Blank
Box
Technologies

For when tradecraft alone is ***not enough.***

Service Definition Document
G-Cloud 14

1. Introduction

The purpose of this document is to provide the reader with an overview of the Skylight Internet Investigations Platform. This document will describe the key capabilities of the Platform and services provided by Blankbox Technologies Ltd.

This document is intended for potential buyers and procurement leads. If you have any questions regarding the content of this document, then please contact us at **sales@blankbox.tech**

2. Who is Blankbox Technologies?

Blankbox Technologies works closely with organisations in the public and private sector delivering Threat Intelligence and Cyber Security Consultancy. We have used this experience and our in-house intelligence gathering capabilities to develop the Skylight platform.

Our vision is to enhance OSINT tradecraft with cutting edge infrastructure

Blankbox Technologies is a privately owned company registered in England and Wales. Our staff clearances range from BPSS to DV.

3. What is Skylight?

Skylight is a highly customisable Software as a Service (SaaS) platform that provides a single portal to a range of disposable secure infrastructure which allows users to browse the internet securely and anonymously. In addition to its core functionality, Skylight offers a range of add-on features to prolong the life of online profiles used by researchers and investigators to gather Open-Source Intelligence (OSINT).

Whilst primarily targeted at the Internet, Intelligence and Investigations community, it can be used by any public sector organisation that requires an internet browsing capability that is separated from their enterprise infrastructure.

Skylight's security was designed by Senior NCSC certified (CCP) security architects. The principles at the core of its design are:

- Zero Trust
- Assume Compromise
- Zero Knowledge

4. How does it work?

Skylight's core objectives are to provide the user with secure anonymous access to the internet and to prolong the life of their online profiles. It is accessible from a trusted device via any modern web browser. There is no need to install any software on the trusted device.

Skylight creates a secure anonymous boundary between the user's trusted device and the disposable desktop and mobile devices used by OSINT researchers and investigators. This enables users to browse untrusted and high-risk websites in confidence. The disposable devices offered within Skylight are treated as untrusted and can be destroyed and rebuilt either on a scheduled basis or manually by the user.

