Foresight Cyber Platform description

Version: 1.3

Release date: 2021-12-14

Document classification: INTERNAL

FORESIGHT® CYBER

1 INTRODUCTION

Foresight Cyber Platform is a collection of application and systems, part open source and part internally coded: designed and created by our technical gurus to enable seamless delivery of our various managed services, such as Skybox Security and Qualys managed services, and other as per clients' requirements.

This document describes the Foresight Cyber Platform focusing on the following:

- Use cases and connectors
- General system architecture
- Compute and storage requirements; Networking and secure connectivity requirements
- Data elements processed by Foresight Cyber in various services and platform hosting options
- Security of our platform

This document is intended for an organisation's IT and Security teams that work with the Foresight Cyber team in implementing our appliance-based Foresight Cyber Platform (referenced as 'the platform' throughout the document) into their environments.

1.1 Use cases and connectors

The Foresight Cyber Platform (referred to as FCP), is an in-house developed software using open-source components. The figure below shows the high-level statements about the FCP.

The FCP features a growing number of connectors to technologies. The connectors are developed based on the requirements from our teams and clients.

1.1.1 Use cases per connector

Technology	Data flow (as seen from FCP point of view)	Use case(s)
Skybox	Import	Import asset data and analyse against other sources, and create/enrich assets in the FCP with updated attributes; Analyse Skybox model; Monitor Skybox server and model health;
Qualys	Bi-directional	Import asset data and analyse against other sources, and create/enrich assets in the FCP with updated attributes; Import vulnerabilities to produce reports; Monitor key health metrics of Qualys data, scanner appliances, scans; Manage Qualys asset groups and asset tags based on the data in the FCP
Zabbix	Bi-directional	Import asset data and analyse against other sources, and create/enrich assets in the FCP with updated attributes; Pre-process data for which Zabbix does not have templates; Send status of the FCP and its data to Zabbix so every collection/job of platform is monitored by Zabbix
AWS	Import	Import asset data and analyse against other sources, and create/enrich assets in the FCP with updated attributes; Enrich assets with tags; *(roadmap for Q3' 22)*
Linux and Windows (via Zabbix)	Import	Import asset data and analyse against other sources, and create/enrich assets in the FCP with updated attributes; Monitor for changes – files , registry, users, groups, etc;

Ansible	Import	Use data from Ansible facts to import accounts; SSH keys used, interfaces, packages, vulnerabilities, and other data; Gather info about DNS settings on hosts assets;
DHCP Logs	Import	Import DHCP leases and analyse against other sources of host asset information; Enrich model with current MAC addresses for IP addresses for host asset deduplication/discovery;
DNS Zones	Bi-directional	Create DNS zones based on the asset data in CMDB; Correlate DNS zones with FCP; Monitor DNS zones for updates; Correlate with actual DNS settings on assets *(roadmap Q3 '22)*
System logs	Import	Import system / security logs for analysis; Correlate account login events with changes made on assets; *(roadmap Q3 '22)*
Firewall logs	Import	Import logs to discover host communicating on the network to correlate with known host assets, and discover previous unknown hosts. Monitor for specific allowed / not-allowed communication flows, report and alert *(roadmap Q4 '22)*
Netflow logs	Import	Import logs to discover host communicating on the network to correlate with known host assets, and discover previous unknown hosts; Find real dependency between hosts assets based on flows; Monitor for specific allowed / not-allowed communication flows, report and alert *(roadmap Q3 '22)*
ServiceNow	Bi-directional	Import asset data and analyse against other sources, and create/enrich assets in the FCP with updated attributes; Create new assets; Enrich assets with attributes using the ServiceNow data model; Create relationships between assets; Import Business Applications and link them to hosts; Create Incidents / Service Requests; *(roadmap tbd based on requirements)*
Hardenize	Import	Import discovered hosts and analyse against other sources; Retrieve analysis of DNS and Email setup per domain and monitor for issues, create alerts; *(roadmap Q3 '22)*
Microsoft Azure AD	Import	Import hosts and analyse against other sources; Import Users and Groups to correlate with other sources of user information; Create links between devices and owners; Tag assets within the FCP based on device state (e.g. no logons, not connected, AzureAD managed, compliant, ...);
Active Directory	Import	Import asset data and analyse against other sources, and create/enrich assets in the FCP with updated attributes;

		Create links between computers and persons who added computers to the AD; Tag host assets within the FCP based on computer state (no logons, not connected, ...)
iTop	Import	Import asset data and analyse against other sources, and create/enrich assets in the FCP with updated attributes; Create relationships between assets; Import Business Applications and link them to hosts;
Request Tracker	Import	Create Incidents / Service Requests; Retrieve ticket updates; Monitor for tickets SLA; Correlate tickets with actual changes on hosts assets; *(roadmap Q3 '22)*
RemedyForce	Import	Import asset data and analyse against other sources; Create relationships between hosts assets within FCP; Import Business Applications and link them to hosts within FCP;

1.1.2 Use case – Asset Discovery & Asset registries data correlation

One of the key use cases is the asset correlation and enrichment. The FCP produces reports showing gaps in the asset registries of the established connectors.

For example, 'server1' is in the Active Directory, no DHCP logs (because of static IP), is scanned for vulnerabilities, but is not in the CMDB (such as ServiceNow).

Such reports enable companies to rectify by either importing missing data or looking into underlying problem, e.g. why the asset data are not updated.

Asset	IT CMDB	Active Directory	DHCP logs	Vulnerability scans
server1	Missing	✓	N/A	✓
PC165	Duplicated 2x	✓	✓	✓
Printer A	✓	Missing	✓	Missing
HVAC_unit_13	Missing	N/A	N/A	Missing
WifiAP-120	Missing	N/A	N/A	✓
DoorSecurity-A14	Missing	Missing	N/A	Missing
Laptop_ceo	✓	✓	✓	Missing
Hacker_PC	Missing	Missing	✓	Missing
Firewall-1	Partial – one interface only	N/A	N/A	✓

1.2 General System Architecture

The platform runs on a Linux appliance based on a minimum Debian install with only required packages deployed.

