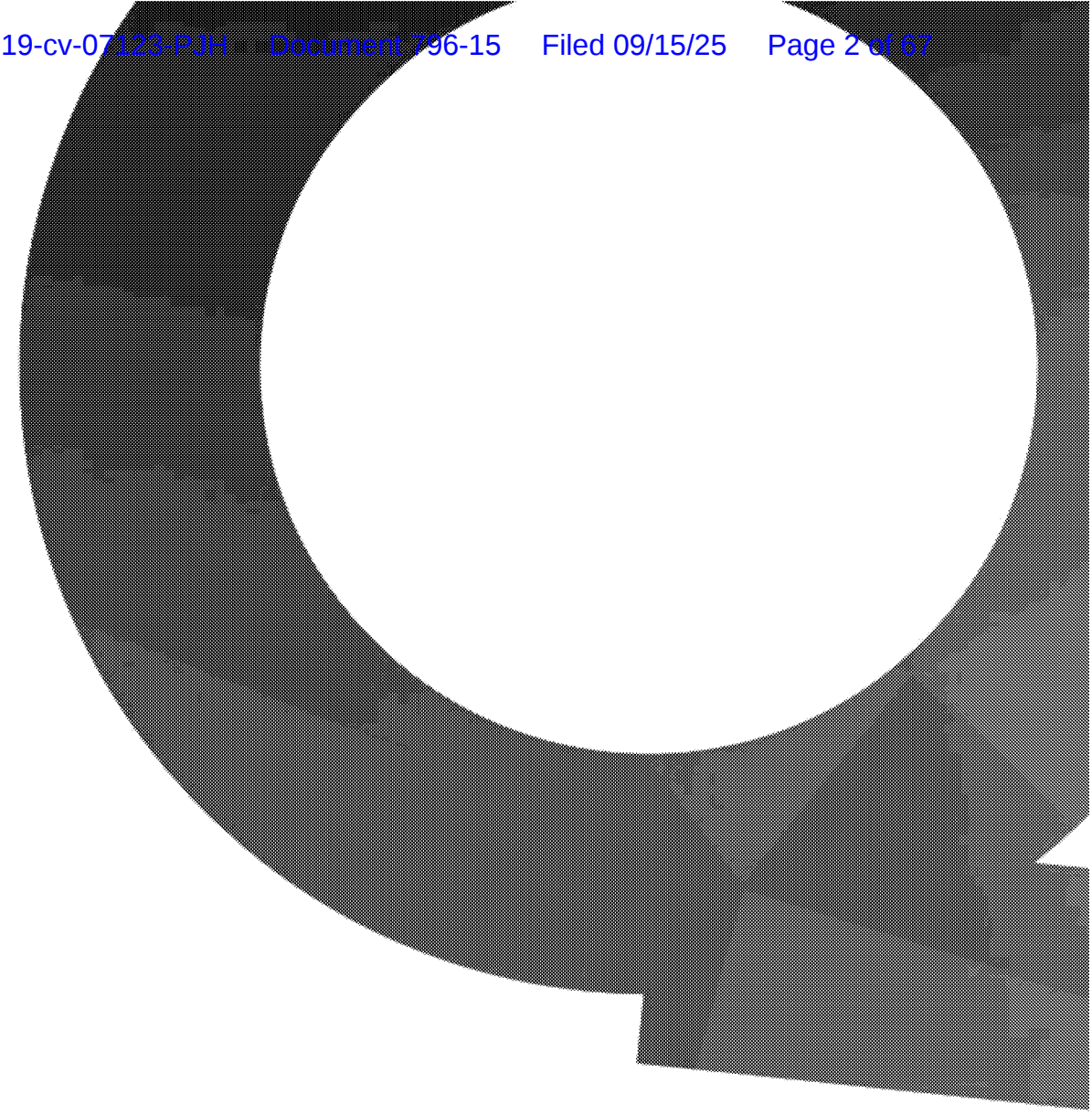
# Exhibit 32

**UNREDACTED VERSION OF DOCUMENT PROPOSED**

**TO BE FILED UNDER SEAL**



# Pegasus

Version 3.0

## Product Description

August 2018

Cyber Technologies

# Copyright and Disclaimer



We make no representation or warranty regarding the accuracy or completeness of this document and reserve the right to alter its contents at any time without notice. Functionality and specifications featured in this document are subject to change without prior notice and vary between configurations.