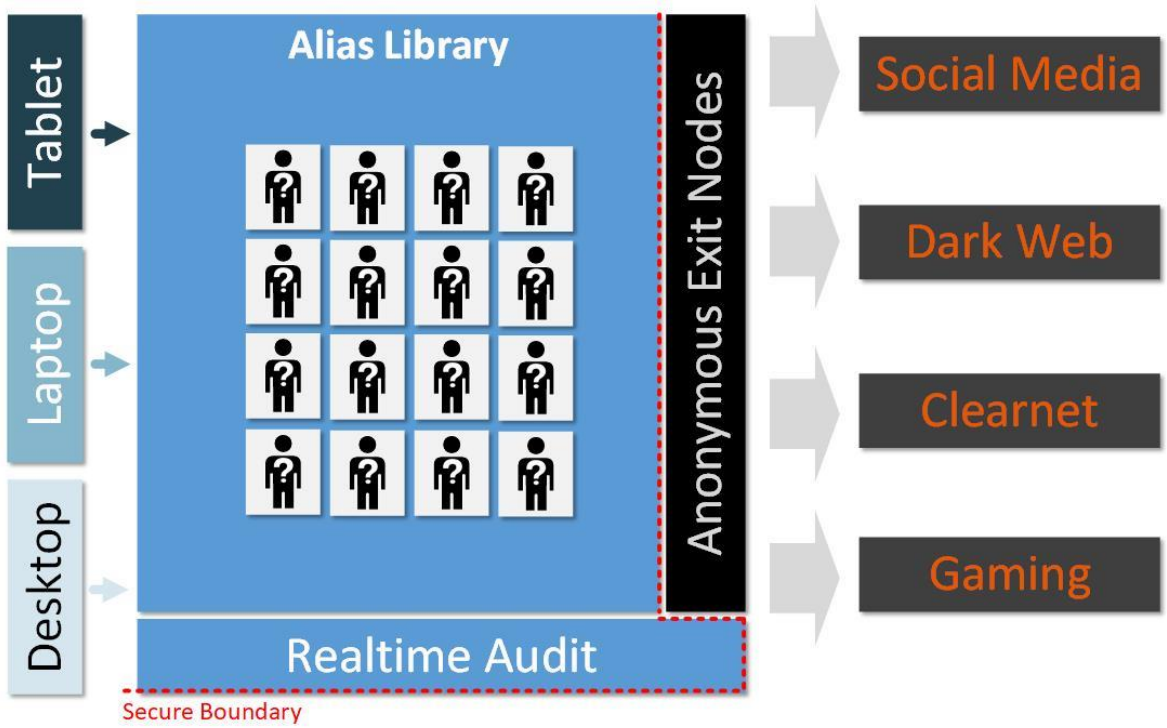

Figure 1: Skylight Alias Library and secure boundary

Skylight has an Alias Library and a range of additional features and components that enables users to customise their digital footprint and to emulate real world social media usage more effectively. This, in conjunction with our OSINT training has resulted in fewer social media profiles being blocked and deleted.

Users can configure every element of their digital footprint to ensure anonymity or to create a misattributable profile. Skylight has Exit Nodes located in 127 different countries with the ability to deploy custom hardware nodes in any country with basic internet access. Skylight allows the user to customise a wide range of attributes that contribute to their digital footprint. These include but are not limited to:

- Public and Private IP addresses
- Operating Systems and associated configurations
- Installed applications
- Browser and extensions
- International Mobile Equipment Identity (IMEI) number on Skylight mobile devices
- Disposable mobile phone numbers
- Mobile GPS coordinates

5. What can it be used for?

Skylight is a multipurpose platform and can be used in a wide range of scenarios. These scenarios can be broadly placed into one of three use cases:

5.1. Internet Intelligence and Investigation

Skylight can be used as the primary tool for Law Enforcement and other Agencies' investigators to collect intelligence online. Skylight offers a range of built-in functionality to aid case management and facilitate the export of data in compliance with evidential standards. Both Skylight desktop and mobile devices can be configured with all the investigative and OSINT tools required by investigators.

5.2. Secure Browsing

Skylight can be configured to provide users within an organisation with a secure browsing capability. There are several reasons why some users within an organisation require unrestricted access to the internet to perform their duties. Unrestricted access increases the risk of compromise. By using Skylight organisations can transfer that risk away from their corporate devices to an environment that is disposable and temporary. Any data that needs to be downloaded from the internet by these users can be passed securely through the Skylight Import Export (IMPEX) gateway to the user's trusted device.

5.3. Special Investigations

Some organisations have a need to conduct specialist and sensitive investigations online, such as investigations involving abuse imagery or highly capable threat actors. Skylight can be configured, hosted and accessed in compliance with the most demanding security and operational requirements.

6. Skylight Service Definition

6.1. Design Overview

Skylight was designed to use the latest virtualisation technologies to be as efficient and effective as possible. Figure 1 below provides a conceptual overview of Skylight's core architecture.

Skylight was designed to be hosted in any major Public Cloud environment.

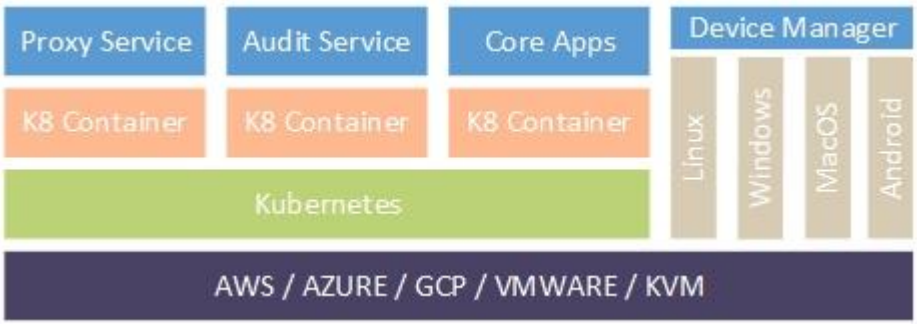

Figure 2: Skylight conceptual architecture

Figure 2 provides a logical view of the Platform. Users can access Skylight over the internet using any modern web browser. Once authenticated to Skylight, the user will be presented with a dashboard displaying their available devices. The user selects a device to spin up and will then be routed via one of the assigned un-attributable Exit Nodes.