1.2.1 Installation

The appliance can be installed as fully installed virtual or hardware appliance – contains all code and applications and requires only network and basic user account configuration, delivered via a wizard-like setup. For this deployment, we supply a vmdk or OVA (other formats possible) to install on virtual hosts. Alternatively, we can supply and ship our hardware appliance to the client's designated address for racking and stacking[1].

1.2.2 Platform components

The platform contains various open-source and internally developed components. The critical ones are listed below:

- Zabbix - https://www.zabbix.com/
- Elastic Search & Kibana - https://www.elastic.co/products/elastic-stack
- Logstash - https://www.elastic.co/products/logstash
- Grafana - https://grafana.com/
- Request Tracker - https://bestpractical.com/request-tracker/
- Rsyslog - https://www.rsyslog.com/
- PostgreSQL - https://www.postgresql.org/
- Python Scripts – internally developed

The choice of the hosting design is typically driven by client's security and compliance requirements.

Software licenses used in components that are part of the FCP:

- GNU General Public License (GPL)
- Apache 2.0
- The PostgreSQL Licence
- BSD License

The FCP code that is developed in house is licensed 'Elastic License 2.0 (ELv2)'[2]

[1] Our teams are skilled in racking and stacking and can, on request, perform such operations.
[2] https://www.elastic.co/licensing/elastic-license

2 FORESIGHT CYBER PLATFORM

2.1 Data processing

As part of our services, Foresight Cyber collect and process various data about client's assets depending on platform option.

Examples of data types processed:

- IP address
- Location
- Contact
- Asset information
- Network topology
- Network device configuration
- Vulnerability occurrences
- Client's documentation
- Service request tickets
- Reports produced by managed software or by Foresight Cyber SOC

Foresight Cyber uses Office365 (EU tenant) internally and to deliver the services. SharePoint data and emails are backed up on daily basis to an off-site backup servers.

2.2 Platform hosting options

We recognise the infrastructure and security requirements of clients vary. As such, we have created flexible options how our platform is hosted and how our SOC team delivers the services:

1. Fully hosted by Foresight Cyber
2. Split hosting between Foresight Cyber and a client
3. Hosting of the platform fully on client's premises

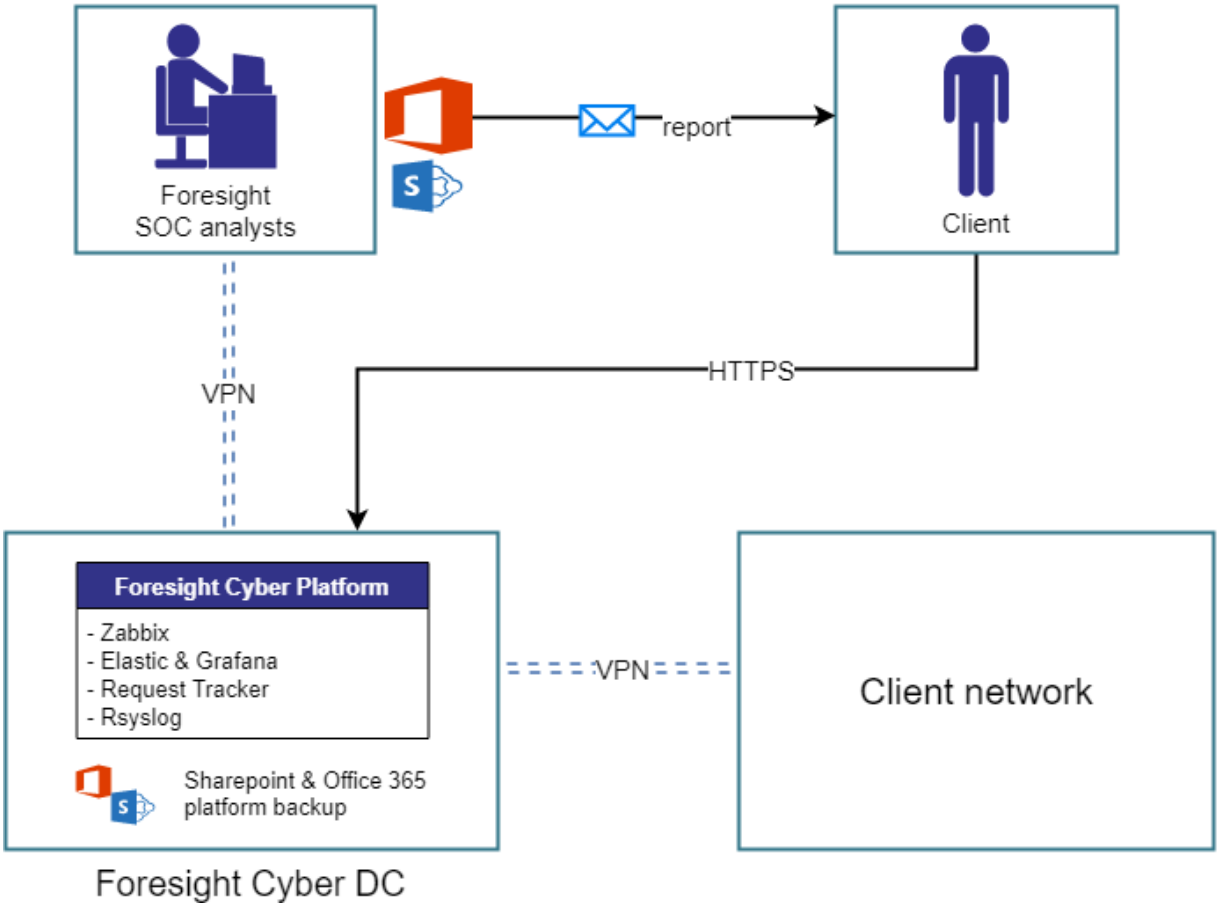
2.2.1 Option 1 - Fully hosted by Foresight Cyber

This option is aimed at small and medium size businesses. Our platform is fully hosted at Foresight Cyber datacentres.

