A-LIGN

SocketLabs

Type 2 SOC 3

2024

SocketLabs

SOC 3 FOR SERVICE ORGANIZATIONS REPORT

January 1, 2024 to December 31, 2024

Table of Contents

SECTION 1

ASSERTION OF SOCKETLABS MANAGEMENT

ASSERTION OF SOCKETLABS MANAGEMENT

March 25, 2025

We are responsible for designing, implementing, operating, and maintaining effective controls within SocketLabs' ('the Company') E-mail Service Provider Services System throughout the period January 1, 2024 to December 31, 2024, to provide reasonable assurance that SocketLabs' service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA, *Trust Services Criteria*. Our description of the boundaries of the system is presented below in "SocketLabs' Description of Its E-mail Service Provider Services System throughout the period January 1, 2024 to December 31, 2024" and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period January 1, 2024 to December 31, 2024, to provide reasonable assurance that SocketLabs' service commitments and system requirements were achieved based on the trust services criteria. SocketLabs' 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 "SocketLabs' Description of Its E-mail Service Provider Services System throughout the period January 1, 2024 to December 31, 2024".

SocketLabs uses Amazon Web Services ('AWS') and Microsoft Azure ('Azure') to provide cloud hosting services (collectively, the 'subservice organizations'). The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at SocketLabs, to achieve SocketLabs' service commitments and system requirements based on the applicable trust services criteria. The description presents SocketLabs' controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of SocketLabs' controls. The description does not disclose the actual controls at the subservice organizations.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary to achieve SocketLabs' service commitments and system requirements based on the applicable trust services criteria. The description presents the applicable trust services criteria and the complementary user entity controls assumed in the design of SocketLabs' controls.

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, 2024 to December 31, 2024 to provide reasonable assurance that SocketLabs' service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of SocketLabs' controls operated effectively throughout that period.

Joe Breslin
Chief Operating Officer
SocketLabs

SECTION 2

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To SocketLabs:

Scope

We have examined SocketLabs' ('SocketLabs' or 'the Company') accompanying assertion titled "Assertion of SocketLabs Management" (assertion) that the controls within SocketLabs' E-mail Service Provider Services System were effective throughout the period January 1, 2024 to December 31, 2024, to provide reasonable assurance that SocketLabs' service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA *Trust Services Criteria*.

SocketLabs uses AWS and Azure to provide cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at SocketLabs, to achieve SocketLabs' service commitments and system requirements based on the applicable trust services criteria. The description presents SocketLabs' controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of SocketLabs' controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at SocketLabs, to achieve SocketLabs' service commitments and system requirements based on the applicable trust services criteria. The description presents SocketLabs' controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of SocketLabs' controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

SocketLabs 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 SocketLabs' service commitments and system requirements were achieved. SocketLabs has also provided the accompanying assertion (SocketLabs assertion) about the effectiveness of controls within the system. When preparing its assertion, SocketLabs 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 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 attestation standards established by the AICPA. 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's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its 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.

Independence and Ethical Responsibilities

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

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 are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating 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

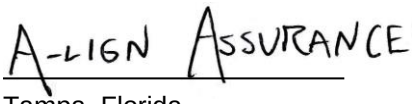
In our opinion, management's assertion that the controls within SocketLabs' E-mail Service Provider Services System were suitably designed and operating effectively throughout the period January 1, 2024 to December 31, 2024, to provide reasonable assurance that SocketLabs' service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects, if complementary subservice organization controls and complementary user entity controls assumed in the design of SocketLabs' controls operated effectively throughout that period.

The SOC logo for Service Organizations on SocketLabs' website constitutes a symbolic representation of the contents of this report and is not intended, nor should it be construed, to provide any additional assurance.

Restricted Use

This report, is intended solely for the information and use of SocketLabs, user entities of SocketLabs' E-mail Service Provider Services during some or all of the period January 1, 2024 to December 31, 2024, business partners of SocketLabs subject to risks arising from interactions with the E-mail Service Provider Services, and those who have sufficient knowledge and understanding of the complementary subservice organization controls and complementary user entity controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.

This report is not intended to be, and should not be, used by anyone other than these specified parties.