Please contact us for current product features and specifications. Any supply of the products featured in this document will be subject to the terms and conditions of the relevant contract.

# Confidentiality

This document contains confidential information and may be used solely for the purpose for which they were provided, that being evaluating the possibility of acquiring a license to use one or more of our solutions or, following purchase, receiving product support, training material, and/or user guides. If you have not received our prior written permission to use this document, you should immediately destroy all copies of it and cease using it in any way.

The licensing, use, sale and implementation of all products referenced in this document is subject to customer provision of the following: signed and stamped End-User Certificate and an import and/or export license issued by the relevant authorities.

Cyber Technologies

# TABLE OF CONTENTS

Cyber Technologies

Cyber Technologies

# 1 OVERVIEW

Q Cyber Technologies—a world leader in the field of cyber product development—owns and develops Pegasus, a cutting-edge cyber-intelligence solution.

Pegasus enables law enforcement and intelligence agencies to remotely and covertly monitor, collect, extract, and analyze valuable intelligence resourced from the most widely-sold Android and BlackBerry smartphone devices.

This breakthrough solution, developed by veterans of elite intelligence agencies, enables governments to address the communication-interception challenges found on today's highly-dynamic, cyber battlefields.

Pegasus—using its capabilities to capture new types of information from mobile devices—bridges a substantial technology gap to deliver complete and accurate intelligence that furthers your security operations.

Since 2009, this system has been used by security and intelligence organizations around the globe—a rigorous vetting process ensures that Pegasus is only made available to organizations that fight crime and terror-related activities.

## 1.1 Overcoming Smartphone Data-interception Challenges

The rapidly growing and highly-dynamic mobile communications market—characterized by the introduction of new devices, operating systems (OS), and applications on an almost daily basis—necessitates rethinking traditional intelligence paradigms.

Changes in the communications landscape pose real obstacles that must be overcome by the world's intelligence and law enforcement agencies. Challenges include,

- **Encryption:** Now mainstream, most applications, services, and devices store and transmit data in an encrypted fashion.
- **Abundance of communication applications:** The communications market is bursting with messaging applications, all of which are IP-based and use proprietary protocols and encryption. Messaging applications are central to a target's personal and group communications as they offer easily-available and secured infrastructures.
- **Roaming targets:** Persons-of-interest are constantly moving between countries and networks.
- **Accessing personal and private data:** Targets carry their smartphones—which hold vast amounts of personal data—everywhere with them. Normally such data is not sent over networks; it is only available on an end-user's device and cannot be intercepted in traditional ways.
- **Masking:** Targets with multiple, virtual identities use any number of free services to hide their presence and activities—this approach makes them seemingly impossible to trace and track.
- **SIM replacement:** SIM are frequently replaced to avoid interception attempts.
- **Complex and expensive implementations:** Increasingly complex communications require more network interfaces—setting up interfaces with mobile network operators (MNO) is a lengthy and expensive process requiring regulation and standardization.

Q Cyber Technologies

## 1.2 Limitations of Standard Interception Solutions

Standard and legacy interception systems leave valuable *intel* unavailable to intelligence agencies. Since these systems only deliver partial results, organizations are left with substantial intelligence gaps. Commonly used systems are outlined below.

**Lawful Interception**

Lawful Interception (LI) requires in-depth relationships with local MNO—public-switched telephone network (PSTN), cellular, and Internet—who enable the legal monitoring of text messages and voice calls.