The secure connectivity, typically a VPN connection, is from the date centre to the client's network – whether that be at a client location or cloud-based. There is nothing for a client to install. We only require configuration of the secure links to connect to specific systems. These connections are dependent on servicer(s) delivered.

Figure 1 below depicts such an architecture.

Figure 1 Platform fully hosted by Foresight Cyber



Data location	Data elements
Foresight Cyber DC	IP addresses, locations, contacts, asset information, network topology, vulnerability occurrences
Office 365	Contact data, emails, reports, vulnerability occurrences, client's documentation
Client network	No special arrangement for data to be hosted on client network

2.2.2 Option 2 - Split architecture option

This option is aimed at medium to large size businesses with standard 3rd party hosting and data governance compliance requirements. The platform is split hosted at Foresight Cyber datacentres and client's environment.

We have designed the platform such as in this option the critical information is retained within the client's environment.

The only two systems retained on our data centres is Request Tracker, used by our teams to manage tasks and deliver services.

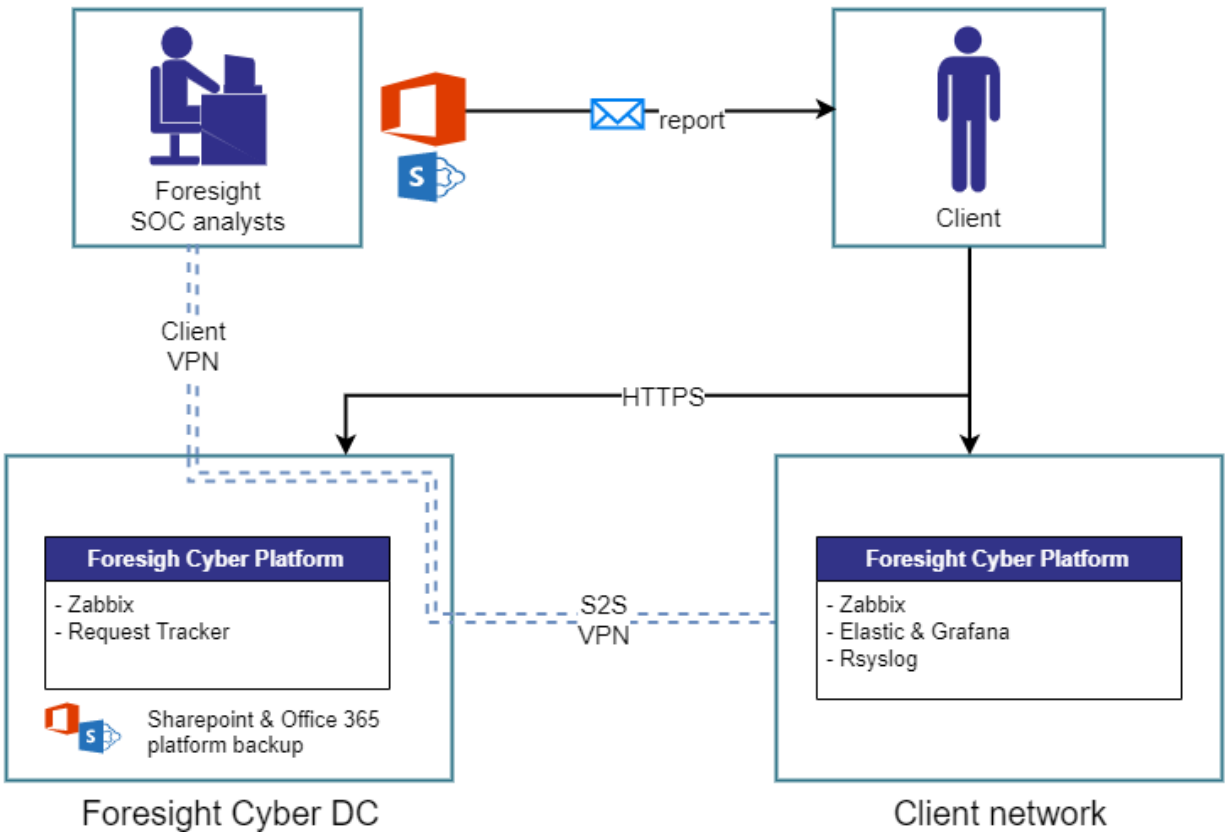
The platform is configured to send alerts to our Zabbix system when parameters of the hosted platform are outside of the optimal values.

The only data exported outside of client's network is:

- System and network information necessary to debug service issues by creating tickets in our Request Tracker and Zabbix

Figure 2 below depicts such an architecture.

Figure 2 Split architecture option



Data location	Data elements

Foresight Cyber DC	IP addresses, contacts, partial asset information
Office 365	Contact data, emails, reports, vulnerability occurrences, client's documentation
Client network	IP addresses, location, contact, asset information, network topology, network device configuration, vulnerability occurrences