Tampa, Florida
March 25, 2025

SECTION 3

SOCKETLABS' DESCRIPTION OF ITS E-MAIL SERVICE PROVIDER SERVICES SYSTEM THROUGHOUT THE PERIOD JANUARY 1, 2024 TO DECEMBER 31, 2024

OVERVIEW OF OPERATIONS

Company Background

SocketLabs was founded over 14 years ago to change the way people and businesses use e-mail. And while SocketLabs' technology and services have evolved, its commitment to the people it serves has not. For customers who have used other ESPs or are seeking help for the first time, the SocketLabs experience will be a new one. This is technology, services, support, and analytics, built for customers.

Description of Services Provided

Technology

SocketLabs Hurricane MTA is the foundation of its e-mail delivery infrastructure. Because SocketLabs built and maintains its own MTA, it can create unique personalized solutions for its customers with the latest industry technologies. Flexible APIs, advanced reporting and analytics, and the latest security and encryption create a superior e-mail experience.

Deliverability

The SocketLabs e-mail solutions are built to give customers the best chance at hitting the inbox. SocketLabs has a strict provisioning process that keeps bad senders out, making it easier for good senders to accomplish their goals. SocketLabs has automatic list suppression, built-in authentication, StreamScore deliverability reporting, and tons of other features working silently in the background to get important e-mail to the inbox.

Consulting

With SocketLabs expert consulting, customers can get as little or as much as they want. Whether it's complete implementation and system management, or data analysis and advising. SocketLabs expert consulting provides access to invaluable levels of e-mail experience.

World Class Support

Call, chat, or e-mail real e-mail experts, not automated support bots. These are e-mail specialists, based in SocketLabs' Philadelphia-area offices ready to get customers back on track.

Customer Experience

SocketLabs understands the need for personalization in this increasingly complex world of e-mail. And while the biggest ESPs build solutions for the masses, SocketLabs build solutions with its customers in mind.

Principal Service Commitments and System Requirements

SocketLabs designs its processes and procedures related to its Hurricane and On-Demand Platforms to meet its objectives for its ESP services. Those objectives are based on the service commitments that SocketLabs makes to user entities, the laws and regulations that govern the provision of ESP services, and the financial, operational, and compliance requirements that SocketLabs has established for the services. The ESP services of SocketLabs are subject to the state privacy security laws and regulations in the jurisdictions in which SocketLabs operates.

Security commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online. Security commitments are standardized and include, but are not limited to, the following:

Security principles within the fundamental designs of the Hurricane and On-Demand Platforms that are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role. Use of encryption technologies to protect customer data both at rest and in transit are enabled.

SocketLabs establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in SocketLabs' system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the Hurricane and On-Demand Platforms.

Components of the System

Infrastructure

Primary infrastructure used to provide SocketLabs' E-mail Service Provider Services System includes the following:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Web Servers	AWS EC2	Control Panel, Customer Facing Website
Firewall	SonicWALL TZ500	Headquarters Firewall
Firewall	Cisco ASA 5508-X	Sungard/Rackspace Co-Location Protection
Firewall	Juniper SRX340	Ntirety Co-Location Protection
Switches	Cisco Catalyst 2960 XR	Connects devices on the corporate network by sending message to the specific device(s) that need to receive it
Platform Servers	Dell PowerEdge R710, 720, 730	Hypervisors, Senders, Receivers, Load Balancers in Co-Locations

Software

Primary software used to provide SocketLabs' E-mail Service Provider Services System includes the following:

Primary Software		
Software	**Operating System**	**Purpose**
Veeam	SaaS	Hyper-V Snapshot Backup
Senders	Server 2019	On-Demand Platform
Receivers	Server 2019	On-Demand Platform

Primary Software		
Software	**Operating System**	**Purpose**
Load Balancer	Server 2019	On-Demand Platform
CrowdStrike	Linux	Managed SOC
Connectwise Control	SaaS	Remote Support Software
Spam Assassin	Linux	Client Server Spam Filtering
Octopus Deploy	SaaS	Deploy Code
MySQL	AWS RDS	Databases
Cisco AnyConnect	SaaS	VPN
BackBlaze	SaaS	Backup Software
Jira/Confluence	Atlassian	Tickets/QA/Deployment/Documentation
Visual Studio	SaaS	Software Development
Azure DevOps	SaaS	Software Development
M365	SaaS	Company Cloud Internal
BitDefender	BitDefender	Endpoint Protection
OnSIP	VoIP	VoIP Software
Zoom	Zoom	Meeting Software
MySQL Workbench	Oracle	MySQL Toolset

People

SocketLabs has a staff of approximately 40 employees organized in the following functional areas:

- Go To Market. Responsible for the full customer lifecycle and funnel, from identification and acquisition to ongoing support. The function is broke up into the following sub-functional focus areas, including:
    - Revenue Marketing. Responsible for identifying potential acquisition opportunities and generating a prospect pipeline across the following focus areas:
        - Demand Generation is responsible for paid media acquisition, through Pay Per Click, website, third-party partner and other growth engines. The team is responsible for monitoring and continuously improving upon the existing efforts in place though data analytics.
        - Growth Marketing is responsible for driving organic acquisition, primarily through Search Engine Optimization, link building and partner engagement.
        - Lifecycle Marketing is responsible for moving engaged prospects into converted customers, for enabling customer success through content and for expanding on existing customers.
    - Sales. Responsible for converting prospects identified by the Revenue Marketing team into paying customers and for expanding on existing customers. Sales team are the primary point of contact in managing deals for prospective customers:
        - Self-service sales are responsible for enabling utility-type buyers to achieve competitive pricing and services for their e-mail needs.
        - Solution sales is responsible for entering a new market by providing value-added services including deliverability, data analytics and custom implementation.
    - Account Management. Responsible for existing account and customer engagement, enabling their success and ensuring satisfaction.

- Support is responsible for all unnamed accounts and customers, responsible through tickets, chat and phone. Support is responsible for addressing issues, providing instruction, creating self-service documentation, and managing first tier compliance issues.
- Customer Success is responsible for named top accounts and is measured on driving their satisfaction, providing awareness to new solutions, leading account expansion, and for managing top customer requests and issues to resolution.
- Product Development. Responsible for all related Product, Engineering, Development and Infrastructure management under unified execution:
    - Product Management. Responsible for capturing customer feedback, establishing personas, measuring product and customer performance, defining and prioritizing product roadmap, and continuously improving the product.
- Self-Service is focused on maintaining and continuously improving the existing product, optimizing the customer experience and increasing attachment rate.
- Solutions is creating future-facing product services and solutions, focused on platform management, third-party “one to many” sender enablement, deliverability services, and advanced reporting:
    - Innovation/Labs. Responsible for rapid prototyping of future solutions and offerings based on Product Management guidance. Proof of concept work created within this department is transitioned to Software Engineering for robust development. Responsibilities include identifying new technologies, creating new platforms and implementing new solutions.
    - DevOps. Responsible for enabling Software Engineering to ship and continuously improve product as quickly as possible, managing platform infrastructure and security and ensuring maximum quality product through continuous improvement.
- Compliance is responsible for monitoring and maintaining platform senders to ensure high quality senders, implementing automated solutions to streamline vetting and managing compliance and blocklist escalations.
- Infrastructure & Security is responsible for providing, maintaining and improving the internal and customer-facing technical infrastructure for its product and platform. The team is responsible for enabling the Software Engineering team to build, deploy and continuously improve their product offerings.
- QA is responsible for defining acceptance criteria, creating testing and managing product development prior to release. QA is also responsible for addressing and prioritizing customer feedback requests on reported issues:
    - Software Engineering. Responsible for working with Innovation/Labs and Product Management to continuously improve existing product and create new products. Manages all product programming, as broken out by:
        - Front-end is responsible for customer-facing experience, including web and mobile development, website development, User Experience, and User Interface.
        - Back-end is responsible for all programmatic engineering including Database development and maintenance, back-end programming, data storage and management, and security.
- Product Marketing. Responsible for generating customer and brand awareness, evangelizing platform and creating new top of funnel sales opportunities:
    - Product Marketing is responsible for content creation (e.g., blogs, webinars, videos, tutorials), updating and creating website content, supporting Sales Go to Market efforts, and plugging in with Revenue Marketing team.
- Team Operations. Responsible for managing ongoing team execution and the employee experience. The team is responsible for enabling and supporting work, developing and managing ongoing business processes, providing overarching guidance and training:
    - Operations is responsible for Financial Management, Human Resources engagement, employee performance management, policy management, and employee experience enablement. Operations acts as the primary conduit into the company ownership.
    - IT is responsible for all employee technology needs including hardware provisioning, software implementation and support, technical/hardware support, technical training.