Today, however, most contemporary communications are comprised of IP-based traffic—characterized by encryption and proprietary protocols—which is extremely difficult to monitor using switch-based solutions.

IP-based traffic, even if intercepted, typically carries vast amounts of technical data unrelated to the content and metadata being communicated. Consequently, analysts spend much time going through irrelevant data that, at best, provides only a partial view of a target's communications.

The number of interfaces required to cover relevant MNO both increases costs and widens the circle of persons who might potentially leak sensitive information.

**Tactical Man-in-the-Middle Interception**

Tactical *Man-in-the-Middle* (MITM) interception solutions effectively monitor voice calls and text messages when targets are within range of MITM tactical teams.

Most of the available solutions only work on 2G GSM networks—they downgrade a target's device to a GSM-based network which, in turn, noticeably impacts user experience and functionality. However, since most communications are encrypted, even solutions that cover 3G and 4G networks are only capable of intercepting a small portion of a target's communications.

MITM solutions require that well-trained, tactical field teams be physically near their targets. On the other hand, sending tactical teams within range of a target can pose serious risks to both the team and the entire intelligence operation.

**Malicious Software (Malware)**

Malware is intended to enable access to a target's mobile device; however, it requires target involvement for successful installation.

Targets are increasingly sophisticated and well aware of the sensitivity of their communications —they are unlikely to fall into a malware trap particularly when multiple confirmations and approvals are needed before the malware becomes functional.

Malware is vulnerable to many commercially-available, anti-virus and anti-spyware packages. Further, the limitations of their security wireframe and protection, leads to transparency issues—visible traces are easily detected on a mobile device.

By addressing and resolving smartphone data-interception challenges, Q Cyber Technologies enables users to *draw back the curtain* behind which criminals and terrorists hide.

Cyber Technologies

# 2 CYBER INTELLIGENCE FOR THE MOBILE WORLD

Q Cyber Technologies' Pegasus is a globally-positioned, cyber-intelligence solution—it is unique in its ability to successfully infiltrate the market's most popular smartphones—those with Android and BlackBerry operating systems.

Pegasus deploys an invisible software (SW) component (agent) on a target's device which extracts and securely transmits data for intelligence analysis.

The agent's installation vectors, which feature remote and tactical methodologies, require zero to minimal engagement with targets—one click at most!

The highly-secure installation mechanism and agent are completely transparent—NOT a trace exists on either device or network.

## 2.1 Benefits of Pegasus

Organizations that deploy Pegasus achieve unmatched intelligence collection from targeted mobile devices—the solution overcomes smartphone data-interception challenges, as well as the limitations associated with standard interception methods.

- **Global coverage:** Monitor targets' devices while they connect to the Internet—from any location.
- **Unlimited access to targets' mobile devices:** Remotely and covertly collect information about a target's relationships, locations, phone calls, plans, and activities.
- **Handle encrypted content and devices:** Overcome encryption, SSL, proprietary protocols, and other hurdles introduced by the complex communications world.
- **Bridge intelligence gaps:** Collect new and unique types of information—contacts, files, environmental wiretaps, and passwords—to build complete and accurate intelligence profiles.
- **Uncover virtual identities:** Ongoing device surveillance—regardless of whether or not a target switches between virtual identities and SIM cards.
- **Operate target devices:** Activate the microphone to listen in on a target's environment, turn on the camera to take snapshots, and take screenshots to collect non-communications data of high *intel* value.
- **Intercept calls:** Transparently monitor voice and VoIP calls in near real-time.
- **Monitor mobile applications:** Monitor a multitude of applications including Skype, WhatsApp, Viber, WeChat, Line, Facebook Messenger, Telegram, and Blackberry Messenger (BBM).
- **Pinpoint targets:** Obtain accurate positioning information and track targets using GPS, Cell ID (CID), and Wi-Fi.
- **MNO-independent:** Cooperation with local MNO is not required.
- **Reduce risks:** Eliminates any need for physical proximity to a target or their device during an operation.