2.2.3 Option 3 - Client hosting only option

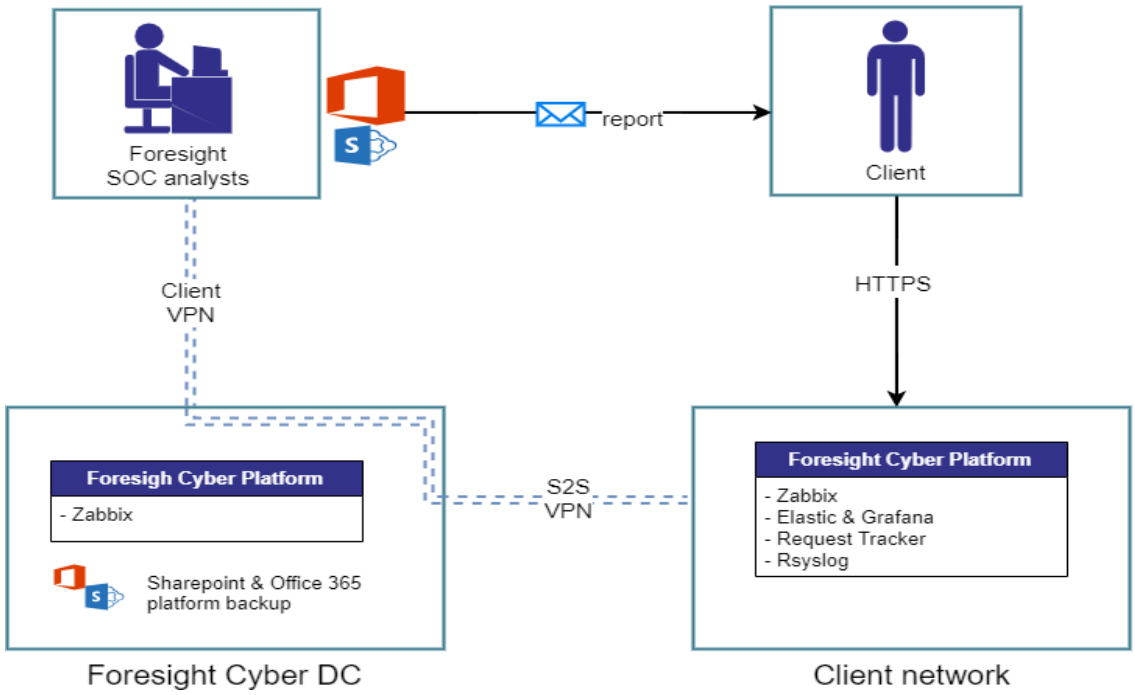
This option is aimed at large size businesses or those with specific 3rd party hosting and data governance compliance requirements. The platform is fully hosted inside the organisation's environment. Our security engineers establish secure links between our platform and specific systems (service dependent) as per the client's 3rd party secure access policies and standards.

With this option, our platform is designed so that all information is retained within the organisation's environment.

The platform inside the client's environment sends monitoring heartbeats and critical alerts to Foresight Cyber Platform in our data centre and these are processes by Zabbix. This setup allows our engineering teams to be alerted about any availability or capacity issues.

Figure 3 below depicts such an architecture.

Figure 3 Client hosting architecture



Data location	Data elements
Foresight Cyber DC	IP addresses, contacts, partial asset information

Office 365	Contact data, emails, reports
Client network	IP addresses, locations, contacts, asset information, network topology, client's documentation, vulnerability occurrences

2.2.4 Option 4 - Client hosting including windows access appliance

This option build on the previous option and adds additional protection by ensuring all windows and Office365 apps run from a virtual server hosted inside client's network. Our security engineers establish secure VPN, using client's approved solution, and access a virtual Windows server appliance, typically located either in DMZ or close to Foresight Cyber Platform Linux appliance.

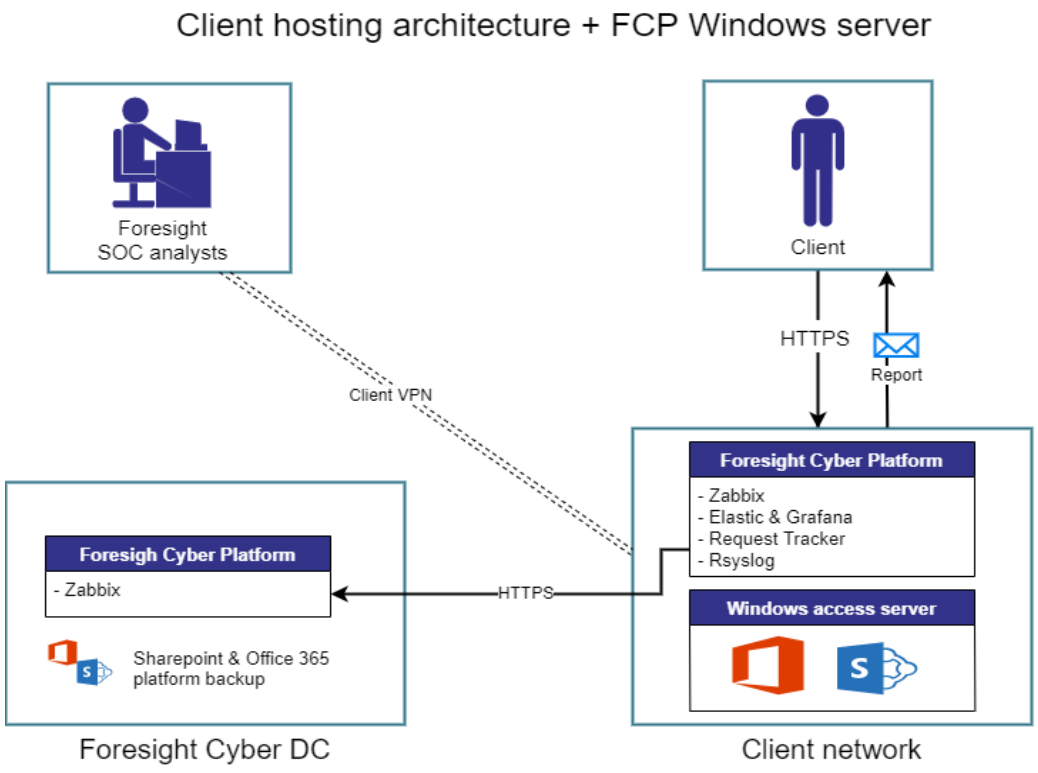
The Windows terminal server runs on the latest Windows server version and is hardened to Microsoft high-security server baseline. Only a Remote Desktop service is open and allows Foresight Cyber analysts to login, but only after establishing secure VPN connection to client's network.

Analysts then use tooling installed locally, such as Office365 apps and Skybox Java app, on the Windows server to deliver services.

The server and terminal server license is delivered by Foresight Cyber.

Figure below depicts such an architecture.