Data

Data, as defined by SocketLabs, constitutes the following:

- E-mail Messages
- E-mail Message Meta Data
- E-mail Message Event Log Data
- E-mail Addresses
- Engagement Log Data
- Suppression List

SocketLabs is an e-mail delivery service, transactions are initiated by the customers submitting e-mail messages to SocketLabs using its ingestion endpoints. These endpoints include the Simple Mail Transfer Protocol (SMTP), REST API Endpoint's or SocketLabs' E-mail Marketing application. These endpoints are secured using TLS encryption. The messages flow from SocketLabs' ingestion nodes to its delivery nodes where messages are delivered to the ultimate destination using the SMTP protocol. As messages are transferred through the system message meta data is stored in event log files. Optionally engagement tracking can be enabled, which will log the recipients IP address and the message meta data when an open, click, or unsubscribe events occurs. This data is stored in the engagement log files. The message event data and engagement data are transferred to a database that is used by the customer and technical support staff for usage tracking, status reports, delivery analytics and trouble shooting. Log files and database rows are purged within 90 days. In addition to the log files, SocketLabs will keep random message samples for 15 days, which can used for compliance and security review.

SocketLabs keeps an e-mail address suppression list that contains invalid e-mail addresses and e-mail addresses of recipients who have asked to have their addresses blocked by the customer. The e-mail address suppression list is kept for the lifetime of the account.

Processes, Policies and Procedures

Formal IT policies and procedures exist that describe physical security, logical access, computer operations, change control, and data communication standards. All teams are expected to adhere to the SocketLabs' policies and procedures that define how services should be delivered. These are located on the Company's intranet and can be accessed by any SocketLabs team member.

<u>Physical Security</u>

To help ensure SocketLabs' assets are physically protected within the secured facility(s) in order to prevent unauthorized access and damage:

- Physical access to IT equipment shall be restricted to authorized personnel who have prior approval to physically access the systems.
- Visitors' access shall be restricted to one entry point for each SocketLabs building in which Confidential Data is stored. Unless a visitor will be always escorted during their visit, they shall be required to sign-in. If the visitor's identity is not known, they need to provide a valid photo ID. Visitors shall not be permitted unescorted access in any area that contains unsecured Confidential Data.

When appropriate, other physical security controls must be implemented to control physical access, and to monitor physical activity in SocketLabs' facilities where IT systems or Confidential Data are located. Such controls may include but are not limited to:

- Walls with locked doors
- Keys, badges and badge readers, key fobs, biometric locks, or other physical authentication methods
- Locked server cages
- Video surveillance

Logical Access

SocketLabs uses role-based security architecture and requires users of the system to be identified and authenticated prior to the use of any system resources. Resources are protected through the use of native system security and add-on software products that identify and authenticate users and validate access requests against the users' authorized roles in access control lists.

All resources are managed in the asset inventory system (Snipe-It) and each asset is assigned an owner. Owners are responsible for approving access to the resource and for performing periodic reviews of access by role.

Employees and approved vendor personnel sign on to the SocketLabs network using an Active Directory user ID and password. Users are also required to separately sign on to any systems or applications that do not use the shared sign-on functionality of Active Directory. Passwords must conform to defined password standards and are enforced through parameter settings in the Active Directory. These settings are part of the configuration standards and force users to change passwords at a defined interval, disable the user ID's ability to access the system and components after a specified number of unsuccessful access attempts, and mask workstation screens, requiring reentry of the user ID and password after a period of inactivity.

Employees accessing the system from inside or outside the SocketLab's network are required to use a token-based two-factor authentication and SSLVPN.

Customer employees' access to the Control Panel through the Internet using the SSL functionality of their web-browser. These customer employees must supply a valid user ID and password to gain access to customer cloud resources. Passwords must conform to password configuration requirements configured on the virtual devices using the virtual server administration account. Customers are strongly encouraged to use two-factor authentication.

Virtual devices are initially configured in accordance with SocketLabs' configuration standards, but these configuration parameters may be changed by the virtual server administration account.

Upon hire, employees are assigned to a position in the HR management system. No more than a week prior to the employees' start date, the HR department triggers a power automate flow initiates and access to be granted. The flow is used by the Infrastructure Team to create user IDs and access rules. Access rules have been pre-defined based on the defined roles. The system lists also include employees with position changes and the associated roles to be changed within the access rules.

On an annual basis, access rules for each role are reviewed by Infrastructure & Security Teams in evaluating role access, group members consider job description, duties requiring segregation, and risks associated with access. Completed rules are reviewed and approved by the Director of DevOps. As part of this process, the Director of DevOps reviews access by privileged roles and requests modifications based on this review.