Cyber Technologies

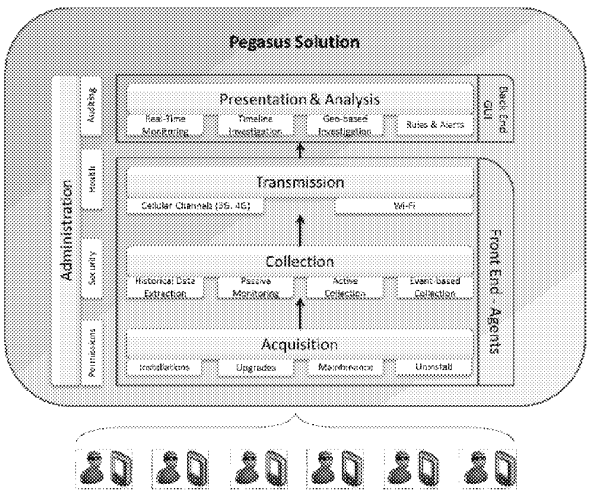
## 2.2 Technology Highlights

The Pegasus solution uses cutting-edge technology—developed by experts coming from intelligence and LI agencies—to offer a rich set of advanced features and sophisticated intelligence-gathering capabilities that are unavailable in standard interception solutions.

- Penetrates Android [redacted] and BlackBerry-based mobile phones—whether or not password-protected
- Endures reboot and factory resets; OS upgrades are quickly handled
- Installs an agent with zero- to 1-click—minimal to no target engagement
- Unaffected by SIM card replacement
- Monitors smartphone applications
- Extracts encrypted content from the majority of popular instant-messaging (IM) applications and secured chats
- Remotely activates and controls phone functionalities—camera, microphone, GPS etc.
- Retrieves for detailed analysis:
  - passwords
  - files
  - messages
  - emails
  - processes list
  - locations
  - contacts
  - photos
  - calendar records
  - and more
- Target remains unaware—Pegasus is completely transparent
- Leaves no trace whatsoever on a target's mobile device
- User can choose to set an automatic self-destruct mechanism
- Minimal battery, memory, and data consumption

## 2.3 High-level Architecture

The Pegasus system features several mechanisms which, together, deliver a comprehensive cyber-intelligence collection and analysis solution. System layers and components are shown below.




## 2.4 System Modules

Pegasus' central functionalities are detailed below.

Cyber Technologies

| | |
|---|---|
| **Acquire** | This module is used for new agent installations, the upgrade and maintenance of installed agents, and the uninstallation of existing agents. |
| **Investigate** | As the main user interface, this layer presents collected data to operators and analysts who turn it actionable intelligence. The modules include,<br>• **Real-time monitoring:** The collected data of one or more targets is presented in near real-time—this is critical to decision making when dealing with sensitive targets or during operational activities.<br>• **Investigation:** Applies deep-analysis procedures to help analysts thoroughly investigate data, while investigation tools reveal crucial hidden connections and analyze events.<br>• **Rules and Alerts (Road Map feature):** Rules are defined—based on specific incoming data or occurring events—that, when met, trigger system alerts. |
| **Cases** | Presents all active cases and their target content. |
| **Commands** | Comprehensive intelligence gathering using these extraction methods:<br>• **Active collection:** Directs the agent to perform functions such as camera and microphone operation, screenshots, and/or retrieve files<br>• **Passive monitoring:** Monitors new data that a device syncs with, receives, and/or sends<br>• **Trigger-based collection (Road Map feature):** Defines scenarios that automatically trigger the activation and collection of specific types of data<br>• **Historical data extraction:** Extracts all data existing on a target's device |
| **Transmit** | Using the securest and most efficient pathways, collected data is transmitted back to the Command and Control (C&C) servers via cellular or Wi-Fi channels. |
| **Administration** | This layer manages all system administration tasks.<br>• **Permissions:** System administrators set up and manage users, define roles, and set permissions to data and modules. Based on this, user groups are defined on the basis of access levels as they relate to targets and cases.<br>• **Security:** Monitors system security to ensure collected and transmitted data is clean, authenticated, and secure before it enters the system.<br>• **Health:** Monitors the status of all hardware (HW) and software (SW) components to ensure healthy functioning—includes communication between system elements, system performance, storage availability, and fault-related alerts.<br>• **Auditing:** Tracks all user activities and operations in the system—from log in to log out. The integrity of all audited data is maintained—it cannot be deleted or changed in any way. |