Figure 4 Enhanced client hosting architecture



Data location	Data elements
Foresight Cyber DC	Alert information, not containing any client's information
Office 365	Contact data, emails
Client network	IP addresses, locations, contacts, asset information, network topology, client's documentation, vulnerability occurrences Reports generated by analysis on Windows server

2.3 Compute and storage requirements

Our platform minimum hosting requirements are as follow – these are applicable to option's 2, 3 and 4

Resource	Value	Note
CPU	4	vCPU or HW processor
RAM	32 GB	Can be expanded based on growing requirements, size of the network, service delivered etc.
System Disk	150GB Minimum standard SAS/SATA 7.2k HDD	Used for standard Debian Linux files including the swap
Data Disk	500 GB Minimum standard SAS 10k HDD Recommended Intel X25-M G2 like IOPS of 8600 for optimal performance Maximum performance: designed between Foresight Cyber CTO and the client's storage architects	Used for platform data Can be expanded based on growing requirements, size of the network, service delivered etc.
Connectivity	Minimum 1Gbps full duplex Optimal 2 x 1 Gbps full duplex in LACP mode for resiliency	

Additionally, in the option 4, a Windows server has the following requirements:

Resource	Value	Note
CPU	8	vCPU or HW processor
RAM	64 GB	Can be expanded based on growing requirements, size of the network, service delivered etc.
System Disk	150GB Minimum standard SAS/SATA 7.2k HDD	Used for standard Windows server installation
Data Disk	1TB GB Minimum standard SAS 10k HDD Recommended Intel X25-M G2 like IOPS of 8600 for optimal performance	Used for user data, reports, temporary files, email offline files Can be expanded based on growing requirements, size of the network, service delivered etc.

	Maximum performance: designed between Foresight Cyber CTO and the client's storage architects	
Ethernet	Minimum 1Gbps full duplex Optimal 2 x 1 Gbps full duplex in LACP mode for resiliency	

When a client provides Virtual Desktop Infrastructure to our teams, in lieu of Windows server hosting, the requirements are discussed during the design phase.

2.4 Networking and secure connectivity requirements

The platform is built with 'secure by design' and 'limit attack surface' principles as standard. As such, this only requires the minimum ports to be open to/from the platform.

The platform needs just one ethernet virtual/physical port to be connected. In exceptional circumstances, we can use admin interfaces: iLO on the physical appliance or virtual access through the hypervisor platform providing out-of-band management of the appliance.

The exact network protocols vary based on service, hence we only exhibit the protocols that are common for all services:

Table 1 – Connectivity flows

Source	Destination	Protocol
Foresight Cyber Engineers	VDI Servers	https, ports to be provided by client
Foresight Cyber Engineers	Skybox server	22/TCP 444/TCP 8443/TCP
Foresight Cyber Engineers	Skybox collector	22/TCP
Skybox server Skybox collector	Foresight Cyber Platform	22/TCP 514/TCP 514/UDP 9201/TCP 10051/TCP
Foresight Cyber Platform	Skybox server Skybox collector	22/TCP
Foresight Cyber Engineers	Allowed list of domains and FQDNs	https; direct or view a proxy
Foresight Cyber Engineers Foresight Cyber Platform	Client's CMDB	https

2.4.1 Domains and FQDNs

From the Bank's VDI (D), Foresight Cyber Engineers (A) will need to access, using https protocol, the following domains and FQDNs:

Table 2 - Access to Internet requirements

Domain / FQDN	Reason
box.foresightcyber.com	Scripts and tools for skybox service

*.skyboxsecurity.com	Skybox updates, support tickets and portal for creating and updating support requests
Office 365 domains (as listed by Microsoft https://docs.microsoft.com/en-us/microsoft-365/enterprise/urls-and-ip-address-ranges?view=o365-worldwide)	For option 4: Manual work on reports
putty.org	For option 4: PuTTY is an SSH and telnet client
winscp.net	For option 4: WinSCP is SFTP/FTP client

2.5 Security of our platform

As an internationally respected security services company, we have designed our platform from the ground up, integrating the most secure security requirements available today. Our effort and the resulting configuration should satisfy even the most security conscious and compliance heavy environments.

The key details of the platform security are:

1. Secure boot enabled on HW appliance – secured by TPM 2.0 and BIOS configuration
2. Minimum Debian install – only package needed to run the platform are installed
3. Linux is securely configured according to CIS Benchmark for Debian Level 2
4. SELinux is enabled and is set to monitoring mode
5. SSH access configured for ed25519 keys only, root login disabled, and only strong ciphers enabled
6. Sudo enabled only for admin users
7. Auditing enabled (via package audit)
8. Partition encryption enabled on request when out-of-band access procedures are agreed
9. Web access is secured by TLS1.3, only strong ciphers allowed, and enforced authentication

2.5.1 Security of platform components

All platform components accessible from web interface are secure via HTTPS protocol with SSL/TLS certificate and specific port. Next, to this, all web interfaces require credentials to be accessible.

3 APPENDIX A – PLATFORM HARDENING

The FCP is hardened against Centre for Internet Security (CIS) Level 2 (where possible).

The following controls are implemented:

- [1] Initial Setup
- [1.1] Filesystem Configuration
- [1.1.1] Disable unused filesystems
    - [1.1.1.1.] Ensure mounting of freevxfs filesystems is disabled (Scored)
    - [1.1.1.2] Ensure mounting of jffs2 filesystems is disabled (Scored)
    - [1.1.1.3] Ensure mounting of hfs filesystems is disabled (Scored)
    - [1.1.1.4] Ensure mounting of hfsplus filesystems is disabled (Scored)
    - [1.1.1.5] Ensure mounting of udf filesystems is disabled (Scored)
    - [1.1.2] Ensure /tmp is configured (Scored)
    - [1.1.3] Ensure nodev option set on /tmp partition (Scored)
    - [1.1.4] Ensure nosuid option set on /tmp partition (Scored)
    - [1.1.5] Ensure noexec option set on /tmp partition (Scored)
    - [1.1.6] Ensure separate partition exists for /var (Scored)
    - [1.1.7] Ensure separate partition exists for /var/tmp (Scored)
    - [1.1.8] Ensure nodev option set on /var/tmp partition (Scored)
    - [1.1.9] Ensure nosuid option set on /var/tmp partition (Scored)
    - [1.1.10] Ensure noexec option set on /var/tmp partition (Scored)
    - [1.1.11] Ensure separate partition exists for /var/log (Scored)
    - [1.1.12] Ensure separate partition exists for /var/log/audit (Scored)
    - [1.1.13] Ensure separate partition exists for /home (Scored)
    - [1.1.14] Ensure nodev option set on /home partition (Scored)
    - [1.1.15] Ensure nodev option set on /dev/shm partition (Scored)
    - [1.1.16] Ensure nosuid option set on /dev/shm partition (Scored)
    - [1.1.17] Ensure noexec option set on /dev/shm partition (Scored)
    - [1.1.18] Ensure nodev option set on removable media partitions (Not Scored)
    - [1.1.19] Ensure nosuid option set on removable media partitions (Not Scored)
    - [1.1.20] Ensure noexec option set on removable media partitions (Not Scored)