Figure 3: Skylight logical high-level architecture

6.2. Access Control

Access to Skylight can be configured in several different ways depending on customer requirements. Skylight supports the following authentication mechanisms:

- Basic username and password
- Multi Factor Authentication
- Single Sign On using SAML2

Within the Platform access control is role based (RBAC). There are three levels of privilege within the Platform:

- Super Admin – This role has access to all the data and functionality within the Platform
- Admin – This role has access to all the data produced by users that are assigned to them. They can also manage users that are assigned to them.
- User – This role is used by investigators and researchers.

6.3. Encryption

Maintaining data confidentiality is an essential objective of the Skylight Platform. As such, ***all*** user generated data can be encrypted within the Platform using AES256. Skylight uses PKI to encrypt the data. This allows customers to supply their own encryption keys, thus strengthening the level of confidentiality further.

It must be noted that some features such as the ability to review recordings and downloaded files within the Platform would not be available when encrypted with customer supplied keys.

6.4. Auditing

Auditing user activity is one of the core capabilities of Skylight. User activity within the Platform and within Skylight devices are captured. All actions triggered by a user from the moment they log in to the moment they disconnect from Skylight are recorded in a secured audit database, accessible only by the super admin role.

Within Skylight devices there are two auditing mechanisms. All HTTP requests from devices are recorded by a web proxy within Skylight. These requests are searchable and can be exported to PDF.

In addition to recording each site visited by a user, Skylight can be configured to record a video of every session, thus capturing all non-browser activities such as disappearing chats on Telegram or Signal. This removes the need for the investigator to capture screenshots of important events, as everything is captured in a video. The recording is generated independently of the device. As such there is no agent software on the Skylight devices that can be tampered with or undermine the credibility of the device's profile.

6.5. Information Assurance

Skylight was designed with input from our experienced NCSC certified security architects to make the assurance of the Platform by customers as straightforward as possible.

Blankbox Technologies uses a Software Development Lifecycle that is based on NCSC secure development guidance[1] and the Microsoft Secure Development Lifecycle (SDL)[2].

As part of our development lifecycle, Blankbox Technologies conducts a range of security activities, including but not limited to attack vector analysis, dynamic security testing and regular developer security training.

[1] https://www.ncsc.gov.uk/collection/developers-collection
[2] https://www.microsoft.com/en-us/securityengineering/sdl

6.6. Pilots and Trial Deployments

Blankbox Technologies offers a 30 calendar day free trial period to all prospective customers. The trial licence provides up to 6 users access to a standard kiosk and mobile device. These devices will be linked to standard Skylight exit nodes.

6.7. Service and Support

Blankbox Technologies offers a second and third line support service in addition to the customer's first line support capability. Blankbox Technologies' support service is UK based and staff are NPPV 3 and SC cleared. The standard support service is available Monday to Friday from 09:00 until 17:00. This excludes Bank Holidays. An Enhanced Support service is available for customers that require extended support hours.

Standard support is provided via email and an online ticketing service. Telephone based support is available under the Enhanced Support service. The standard service response times to incidents are provided below:

Severity	Description	Response Time	Resolution Time	Response Updates
P1	Skylight is unavailable	1 business hour	24 hours	Every 2 hours within business hours
P2	Skylight performance is severely degraded	2 business hours	48 hours	Every 4 hours within business hours
P3	Skylight performance is degraded	4 business hours	72 hours	Daily (Monday to Friday)
P4	Standard Support request	24 business hours	5 working days	As required