Cyber Technologies

# 3 TARGET ACQUISITION

A target's smartphone, and the cloud accounts connected to it, offer a deep well of intelligence. Redacted – Export Controlled agent and [redacted] data extraction offer unlimited quantities of target-related data.

## 3.1 Agent Endpoint

Data collection begins following installation of a software-based component (agent) on your target's mobile device.

System users configure the type of data to be collected by the agent; it can be installed on smartphones that use today's most popular operating systems—Android Redacted –Export Controlled and BlackBerry.

Every agent is independently configured to collect and transmit specific types of information; this is achieved using a reliable Internet connection. The hidden, compressed, and encrypted data is transmitted to Pegasus servers along select channels at pre-defined times.

Once an agent is installed, a target's activities will no longer be hidden behind encryption protocols, the parallel use of multiple applications, and/or other communication-concealing methodologies.

## 3.2

**Redacted – Export Controlled**

### Data Collection

Data is securely extracted from clouds—there is no impact, whatsoever, on the behavior of device applications and user accounts.

Data stored on mobile devices merely hints at the mass of available historical information—dating back months and even years—that can be retrieved. Cloud brings in a continual flow of information that can last months at a time.

Newly generated information is securely transmitted to the Pegasus system.

- Instant messaging
- Location history
- Account backups
- Email
- Browsing history
- File-sharing storage

Cyber Technologies

# 4 AGENT INSTALLATION VECTORS

Installing an agent on a target's device is the heart of any intelligence operation using Pegasus—each installation is carefully planned to ensure success.

The Pegasus system supports installation methods and vectors that are designed, as shown by high installation success rates, to satisfy varying operational scenarios. In the following sections, remote and Redacted – Export Controlled Pegasus Redacted – Export Controlled are described.

## Installation Vector Comparison Table

| Vector | Global | Home Country | Uses | No MNO | Field Team |
|---|---|---|---|---|---|
| Remote | ✓ | ✓ | Triggered / Covert | ✓ | × |
| Redacted – Export Controlled | | | | | |
| Physical | × | ✓ | Physical access to device | ✓ | ✓ |

## 4.1 Remote Installation (Unlimited range)

Remote installations include both covert and social-engineering methodologies. The Pegasus solution offers many tools for composing tailored, yet innocent-looking messages—this is crucial as content credibility greatly affects whether or not a target will click a link.

Using the below methods, only a target's phone number (MSISDN) is required for a successful installation.

### Covert

1. A covert message is sent to a mobile device; the target is not engaged—there is no need to click a link or open a message.
2. The message causes the smartphone to download and install the agent—the device shows no signs of change or interference.
3. The installation is completely invisible.

The Pegasus system's unique, remote installation capability gives our solution a vast advantage over other offerings found in the market.

- Covert installation process is invisible to the target and doesn't require their engagement.
- System is MNO independent.
- Activation is handled from a command and control center.
- Solution has an unlimited range and works using any MNO. Thus, the Pegasus agent can be installed on any supported device, anywhere in the world.

### Triggered (Social Engineering)

System operators can choose a different approach and craft an SMS, instant message (IM), or email. This approach prompts a target to click on a message link.

- One click, whether active or unintentional, leads to an agent installation.
- The process is completely covert and there is absolutely no sign that software is being installed on their smartphone.

## 4.2 Redacted – Export Controlled Field Redacted – Export Controlled (Within range)

Field Redacted – Export Controlled include a Redacted – Export Controlled or even physical access to a mobile device.