- [1.1.21] Ensure sticky bit is set on all world-writable directories (Scored)
- [1.1.22] Disable Automounting (Scored)

- [1.2] Configure Software Updates
  - [1.2.1] Ensure package manager repositories are configured (Not Scored)
  - [1.2.2] Ensure GPG keys are configured (Not Scored)
- [1.3] Filesystem Integrity Checking
  - [1.3.1] Ensure AIDE is installed (Scored)
  - [1.3.2] Ensure filesystem integrity is regularly checked (Scored)
- [1.4] Secure Boot Settings
  - [1.4.1] Ensure permissions on bootloader config are configured (Scored)
  - [1.4.2] Ensure bootloader password is set (Scored)
  - [1.4.3] Ensure authentication required for single user mode (Scored)
- [1.5] Additional Process Hardening
  - [1.5.1] Ensure core dumps are restricted (Scored)
  - [1.5.2] Ensure XD/NX support is enabled (Not Scored)
  - [1.5.3] Ensure address space layout randomization (ASLR) is enabled (Scored)
  - [1.5.4] Ensure prelink is disabled (Scored)
- [1.6] Mandatory Access Control
- [1.6.1] Configure SELinux
  - [1.6.1.1] Ensure SELinux is enabled in the bootloader configuration (Scored)
  - [1.6.1.2] Ensure the SELinux state is enforcing (Scored)
  - [1.6.1.3] Ensure SELinux policy is configured (Scored)
  - [1.6.1.4] Ensure no unconfined daemons exist (Scored)
- [1.6.2] Configure AppArmor
  - [1.6.2.1] Ensure AppArmor is enabled in the bootloader configuration (Scored)
  - [1.6.2.2] Ensure all AppArmor Profiles are enforcing (Scored)
  - [1.6.3] Ensure SELinux or AppArmor are installed (Scored)
- [1.7] Warning Banners
- [1.7.1] Command Line Warning Banners
  - [1.7.1.1] Ensure message of the day is configured properly (Scored)
  - [1.7.1.2] Ensure local login warning banner is configured properly (Scored)
  - [1.7.1.3] Ensure remote login warning banner is configured properly (Scored)

    - [1.7.1.4] Ensure permissions on /etc/motd are configured (Scored)
    - [1.7.1.5] Ensure permissions on /etc/issue are configured (Scored)
    - [1.7.1.6] Ensure permissions on /etc/issue.net are configured (Scored)
    - [1.7.2] Ensure GDM login banner is configured (Scored)
    - [1.8] Ensure updates, patches, and additional security software are installed (Not Scored)
- [2] Services
- [2.1] inetd Services
    - [2.1.1] Ensure xinetd is not installed (Scored)
    - [2.1.2] Ensure openbsd-inetd is not installed (Scored)
- [2.2] Special Purpose Services
- [2.2.1] Time Synchronization
    - [2.2.1.1] Ensure time synchronization is in use (Not Scored)
    - [2.2.1.2] Ensure ntp is configured (Scored)
    - [2.2.1.3] Ensure chrony is configured (Scored)
    - [2.2.2] Ensure X Window System is not installed (Scored)
    - [2.2.3] Ensure Avahi Server is not enabled (Scored)
    - [2.2.4] Ensure CUPS is not enabled (Scored)
    - [2.2.5] Ensure DHCP Server is not enabled (Scored)
    - [2.2.6] Ensure LDAP server is not enabled (Scored)
    - [2.2.7] Ensure NFS and RPC are not enabled (Scored)
    - [2.2.8] Ensure DNS Server is not enabled (Scored)
    - [2.2.9] Ensure FTP Server is not enabled (Scored)
    - [2.2.10] Ensure HTTP server is not enabled (Scored)
    - [2.2.11] Ensure IMAP and POP3 server is not enabled (Scored)
    - [2.2.12] Ensure Samba is not enabled (Scored)
    - [2.2.13] Ensure HTTP Proxy Server is not enabled (Scored)
    - [2.2.14] Ensure SNMP Server is not enabled (Scored)
    - [2.2.15] Ensure mail transfer agent is configured for local-only mode (Scored)
    - [2.2.16] Ensure rsync service is not enabled (Scored)
    - [2.2.17] Ensure NIS Server is not enabled (Scored)
- [2.3] Service Clients
    - [2.3.1] Ensure NIS Client is not installed (Scored)

