult to deploy, manage and use an effective combination of expertise and tools that provide early detection of targeted, advanced threats and insider threats. With EventTracker Enterprise, the SOC team works with customers to analyze event data in real-time, then collect, store, investigate, and report on log data for incident response, forensics, and regulatory compliance.

EventTracker Essentials

EventTracker Essentials is a managed security service powered by enterprise technology yet packaged to deliver advanced threat protection with endpoint detection and response plus IT compliance to small and medium-sized organizations that demand practical and cost-effective solutions.

EventTracker Essentials provides 24/7 monitoring of its customer network for advanced threats that evade antivirus and firewalls. With real-time alerting and remediation recommendations, customers can be confident that their network is defended. Adaptive machine learning optimizes firewall and Office 365 security by quickly detecting unknown and out-of-the-ordinary behavior.

The EventTracker Essentials service is an easy-to-deploy, multi-tenant, software-only solution hosted by Netsurion at its SOC 2 compliant data centers in the US. Service is delivered to end-customers or to managed service providers (MSPs) who in turn have their customer base. Both of these are referenced as "customer".

Secure Edge Networking

Businesses are embracing digital transformation, adapting to changing consumer behaviors, and optimizing for cost efficiencies. Doing so requires a secure, always-on, and easy to manage network that can act as a launchpad for innovation and growth amid a world of rapidly evolving threats. Protecting data and transactions, and quickly responding to cybersecurity threats, is a must for agile IT teams.

Netsurion® Secure Edge Networking is an all-in-one solution offering managed networking, security, resilience, and compliance. In 2021, Cybersecurity Excellence Award named Netsurion® Secure Edge Networking a Gold winner for Best Zero Trust Security and Best Cybersecurity Solution for Retail Industry.

.

Netsurion's Edge Networking Platform - BranchSDO

BranchSDO, Netsurion's flagship edge networking platform, enables multi-location enterprises to maintain a strong security posture, resilient connectivity, command and control of all locations, and the flexibility to adapt to rapidly changing technology needs. BranchSDO combines a multi-function edge device, cloud orchestration, and a 24/7 network operations center (NOC) to deliver security, cellular failover, Wi-Fi, and PCI DSS compliance support to all branch locations. Netsurion's BranchSDO has certified its compliance with PCI DSS and ISO 20000-1:2018 standards.

Netsurion Secure Edge Networking, called BranchSDO, is comprised of Netsurion SD-Branch & Netsurion Managed Firewall Services.

Netsurion SD-Branch Services

At the core of Netsurion BranchSDO is the power-packed and cost-effective edge device, the CXD, this multi-function device dramatically reduces hardware complexity and cost by combining multi-WAN connectivity, Wi-Fi, cellular failover, and a stateful firewall while future-proofing the edge location networks by enabling cloud-delivery of network services via SD-WAN. With Netsurion SD-Branch Services, customers are provided a fully managed service building of the standalone CXD with the many "optional" features.

Netsurion Managed Firewall Services

Netsurion BranchSDO is available with on-premise next-generation firewalls. Netsurion complements industry-leading next-generation firewalls with a managed service that simplifies implementation and management, making it easy for any-size business to have enterprise-class security without the cost of dedicated onsite IT Staff. Netsurion Managed Firewall Services provides 24/7 firewall management, managed security services, cellular failover for network resilience, PCI DSS compliance support, and more, making it easy for any-size office or operation to have enterprise-class security without the cost of dedicated onsite IT staff.

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 customer 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 Secure Edge Networking and Managed Threat Protection Services

People

Netsurion's staff is organized in the following functional areas.

- Leadership
- Sales and Marketing
- Secure Edge Networking Team
- Managed Threat Protection Team (SOC)
- Research and Development Team
- Finance
- Human resource
- Infrastructure Team
- Finance and Operations Team
- Information Security and Compliance Team

Procedures

Netsurion has developed the Information Security Management System (ISMS) and Service Management System (SMS) policies and procedures. The policies and procedures are reviewed and changes if any, are authorized by the Information Security Steering Committee.

[Space left blank intentionally]

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 and
- Vulnerability Management.

Standard Operating Procedures are defined across which are primarily used internally to guide Netsurion's 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

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. Netsurion has a documented and approved code of conduct defined 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 training portal.

Information security related policies and procedures are communicated to the employees during the induction training and are made accessible to employees via the 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 trainings are conducted periodically.

Communication and Information

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 rules. Access to Internet is controlled and monitored through content filtering settings configured in firewall. WAF is being used in EventTracker servers hosted for customers to prevent common attack traffic. 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 internal network are through firewalls. All the connections to client network is allowed only after reviewing the requirement by the Infrastructure Team. Connection to 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 port other than 80 and 443 are allowed only from Netsurion's corporate network.

Endpoint Protection

Antivirus solution is implemented on all Netsurion's Assets (servers, workstations) which are in the Netsurion domain. Virus scans are performed automatically on a continuous basis. Scheduled full scan is performed on a weekly basis.

Antivirus Compliance email reminders are sent to users. Live update/force AV update policy is enabled which takes the definitions from the Antivirus server irrespective of the network. EventTracker SIEM Agent is installed in all windows systems to detect new / zero-day vulnerabilities.

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. USB access is disabled for all users in the SOC Team. 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 at regular intervals to verify if the servers, workstations, and network devices are configured as per the standard.