When an employee has left the Company, the HR Manager triggers a termination Power Automation flow which assigns tasks to all relevant personnel to accomplish relevant tasks including removal of access from all systems, and the recovery of all equipment and property belonging to SocketLabs.

Computer Operations - Backups

Backup copies of critical systems/data must be maintained to avoid loss of data or compute capacity in case of a disaster or a system outage:

- Systems that hold critical data or are critical to business operations should be identified and included in the backup process.
- A backup solution should be implemented, and regular backups should be performed.
- Backup copies and backup compute capacity should reside in a location that is geographically remote from the primary processing data center.

- Periodic restoration testing of the backup data and systems should be performed to test the effectiveness of the backups:
    - The results of such testing should be documented.
- Backups and procedures must be established for restoring any unintentionally lost PII or Confidential Data.

Employee (end-user laptops) are backed up using BackBlaze with encryption enabled. All VM snapshots are backed up with Veeam and stored internally in the colocation datacenters.

Computer Operations - Availability

Incident response policies and procedures are in place to guide personnel in reporting and responding to information technology incidents but need some work.

SocketLabs monitors the capacity utilization of physical and computing infrastructure both internally and for customers to ensure that service delivery matches service level agreements. Socketlabs evaluates the need for additional infrastructure capacity in response to growth of existing customers and/or the addition of new customers. Infrastructure capacity monitoring includes, but is not limited to, the following infrastructure:

- Data center space, power and cooling
- Disk storage
- Cloud storage
- Network bandwidth

SocketLabs has implemented a monthly patch management process to ensure contracted customer and infrastructure systems are patched in accordance with vendor recommended operating system patches. Customers and SocketLabs system owners review proposed operating system patches to determine whether the patches are applied. Customers and SocketLabs systems are responsible for determining the risk of applying or not applying patches based upon the security and availability impact of those systems and any critical applications hosted on them. SocketLabs staff validate that all patches have been installed and if applicable that reboots have been completed.

Change Control

SocketLabs Change Management Policy

Purpose

The purpose of this document is to outline the change management and review process.

Definitions:

- Change - A change for the sake of this policy means any change that may impact production systems in any way, any aspect of SocketLabs networks, including firewalls, DNS, etc., or a change that impacts more than one user, employee or customer. Specific exceptions may be made by documented procedures and processes per department.
- Change Request - Process for approval of changes not defined as normal operations by policies and procedures.
- Change Tracking - The documentation of what changes were made, by whom, and when.

Change Request Process:

- Change Request Proposal:
  - Change requests must be submitted via the official form, or by sending a helpdesk ticket to spiceworks@socketlabs.com indicating the change requested, reason for the change, involved systems, users and services as well as potential impact, process to be followed in implementation of the change, change window, and expected result of the change, and procedure to undo the change if necessary.
- Change Approval:
  - The requested change must be approved by the system owner, or if the owner is proposing the change, it must be approved by the director of engineering, the ISO, or the CEO. At the discretion of the approver, testing of changes in a non-production environment may be required, or other addendums/requirements may be defined as a contingency for approval.
- Change Implementation Preparation:
  - If the change may or will have major impact customers or employees, they must be notified prior to the change(s) being implemented. Before a change is made, a backup or documentation of the current configuration should be made in case a change roll-back is required.
- Change Implementation:
  - Once change proposal, approval, and preparation are complete, the change may be implemented. Changes must be implemented in the time frame proposed and approved, or time frame amended and approved during the change approval process. Whenever changes are implemented, the ticket for the change must be updated to confirm the proposed change process was followed, or to document any discrepancies from the approved change proposal.
- Change Review:
  - After change implementation, impacted systems must be reviewed and functionality of impacted systems confirmed. This must be documented in the ticket for the change.
- Change Tracking:
  - Any operational procedure that is not automatically tracked or exempted from change tracking must be documented. This may be done with the official form or by sending an e-mail to spiceworks@socketlabs.com with the description and timing of the change.

Data Communications

SonicWALL and Cisco ASA Firewall systems are in place to filter unauthorized inbound network traffic from the Internet and deny any type of network connection that is not explicitly authorized. Network address translation (NAT) functionality is utilized to manage internal IP addresses. Administrative access to the firewall is restricted to authorized employees.

High availability redundancy is built into the system infrastructure supporting the data center services to help ensure that there is no single point of failure that includes firewalls, routers, and servers. In the event that a primary system fails, the redundant hardware is configured to take its place.