    - [2.3.2] Ensure rsh client is not installed (Scored)
    - [2.3.3] Ensure talk client is not installed (Scored)
    - [2.3.4] Ensure telnet client is not installed (Scored)
    - [2.3.5] Ensure LDAP client is not installed (Scored)
- [3] Network Configuration
- [3.1] Network Parameters (Host Only)
    - [3.1.1] Ensure IP forwarding is disabled (Scored)
    - [3.1.2] Ensure packet redirect sending is disabled (Scored)
- [3.2] Network Parameters (Host and Router)
    - [3.2.1] Ensure source routed packets are not accepted (Scored)
    - [3.2.2] Ensure ICMP redirects are not accepted (Scored)
    - [3.2.3] Ensure secure ICMP redirects are not accepted (Scored)
    - [3.2.4] Ensure suspicious packets are logged (Scored)
    - [3.2.5] Ensure broadcast ICMP requests are ignored (Scored)
    - [3.2.6] Ensure bogus ICMP responses are ignored (Scored)
    - [3.2.7] Ensure Reverse Path Filtering is enabled (Scored)
    - [3.2.8] Ensure TCP SYN Cookies is enabled (Scored)
    - [3.2.9] Ensure IPv6 router advertisements are not accepted (Scored)
- [3.3] TCP Wrappers
    - [3.3.1] Ensure TCP Wrappers is installed (Scored)
    - [3.3.2] Ensure /etc/hosts.allow is configured (Not Scored)
    - [3.3.3] Ensure /etc/hosts.deny is configured (Not Scored)
    - [3.3.4] Ensure permissions on /etc/hosts.allow are configured (Scored)
    - [3.3.5] Ensure permissions on /etc/hosts.deny are configured (Scored)
- [3.4] Uncommon Network Protocols
    - [3.4.1] Ensure DCCP is disabled (Not Scored)
    - [3.4.2] Ensure SCTP is disabled (Not Scored)
    - [3.4.3] Ensure RDS is disabled (Not Scored)
    - [3.4.4] Ensure TIPC is disabled (Not Scored)
- [3.5] Firewall Configuration
- [3.5.1] Configure IPv4 iptables
    - [3.5.1.1] Ensure default deny firewall policy (Scored)

    - [3.5.1.2] Ensure loopback traffic is configured (Scored)
    - [3.5.1.3] Ensure outbound and established connections are configured (Not Scored)
    - [3.5.1.4] Ensure firewall rules exist for all open ports (Scored)
- [3.5.2] Configure IPv6 ip6tables
    - [3.5.2.1] Ensure IPv6 default deny firewall policy (Scored)
    - [3.5.2.2] Ensure IPv6 loopback traffic is configured (Scored)
    - [3.5.2.3] Ensure IPv6 outbound and established connections are configured (Not Scored)
    - [3.5.2.4] Ensure IPv6 firewall rules exist for all open ports (Not Scored)
    - [3.5.3] Ensure iptables is installed (Scored)
    - [3.6] Ensure wireless interfaces are disabled (Not Scored)
    - [3.7] Disable IPv6 (Not Scored)
- [4] Logging and Auditing
- [4.1] Configure System Accounting (auditd)
- [4.1.1] Configure Data Retention
    - [4.1.1.1] Ensure audit log storage size is configured (Not Scored)
    - [4.1.1.2] Ensure system is disabled when audit logs are full (Scored)
    - [4.1.1.3] Ensure audit logs are not automatically deleted (Scored)
    - [4.1.2] Ensure auditd service is enabled (Scored)
    - [4.1.3] Ensure auditing for processes that start prior to auditd is enabled (Scored)
    - [4.1.4] Ensure events that modify date and time information are collected (Scored)
    - [4.1.5] Ensure events that modify user/group information are collected (Scored)
    - [4.1.6] Ensure events that modify the system's network environment are collected (Scored)
    - [4.1.7] Ensure events that modify the system's Mandatory Access Controls are collected (Scored)
    - [4.1.8] Ensure login and logout events are collected (Scored)
    - [4.1.9] Ensure session initiation information is collected (Scored)
    - [4.1.10] Ensure discretionary access control permission modification events are collected (Scored)

    - [4.1.11] Ensure unsuccessful unauthorized file access attempts are collected (Scored)
    - [4.1.12] Ensure use of privileged commands is collected (Scored)
    - [4.1.13] Ensure successful file system mounts are collected (Scored)
    - [4.1.14] Ensure file deletion events by users are collected (Scored)
    - [4.1.15] Ensure changes to system administration scope (sudoers) is collected (Scored)
    - [4.1.16] Ensure system administrator actions (sudolog) are collected (Scored)
    - [4.1.17] Ensure kernel module loading and unloading is collected (Scored)
    - [4.1.18] Ensure the audit configuration is immutable (Scored)
- [4.2] Configure Logging
- [4.2.1] Configure rsyslog
    - 4.2.1.1 Ensure rsyslog Service is enabled (Scored)
    - 4.2.1.2 Ensure logging is configured (Not Scored)
    - 4.2.1.3 Ensure rsyslog default file permissions configured (Scored)
    - 4.2.1.4 Ensure rsyslog is configured to send logs to a remote log host (Scored)
    - 4.2.1.5 Ensure remote rsyslog messages are only accepted on designated log hosts. (Not Scored)
- [4.2.2] Configure syslog-ng
    - [4.2.2.1] Ensure syslog-ng service is enabled (Scored)
    - [4.2.2.2] Ensure logging is configured (Not Scored)
    - [4.2.2.3] Ensure syslog-ng default file permissions configured (Scored)
    - [4.2.2.4] Ensure syslog-ng is configured to send logs to a remote log host (Not Scored)
    - [4.2.2.5] Ensure remote syslog-ng messages are only accepted on designated log hosts (Not Scored)
    - [4.2.3] Ensure rsyslog or syslog-ng is installed (Scored)
    - [4.2.4] Ensure permissions on all logfiles are configured (Scored)
    - [4.3] Ensure logrotate is configured (Not Scored)
- [5] Access, Authentication and Authorization
- [5.1] Configure cron
    - [5.1.1] Ensure cron daemon is enabled (Scored)
    - [5.1.2] Ensure permissions on /etc/crontab are configured (Scored)
    - [5.1.3] Ensure permissions on /etc/cron.hourly are configured (Scored)