Cyber Technologies

## Tactical Network Element (PiXcell)

- Pegasus agent is covertly deployed once a mobile device is acquired by and connected to a tactical network solution (PiXcell)—whether it be native 3G/4G or Wi-Fi MITM.
- Pegasus solution leverages the capabilities of PiXcell to perform a covert agent installation while a target browses; there is no target engagement.
- Once installed, data is extracted and transmitted remotely—in the same manner and with the same capabilities of a remote installation.

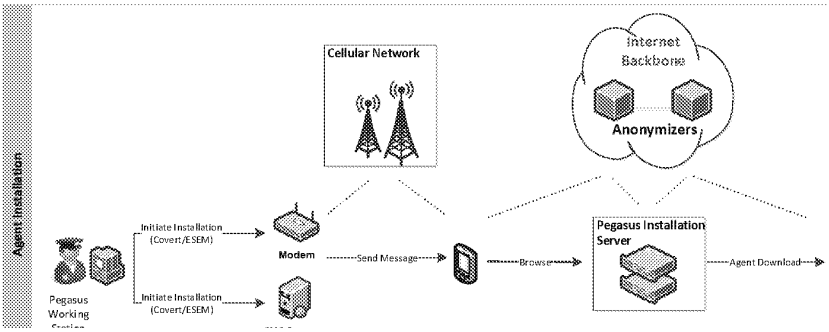
## Physical

- If a team has physical access to a device, then the Pegasus agent can be installed within a few minutes.
- Once installed, data is extracted and transmitted remotely—in the same manner and with the same capabilities of a remote installation.

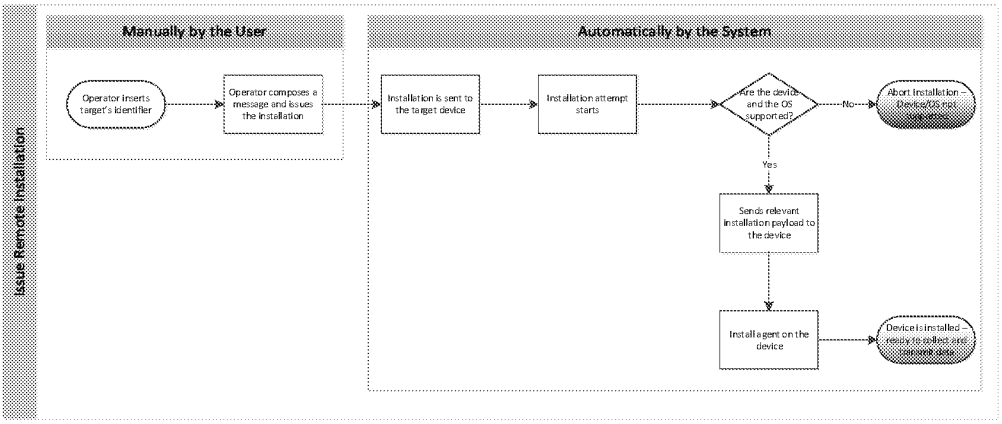
Cyber Technologies

# 5 AGENT INSTALLATION FLOW

The remote installation of a Pegasus agent is outlined below.




To initiate an agent installation, the system operator only needs a target's MSISDN—the rest of the installation process is performed automatically by the system; see the below image.




## 5.1 Device Behavior after Installation

Introduction of an agent leaves a target's mobile device totally unaffected—there is no change in the phone's behavior. The agent is designed to be lightweight, yet extremely efficient; it compresses, stores, then transmits collected data in the most efficient and economical way. This ensures that device resources, such as its battery and data plan, are wisely utilized.

## 5.2 Installation Failure

If a system operator initiates a remote installation to an unsupported device, OS, or browser, then the installation will be aborted. However, the target's browsing experience remains unaffected—the target's device will present the URL defined by the system operator.

**Note:** The system and system operator don't need advance knowledge of the device, OS, and/or browser type; this information is automatically identified during the installation process.