Penetration will be conducted in Q4 to measure the security posture of a target system or environment. The third-party vendor, AT&T will use an accepted industry standard penetration testing methodology (Digital Defense) to accomplish the testing. AT&T's approach begins with a vulnerability analysis of the target system to determine what vulnerabilities exist on the system that can be exploited via a penetration test, simulating a disgruntled/disaffected insider or an attacker that has obtained internal access to the network. Once vulnerabilities are identified, AT&T will attempt to exploit the vulnerabilities to determine whether unauthorized access or other malicious activity is possible. Penetration testing includes network and application layer testing as well testing of controls and processes around the networks and applications and occurs from both outside (external testing) and inside the network.

Vulnerability scanning is performed by AT&T on an annual basis in accordance with SocketLabs' agreement. AT&T uses industry standard scanning technologies and a formal methodology specified by SocketLabs. These technologies are customized to test the organization's infrastructure and software in an efficient manner while minimizing the potential risks associated with active scanning. Retests and on-demand scans will be performed on an as needed basis. Scans are performed during non-peak windows. Tools requiring installation in the SocketLabs' system are implemented through the Change Management process. Scanning is performed with approved scanning templates and with bandwidth-throttling options enabled.

Authorized employees may access the system through from the Internet through the use of leading VPN technology. Employees are authenticated through the use of a token-based two-factor authentication system.

Boundaries of the System

The scope of this report includes the E-mail Service Provider Services System performed in the Aston, Pennsylvania facilities.

This report does not include the cloud hosting services provided by AWS and Azure at multiple facilities.

Changes to the System Since the Last Review

No significant changes have occurred to the services provided to user entities since the organization's last review.

Incidents Since the Last Review

No significant incidents have occurred to the services provided to user entities since the organization's last review.

Criteria Not Applicable to the System

All Common/Security criterion was applicable to the SocketLabs E-mail Service Provider Services System.

Subservice Organizations

This report does not include the cloud hosting services provided by AWS and Azure at multiple facilities.

Subservice Description of Services

AWS and Azure provide cloud hosting services, which includes implementing physical security controls for the housed in-scope systems.

Complementary Subservice Organization Controls

SocketLabs' services are designed with the assumption that certain controls will be implemented by the subservice organization. Such controls are called complementary subservice organization controls. It is not feasible for all of the trust services criteria related to SocketLabs' services to be solely achieved by SocketLabs control procedures. Accordingly, the subservice organization, in conjunction with the services, should establish their own internal controls or procedures to complement those of SocketLabs.

The following subservice organization controls should be implemented by AWS to provide additional assurance that the trust services criteria described within this report are met:

Subservice Organization - AWS		
Category	**Criteria**	**Control**
Common Criteria / Security	CC6.4	Physical access to data centers is approved by an authorized individual.
		Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
		Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.
		Physical access points to server locations are recorded by closed circuit television camera (CCTV). Images are retained for 90 days, unless limited by legal or contractual obligations.
		Physical access points to server locations are managed by electronic access control devices.

The following subservice organization controls should be implemented by Azure to provide additional assurance that the trust services criteria described within this report are met:

Subservice Organization - Microsoft Azure		
Category	**Criteria**	**Control**
Common Criteria/Security	CC6.4	Procedures have been established to restrict physical access to the datacenter to authorized employees, vendors, contractors, and visitors.
		Security verification and check-in are required for personnel requiring temporary access to the interior datacenter facility including tour groups or visitors.
		Physical access to the datacenter is reviewed quarterly and verified by the Datacenter Management team.
		Physical access mechanisms (e.g., access card readers, biometric devices, man traps / portals, cages, locked cabinets) have been implemented and are administered to restrict access to authorized individuals.
		The datacenter facility is monitored 24x7 by security personnel.

SocketLabs have a defined scope of responsibility as outlined in written contracts between SocketLabs and the subservice organizations, including:

- Ensure subservice organizations comply by collecting/reviewing attestations as per the Vendor Management processes and policies
- Monitoring external communications, such as customer complaints relevant to the services provided by the subservice organizations

COMPLEMENTARY USER ENTITY CONTROLS

SocketLabs' services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all of the Trust Services Criteria related to SocketLabs' services to be solely achieved by SocketLabs control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of SocketLabs'.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for understanding and complying with their contractual obligations to SocketLabs.
2. User entities are responsible for notifying SocketLabs of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own systems of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of SocketLabs services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize SocketLabs services.
6. User entities are responsible for providing SocketLabs with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying SocketLabs of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.