    - [5.1.4] Ensure permissions on /etc/cron.daily are configured (Scored)
    - [5.1.5] Ensure permissions on /etc/cron.weekly are configured (Scored)
    - [5.1.6] Ensure permissions on /etc/cron.monthly are configured (Scored)
    - [5.1.7] Ensure permissions on /etc/cron.d are configured (Scored)
    - [5.1.8] Ensure at/cron is restricted to authorized users (Scored)
- [5.2] SSH Server Configuration
    - [5.2.1] Ensure permissions on /etc/ssh/sshd_config are configured (Scored)
    - [5.2.2] Ensure permissions on SSH private host key files are configured (Scored)
    - [5.2.3] Ensure permissions on SSH public host key files are configured (Scored)
    - [5.2.4] Ensure SSH Protocol is set to 2 (Scored)
    - [5.2.5] Ensure SSH LogLevel is appropriate (Scored)
    - [5.2.6] Ensure SSH X11 forwarding is disabled (Scored)
    - [5.2.7] Ensure SSH MaxAuthTries is set to 4 or less (Scored)
    - [5.2.8] Ensure SSH IgnoreRhosts is enabled (Scored)
    - [5.2.9] Ensure SSH HostbasedAuthentication is disabled (Scored)
    - [5.2.10] Ensure SSH root login is disabled (Scored)
    - [5.2.11] Ensure SSH PermitEmptyPasswords is disabled (Scored)
    - [5.2.12] Ensure SSH PermitUserEnvironment is disabled (Scored)
    - [5.2.13] Ensure only strong ciphers are used (Scored)
    - [5.2.14] Ensure only strong MAC algorithms are used (Scored)
    - [5.2.15] Ensure only strong Key Exchange algorithms are used (Scored)
    - [5.2.16] Ensure SSH Idle Timeout Interval is configured (Scored)
    - [5.2.17] Ensure SSH LoginGraceTime is set to one minute or less (Scored)
    - [5.2.18] Ensure SSH access is limited (Scored)
    - [5.2.19] Ensure SSH warning banner is configured (Scored)
- [5.3] Configure PAM
    - 5.3.1 Ensure password creation requirements are configured (Scored)
    - [5.3.2] Ensure lockout for failed password attempts is configured (Scored)
    - [5.3.3] Ensure password reuse is limited (Scored)
    - [5.3.4] Ensure password hashing algorithm is SHA-512 (Scored)
- [5.4] User Accounts and Environment

- [5.4.1] Set Shadow Password Suite Parameters
  - [5.4.1.1] Ensure password expiration is 365 days or less (Scored)
  - [5.4.1.2] Ensure minimum days between password changes is 7 or more (Scored)
  - [5.4.1.3] Ensure password expiration warning days is 7 or more (Scored)
  - [5.4.1.4] Ensure inactive password lock is 30 days or less (Scored)
  - [5.4.1.5] Ensure all users last password change date is in the past (Scored)
  - [5.4.2] Ensure system accounts are non-login (Scored)
  - [5.4.3] Ensure default group for the root account is GID 0 (Scored)
  - [5.4.4] Ensure default user umask is 027 or more restrictive (Scored)
  - [5.4.5] Ensure default user shell timeout is 900 seconds or less (Scored)
  - [5.5] Ensure root login is restricted to system console (Not Scored)
  - [5.6] Ensure access to the su command is restricted (Scored)
- [6] System Maintenance
- [6.1] System File Permissions
  - [6.1.1] Audit system file permissions (Not Scored)
  - [6.1.2] Ensure permissions on /etc/passwd are configured (Scored)
  - [6.1.3] Ensure permissions on /etc/shadow are configured (Scored)
  - [6.1.4] Ensure permissions on /etc/group are configured (Scored)
  - [6.1.5] Ensure permissions on /etc/gshadow are configured (Scored)
  - [6.1.6] Ensure permissions on /etc/passwd- are configured (Scored)
  - [6.1.7] Ensure permissions on /etc/shadow- are configured (Scored)
  - [6.1.8] Ensure permissions on /etc/group- are configured (Scored)
  - [6.1.9] Ensure permissions on /etc/gshadow- are configured (Scored)
  - [6.1.10] Ensure no world writable files exist (Scored)
  - [6.1.11] Ensure no unowned files or directories exist (Scored)
  - [6.1.12] Ensure no ungrouped files or directories exist (Scored)
  - [6.1.13] Audit SUID executables (Not Scored)
  - [6.1.14] Audit SGID executables (Not Scored)
- [6.2] User and Group Settings
  - [6.2.1] Ensure password fields are not empty (Scored)
  - [6.2.2] Ensure no legacy "+" entries exist in /etc/passwd (Scored)
  - [6.2.3] Ensure no legacy "+" entries exist in /etc/shadow (Scored)

- [6.2.4] Ensure no legacy "+" entries exist in /etc/group (Scored)
- [6.2.5] Ensure root is the only UID 0 account (Scored)
- [6.2.6] Ensure root PATH Integrity (Scored)
- [6.2.7] Ensure all users' home directories exist (Scored)
- [6.2.8] Ensure users' home directories permissions are 750 or more restrictive (Scored)
- [6.2.9] Ensure users own their home directories (Scored)
- [6.2.10] Ensure users' dot files are not group or world writable (Scored)
- [6.2.11] Ensure no users have .forward files (Scored)
- [6.2.12] Ensure no users have .netrc files (Scored)
- [6.2.13] Ensure users' .netrc Files are not group or world accessible (Scored)
- [6.2.14] Ensure no users have .rhosts files (Scored)
- [6.2.15] Ensure all groups in /etc/passwd exist in /etc/group (Scored)
- [6.2.16] Ensure no duplicate UIDs exist (Scored)
- [6.2.17] Ensure no duplicate GIDs exist (Scored)
- [6.2.18] Ensure no duplicate user names exist (Scored)
- [6.2.19] Ensure no duplicate group names exist (Scored)
- [6.2.20] Ensure shadow group is empty (Scored

FORESIGHT®
CYBER

Foresight Cyber Ltd

Registered & Business address UK
71-75 Shelton Street,
Covent Garden, London, WC2H 9JQ,
United Kingdom

Business address CZ:
Fryštátská 64/9, 733 01 Karvina,
Czech Republic

Contacts:
UK Office: +44 20 8159 8942
General enquiries: info@foresightcyber.com
Finance team: finance@foresightcyber.com
Data protection Office: dpo@foresightcyber.com
Directors: directors@foresightcyber.com

https://foresightcyber.com
@foresightcyber.com

VAT: GB144735213
Company number: 06871193
D-U-N-S number: 211601017