Vulnerability Assessment and Penetration Testing

Netsurion conduct 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 is published by the SOC team on a daily basis 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 Control

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 system 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.EventTracker product update/ patch management process is documented which provides detailed information about the process that is defined and followed by the SOC Team in the EventTracker Patch Management. All patches are tested before applying to the production environment. A record of each update is maintained in the ticketing tool.

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 softwares are fully patched.

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 Plan

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.

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.

Physical Security and Environmental Safeguards

Physical Access to Netsurion's premises is controlled through 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

Subservice Organizations (carved-out)

Data Foundry

Netsurion utilizes SOC 2 Type II compliant data center colocation services provided by Data Foundry, Houston Data Center (HOU2) for hosting their application and servers. The following key controls are expected to be implemented by Data Foundry however they have not been included in the scope of this examination.

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, an 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 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.

Amazon Web Services

Netsurion utilizes AWS infrastructure for hosting its service environment. Controls at Amazon Web Services are not included in the scope of this examination. 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

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 includes 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.

[Space left blank intentionally]

ATTACHMENT B

Netsurion
Powering Secure and Agile Networks

ATTACHMENT B

Principal Service Commitments and System Requirements

Netsurion makes service commitments to its customers and has established system requirements as part of the Secure Edge Networking (SEN) and 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 offerings provided online, Information Security Management System (ISMS policy), Service Management System (SMS policy).

Service commitments includes, but are not limited to, the following:

Service Delivery SLO's

Netsurion has established Service Level Objectives with respect to the Secure Edge Networking and Managed Threat Protection Services. SLO's may vary/differ as per customer/client requirements. Key performance indicators are identified and reviewed on a monthly basis.

Security

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 define 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's (also referred to as "Netsurion" or "service organization") accompanying assertion titled "Assertion of Netsurion's Management" (assertion) that the controls within Netsurion's Secure Edge Networking and Managed Threat Protection Services (system) were effective throughout the period January 1, 2020 to December 31, 2020 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 SOC 2 Type 2 compliant data center colocation services provided by Data Foundry, Houston Data Center (HOU2) for hosting its application and servers and AWS infrastructure for hosting its service environment. The description indicates that complementary subservice organizations 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.

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 Secure Edge Networking and Managed Threat Protection Services (system) were effective throughout the period January 1, 2020 to December 31, 2020, 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 organizations controls assumed in the design of Netsurion's controls operated effectively throughout the period January 1, 2020 to December 31, 2020.

Shaheen Jhariya, CPA, CCSFP

CPA License Number # 4143
Mumbai, India
April 9, 2021

Appendix A: Glossary

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 that has the authority to grant such access.

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.

controls. Policies and procedures that are part of the entity's system of internal control. The objective of an entity's system of internal control is to provide reasonable assurance that principal system objectives are achieved.

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

infrastructure. The collection of physical or virtual resources that supports an overall IT environment, including the server, storage, and network elements.

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.

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.

system boundaries. The specific aspects of an entity's infrastructure, software, people, procedures, and data necessary to perform a function or provide a service. When systems for multiple functions or services share aspects, infrastructure, software, people, procedures, and data, the systems will overlap, but the boundaries of each system will differ.

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.)

Appendix A: Glossary

system requirements. Specifications regarding how the system should function to (a) meet the entity's commitments to customers and others (such as customers' customers); (b) meet the entity's commitments to suppliers 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 entity objectives that are relevant to the trust services category or categories addressed by the description. Requirements are often specified in the entity's system policies and procedures, system design documentation, contracts with customers, and government regulations.

System requirements may result from the entity's commitments relating to security, availability, processing integrity, confidentiality, or privacy. For example, a commitment to programmatically enforce segregation of duties between data entry and data approval creates system requirements regarding user access administration.

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.

trust services. A set of professional attestation and advisory services based on a core set of 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).

vendor. (or supplier). An individual or business (and its employees) that is engaged to provide goods or services to the entity. Depending on the services provided (for example, if the vendor operates certain controls on behalf of the entity that are necessary to achieve the entity's objectives), it also might be a service provider.

[Space left blank intentionally]

Appendix B: Abbreviations

Abbreviation	Expanded Form
AICPA	American Institute of Certified Public Accountants
ASV	Approved Scanning Vendor
ATS	Automatic Transfer Switch
AV	Antivirus
BCP	Business Continuity Plan
CAB	Change Advisory Board
CEO	Chief Executive Officer
CPA	Certified Public Accountant
COO	Chief Operating Officer
CRAC	Computer Room Air Conditioner
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
GRC	Governance Risk Compliance
HSSD	High Sensitivity Smoke Detection
IPS	Intrusion Prevention System
ISMS	Information Security Management System
ISC	Information Security Compliance
ISO	International Standard Organization
IT	Infrastructure Team
MSP	Managed Service Provider
MSSP	Managed Security Service Provider
PCI DSS	Payment Card Industry Data Security Standard
PDU	Power Distribution Unit
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SD-WAN	Software Defined Wide Area Network
SEN	Secure Edge Networking
SIEM	Security Information Event Management
SLO	Service Level Objectives
SMS	Service Management System
SOC	Security Operations Center
SOC 3	System and Organization Controls 3
STS	Static Transfer Switch
USB	Universal Serial Bus
VPN	Virtual Private Network
WAF	Web Application Firewall
WAN	Wide Area Network

End of Report