Cyber Technologies

# 6 DATA COLLECTION

Following the target acquisition stage, during which the agent is installed and the [redacted] Eye [redacted], the Pegasus system begins to monitor and collect a wide range of data from a target's mobile device.

The types of information include the following:

- **Text:** Textual information, which is usually structured and small in size, is easier to transmit and analyze; it includes text messages (SMS), emails, calendar records, call log history, instant messaging, contact list, and browsing history.
- **Audio:** Includes call recording (GSM & VoIP), environmental taps (microphone activation and recording), and other audio-recorded files.
- **Visual:** Includes photo and video retrieval, and new camera and screen shots.
- **Files:** Every mobile device contains hundreds of files such as databases, documents, and videos—some may contain vital intelligence.
- **Location:** Includes ongoing monitoring of a device's location (GPS and CID).

Data is collected by means of historical data extraction, passive monitoring, and active collection.

## 6.1 Historical Data Extraction

The types of historical data that can be extracted from a target's device, and sent to the C&C server, include the following:

- SMS records
- Contact details
- Call history (call log)
- Calendar records
- Emails
- Instant messaging
- Browsing history
- Installed applications
- Wi-Fi networks

Pegasus enables the extraction of all data from a device—existing *intel* and real-time additions. Other market offerings are limited to data generated after the installation and partial monitoring.

Intelligence agencies greatly benefit from their ability to access historical data as it helps build a comprehensive and accurate intelligence picture of a target/s and their associates. Normally organizations devote months to collecting such information, with Pegasus this is achieved in minutes.

**Note:** Historical data extraction is a valuable option. If, however, an organization is not permitted to access and extract historical data, then this option can be disabled. The agent will only monitor newly-arrived data.


## 6.2 Passive Monitoring

The agent, once installed, continuously monitors a device and retrieves—in near real time—all new data that becomes available. Data that is passively monitored includes the following:

- SMS records
- Contact details
- Call history (call log)
- Audio call recordings (GSM & VoIP)
- Calendar records
- Emails
- Instant messaging
- Target location (CID, network-based)
- Activity location; e.g., site from which a phone call originated
- Device location—monitoring a target's movements

## 6.3 Active Collection

In addition to passive monitoring, a wide range of active collection features are available. Active requests (actions) collect specified data based on orders issued by a system operator and/or system triggers.

Active collection allows near real-time actions to take place on a target's device—unique information is retrieved from both it and the surrounding area:

- Location (GPS and Wi-Fi-based)
- File retrieval
- Environmental tap (device microphone)
- Snapshots (front & back cameras)
- Screenshots

Pegasus' active collection capability sets it far above all other intelligence-collection solutions.

- System operators control information collection; they actively retrieve crucial data from a target's device. There is no passive waiting for *hopefully* relevant data to arrive.
- Your organization can access personal information never intended to leave a target's phone, or catch moments never meant to be captured.
- Pegasus accurately tracks a targets, takes photos, and/or records face-to-face meetings without the need for tactical teams.

### Manual Actions

Active data collection is initiated by a system operator. Actions are normally issued on the basis of pre-existing target information and the need to seek specific, related intelligence.

Example:

1. Target's calendar record shows s/he is currently in a face-to-face meeting.
2. Collected location data verifies this information.
3. System operator initiates an action that activates the microphone and camera on the target's mobile device.

Further, a system operator can actively retrieve any file found on a target's device—it can be an email attachment, video sent via a messaging application, or a document synced to the device from a cloud-storage service.


## 6.4 Time Limitation and Selective Collection

Pegasus' capabilities enable the collection of historical, passive, and active data. A partial data collection can be performed in order to optimize resources, comply with a country's legal wireframe, or comply with a warrant issued for a target.

The following example shows how the agent collects and operates within time and data constraints.

- Data collection is only permitted during a time frame set by a warrant.
- Upon reaching the uninstall date, the agent stops sending data and removes itself from the target's device.
- If warrant conditions change, then the agent life cycle can be reconfigured.

