

StingBox White Paper 2021

June 1, 2021 - V1.36

StingBox- A simple,
secure and affordable
solution for detecting
network intrusions



StingBox

Security Guide



StingBox has implemented reasonable administrative, technical and physical safeguards to help protect against security incidents and privacy breaches involving the StingBox honeypot products, provided the products are used in accordance with StingBoxes' instructions for use. However, as systems and threats evolve, no system can be protected against all vulnerabilities and we consider our customers the most important partner in maintaining security and privacy safeguards. If you have any concerns, we ask that you bring them to our attention and we will investigate. Where appropriate, we will address the issue with product changes, technical bulletins and/or responsible disclosures to customers and regulators. StingBox continuously strives to improve security and privacy throughout the product lifecycle using practices such as:



- Privacy and Security by Design
- Vulnerability and Patch Management
- Secure Coding Practices and Analysis
- Vulnerability Scanning
- Access Controls appropriate to Customer Data
- Incident Response
- Clear paths for two-way communication between customers and StingBox

If you would like to report a potential product related privacy or security issue (incident, breach or vulnerability), please contact security@stingbox.com.

The purpose of this document is to detail how StingBox's security and privacy practices have been applied to the StingBox honeypot, what you should know about maintaining security of this product and how we can partner with you to ensure security throughout this product's lifecycle.

StingBox

White Paper 2021



Product Description	4
Hardware Specifications	4
Operating Systems	4
Third-party Software	4
Network Ports and Services	5
Sensitive Data Transmitted	5
Sensitive Data Stored	5
Network Diagram	6
Malware Protection	6
Authentication Authorization	6
Encryption	7
Audit Logging	7
Remote Connectivity	7
Service Handling	7
End-of-Life and End-of-Support	8
Penetration Testing	8
Disclaimer	8

Product Description

The StingBox honeypot is a network security device which detects non-expected network and host scans on a network. The device alerts users of these intrusion/discovery attempts so that StingBox owners are able to respond and reduce the impact of these attempts.

Hardware Specifications

Single board computer:

- AllWinner H2 SoC
- 512MB DDR3 SDRAM
- H2 Quad-core Cortex-A7
- XR819, IEEE 802.11 b/g/n wifi (Disabled)
- 10/100M Ethernet RJ45 w/POE
- 8GB TF card / 2MB Spi Flash

Operating Systems

- Ubuntu 16.04.7 LTS
(GNU/Linux 5.3.5+ armv7l)
 - Security Patches/Updates nightly

Third-party Software

Vendor and Name	Version	Description
Python Twisted Event Driven Networking	18.4.0	Python Library for Event Driven networking

Network Ports and Services

Port	Protocol	Service Name	Description of Service	Encrypted
Various	Various	Honeypot simulated services	Set of services which simulate standard services of a networked host/device (FTP, SMB, etc)	Various
2222	SSH	SSH	SSH service for local network remote administration. Password login not allowed. System only contains a public key which allows a stingbox administrator on the local network to troubleshoot the stingbox. No remote access from outside of a local network is established.	Yes

