Goldilock

FAQs

Technical FAQs

Document Introduction

The purpose of this document is to provide detailed technical responses to the most frequently asked questions that relate to usage, hardware, software, implementation and ongoing maintenance for Goldilocks TruAirgap™ range of secure remote access airgap platforms.

Contents

Solution Overview

Goldilock is a simple yet revolutionary patented technology that physically isolates sensitive data, networks and critical infrastructure from harm or interference, yet retains a layer of convenience for authenticated users.

Unlike existing network segregation techniques, Goldilock is an intelligent hardware appliance that uniquely contains a series of non-ip-controlled electromechanical relays to achieve total network disconnection. Only Goldilock's technology can be remotely controlled using out-of-band non-IP mechanisms, without using the a network or the internet.

This creates an inconvenience layer for attackers and protects potentially disruptive IT procedures, and physically shields digital assets.

There are a huge number of applications for Goldilock, and these can be best split into two categories:

Disconnected mode

- The network is physically severed until an authenticated user remotely controls the reconnection, typically for protection of critical data (physical isolation)

Connected mode

- The network is connected until an authenticated user remotely controls the disconnection, typically to act as a network circuit breaker

These modes are described in more detail below.

Use Cases

Access on Demand; Protection of critical data

Disconnected Mode:

- Bring application servers and data on-line quickly and simply, but only when required – such as backups, know-your-customer (KYC) data, legacy data, crypto currency, multimedia exchange, secure transaction signing, off-line root certificate authority, policy holder data etc.

Disconnected Mode:

- Keep back-up storage within convenient reach yet have it physically isolated from production systems – e.g. prevent ransomware entering back-ups and for ransomware recovery.

Disconnected Mode:

- Secure on-line private storage - ability to switch on a 'safety deposit box' of storage on command.

Connected Mode:

- Network segregation of development & test networks from production networks, e.g. only allow authorised updates to production systems during controlled time periods to avoid profit loss or customer disruption

Kill Switch / Network-level Isolation

Connected Mode:

- Take network devices off-line quickly and simply when required - such as WANs, MANs, LANs, WLANs, IoT networks, building management, utility monitoring, industrial control systems & CCTV etc. for routine or emergency work.

Connected Mode:

- Supply chain control to prevent unnecessary permanent access to the organisations network. Limit such access by 3rd party suppliers that are required to carry out work or when they are compromised during a cyber-attack.

Goldilock 12-Port Appliance

Hardware Specification Questions

1. Does the appliance function as a hub or a network switch?

a. It is neither a Layer 1 hub nor a Layer 2 switch, from a networking perspective it is the equivalent of a patch cable

Think of it as a Layer 1 'cable' that can be remotely plugged in or removed from a physical network port. Devices and networks can be electronically (and physically) connected or disconnected as and when required.

Imagine a simple RJ45 patch lead with a connection to your LAN at one end and a server or network at the other. The airgap switch sits in the middle of the patch lead in a similar way as if you were joining two patch leads.

2. What is the performance throughput of the appliance ports?

a. Each of the 12 available ports is capable of 10Gbps with a minimal degradation of less than 0.1%

3. Which Electromagnetic Compatibility Regulations and Standards (EMC) does the appliance adhere to?

a. The Power Supply Unit (PSU) is certified to the following standards;

IEC 61000-4-2 - Electrostatic Discharge (ESD)

IEC 61000-4-5 - Surge Immunity.

4. What happens in the event of a power failure to the device?

a. The appliance will automatically power up once power is restored.

There are three configurable states each port defaults to upon power up;

1. Default to connected state: The device will physically connect networks or;
2. Default to disconnected state: The device will physically disconnect networks
   or;
3. Default to previously set state: Whichever was the last known state.

5. What surge protection measures are integrated into the appliance?

a. There are two scenarios relating to power surges;

The power lead plug typically has a 10A fuse that would trip, and isolate the appliance from any power surge.

If the power cable has no fuse, the onboard power supply would temporarily cut off should the power surge go above the above standard operating tolerance levels. In this scenario, the appliance would power back on when electrical supplies are back to normal.

6. As there are 12-ports on the appliance does that mean 12 separate servers (or other network devices) can be protected simultaneously?

a. Yes.

Each port is a pair of Layer 1 network interfaces, one in and one out, with no crossover or physical connection to any other port.

Ports are independently controlled and defined as a Layer 1 patch.

Each port can be configured to one of two specific operational modes; connected or disconnected.

It is possible to utilise a single port individually, or all of them, as required.

7. Is a separate phone number needed for each device port?

a. No. A single number is all that is required.

The phone number is linked to user profiles, not the port.

Users can be assigned to specific port(s), so when they attempt to control the port(s), they are challenged with the keywords attached to the user profile.

Operational Questions

8. What roles are defined when using the appliance?

a. There are two roles, defined as follows;

Administrator

- This role exclusively logs in via the Management Port located at the rear of the appliance to provide total physical separation of duties. Administrators can add/remove Administrators, add/edit/configure/remove Users, and general configuration and maintenance duties

User

- This role is defined as an approved User who has been authorised to remotely control the device using SMS. This role has no access to the Management Port, neither physically nor by proxy.

9. Can the device ports timeout after a period of inactivity? For example, if it was left open or closed by accident by a User?

a. Yes. From v2.1 of Goldilock's firmware, port opening and closing can be scheduled via the management interface.

10. How long does the complete system take to install?

a. No longer than an hour.

The appliance ships in a ready to be used condition, with everything pre-installed.

It is simply a matter of racking the equipment if applicable, connecting the cabling, powering on logging in as Administrator via the Management Port and being set up.

11. What commands are available via SMS?

a. A range of intuitive commands are available to users when sending SMS to the appliance, these include examples such as. These are sent to authorised administrator during the sale process.

12. How are User credentials and passphrases managed?

a. Only the Administrator role is authorised to add Users. Users are added to the list of approved Users with basic detail such as name,, passphrases and phone number. From there, Users can log in, change their password, and send SMS commands.

13. What can be backed up, and how does this process work?

a. There is no external back up procedure or process at this time to prevent details of device configuration being inadvertently downloaded and stored. A secure way of doing so is being considered.

Security Questions

14. How do Administrators authenticate and access the GUI?

a. Administrator Authentication for managing the appliance leverages strong authentication.

User credentials must be added to gain access by an approved administrator

Approved users are provided a One Time Passphrase upon initial access, which they are forced to change

Authentication Access the GUI

15. What method of strong authentication is available for the Management Console?

a. Administrator access via the physical Management Port located on the rear of the appliance, access permissions are standard domain level credentials.

16. What steps are taken to secure the device trigger mechanism?

a. SMS is utilised as just one part of a multi-step authentication process, that leverages different methods to further enhance security.

The device is configured to only receive, and then transmit, to registered phone numbers.

This ensures that as part of the challenge/response process, only authorised phone numbers receive the subsequent prompts.