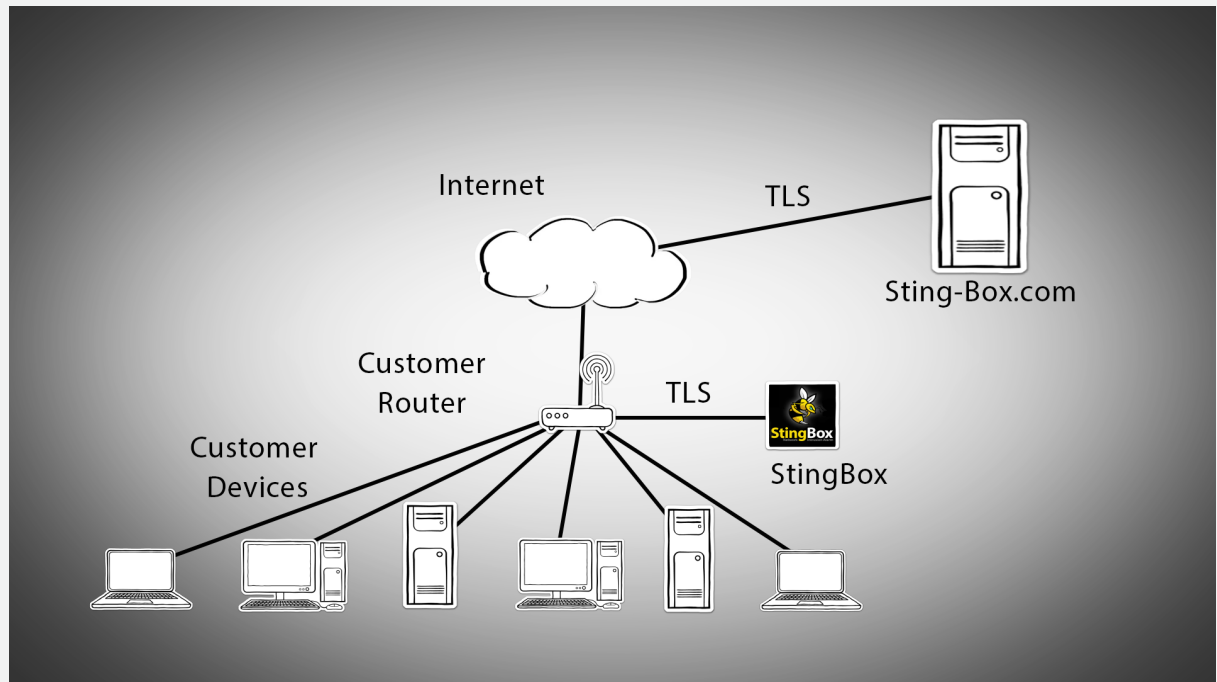
Sensitive Data Transmitted

- Host Names on Network
- Ethernet Adapter MAC addresses

Sensitive Data Stored

- Host Names on Network
- Ethernet Adapter MAC addresses

Network Diagram



Malware Protection

- No specific malware protections
- Unattended and automatic upgrades and security patches

Authentication Authorization

- StingBox hosts:
 - Hosts have a key-pair file which uniquely identifies the host to the server. This file can only be read by the root user of the device and is transferred along with updates to the StingBox.com servers with each request (using HTTPS)
- User Authentication to StingBox.com:
 - Username/Password authentication. Passwords are stored as hashed

Encryption

- All network traffic is TLS 1.2

Audit Logging

- StingBox Host: Device Syslogging
- StingBox.com – stored in server logs by StingBox.com administrators
 - User login/logout
 - Failed client authorization and access attempts
 - Administrator groups: read and changes
 - Adding/Removing StingBoxes

Remote Connectivity

- Check-in and updates: Each 5 minutes StingBoxes check-in (report connectivity and check for updates). This request is originated from the StingBox as a cron job and has a specific endpoint on StingBox.com for check-in (via HTTPS, TLS 1.2)
- Network Scanning: Each 5 minutes, StingBoxes scan the local network for hosts and report discovered hosts back to StingBox.com via an HTTP request. Scanning is done via TCP syn scanning.

Service Handling

- Devices are updated automatically from StingBox.com.
- In the event a device is unable to be updated, a replacement StingBox will be sent to the customer, returned StingBoxes are wiped (secure disk wipe, or disk destruction) before being refurbished or destroyed
- Upon authorization of the customer, a StingBox support agent may add the customer's StingBox to their support dashboard to troubleshoot. All information contained on the user's dashboard will then be available to the support agent.

End-of-Life and End-of-Support

- Customers will be provided 1 month advanced notice of a device end-of-life. Customers will be shipped new devices to replace existing StingBoxes.

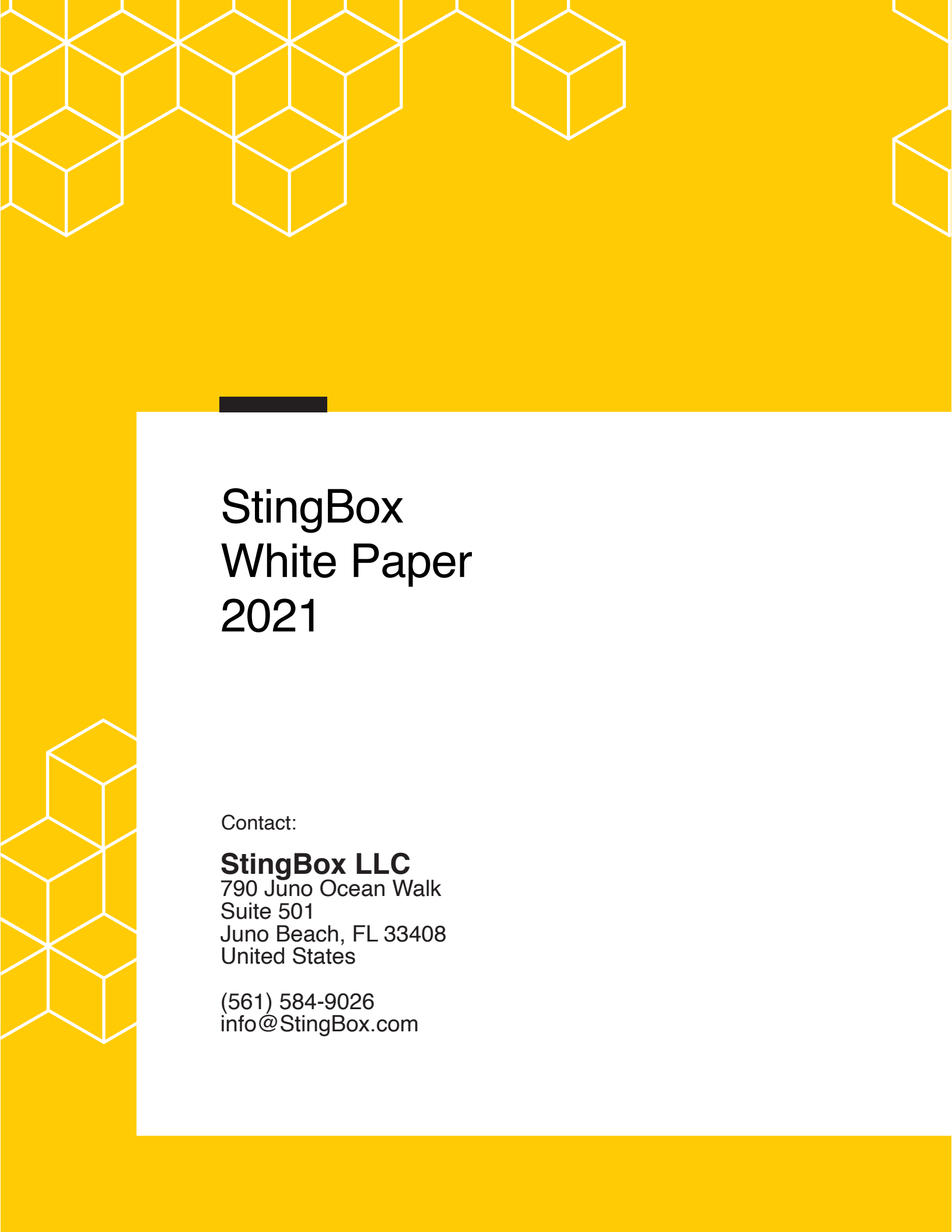
Penetration Testing

- StingBox engaged an independent 3rd party penetration testing firm to conduct a security assessment and penetration testing against its web service and the StingBox device. The purpose of the engagement was to utilize active exploitation techniques in order to evaluate the security of the application and device against best practices, to validate its security mechanisms and identify possible threats and vulnerabilities. Upon completion, the assessment did not reveal any high or critical issues. One medium issue was discovered (cross site request forgery for alert settings) and was remediated and validated. The penetration testing report is available under NDA.



Disclaimer

The information shared in this Product Security White Paper (“White Paper”) is not all-encompassing or comprehensive and does not in any way intend to create or put into implicit effect any elements of a contractual relationship. The primary purpose of this White Paper is to provide potential customers with pertinent information in order for them to analyze the product and make an informed decision. Nothing contained in this document or relayed verbally to any potential customer will be deemed to amend, modify or supersede the terms and conditions of any written agreements between existing customers and StingBox. StingBox does not make any promises or guarantees that any of the methods or suggestions described in this White Paper will restore customer’s systems, resolve any issues related to any malicious code or achieve any other stated or intended results. Customers exclusively assume all risk of utilizing or not utilizing any guidance described in this Whitepaper. Customers exclusively assume all risk of utilizing StingBox products.



StingBox White Paper 2021

Contact:

StingBox LLC
790 Juno Ocean Walk
Suite 501
Juno Beach, FL 33408
United States

(561) 584-9026
info@StingBox.com