## 6.5 Collection Buffer

The installed agent monitors device data and transmits it to the C&C servers.

Data transmission, on occasion, may not be possible for a number of reasons: no available data channels, device is roaming, or the agent is dormant. In such instances, the agent continues to collect new information; it is stored until a connection become available, and then transmitted.

Collected data is stored in a hidden, encrypted buffer; it is preset to hold no more than 5% of a device's free space.

Example:

Buffer can store up to 50 MB on a monitored device with 1 GB of free space.

If the buffer limit is reached, the oldest data is deleted and replaced with new data.

Transmitted data is immediately deleted from the buffer.

## 6.6 Description of Collected Data

The agent collects available data from supported applications found on the device—these include globally-popular applications.

Our developers understand that less popular and/or new applications can quickly come to the forefront of use—when requirements are raised, our company can choose to prioritize the development of new capabilities.

The types of data available for historical extraction, passive monitoring, and active collection are set out in the below table; they all have the potential to be collected by an agent.

Cyber Technologies

| Category | Collected Data | Agent Description | Historical Extraction | Passive Monitoring | Active Collection |
|---|---|---|---|---|---|
| | SMS | • Extracts history<br>• Monitors all incoming & outgoing text messages (SMS) | ✓ | ✓ | N/A |
| | | **Redacted –Export Controlled** | | | |
| **Communications** | Instant messages | • Extracts history<br>• Monitors incoming & outgoing messages sent to/from a device via a multitude of applications<br>• Covers leading IM services: WhatsApp, Telegram, Facebook Messenger, Signal, Viber and more<br>• Collects textual messages (including group chats)<br>• Indicates files transfers (which are retrievable) | ✓ | ✓ | Retrieval request: transferred files |
| | Emails | • Extracts history<br>• Monitors all emails from Gmail application and native email application | ✓ | ✓ | Retrieval request: email attachments |
| | Call log | • Extracts history<br>• Monitors all incoming & outgoing calls made to/from a device<br>• Collects Cellular phone call logs<br>• Collects call logs from applications such as WhatsApp, Telegram, and more | ✓ | ✓ | N/A |
| | Call recording | • Records incoming & outgoing calls to/from a device<br>• Records regular Cellular calls<br>• Records VoIP calls made from various applications such as WhatsApp, Telegram and more | N/A | ✓ | N/A |

Cyber Technologies

| Category | Collected Data | Agent Description | Historical Extraction | Passive Monitoring | Active Collection |
|---|---|---|---|---|---|
| **Personal** | Contact details | • Extracts history<br>• Monitors all contacts on a device including assigned photos<br>• Includes contacts synced to the contact list from external services; e.g., Gmail, Facebook | ✓ | ✓ | N/A |
| | Calendar | • Extracts history<br>• Monitors calendar events on a device, including those synced from multiple external accounts; e.g., MS Exchange, Gmail, and more | ✓ | ✓ | N/A |
| | Browsing history | • Extracts history<br>• Monitors websites browsed via Chrome [Redacted -Export Controlled] | ✓ | ✓ | N/A |
| | Installed applications | • Extracts a list of installed applications<br>• Monitors newly installed applications<br>• Monitors applications updates and deletions | ✓ | ✓ | N/A |
| | Device & network information | • Monitors the following:<br>– Device and network details<br>– IMSI, IMEI, Wi-Fi networks, SSID, MNC, MCC<br>– Battery level and more | N/A | ✓ | N/A |
| | File retrieval | • Retrieve any file—whether on a target device's internal memory or SD card<br>• In addition, with the cloud solution, the user can retrieve files from cloud-based services such as Google Drive. (see Pegasus 3 Product Description section 3.2) | Retrieval request: historical files | × | ✓ |

Cyber Technologies

| Category | Collected Data | Agent Description | Historical Extraction | Passive Monitoring | Active Collection |
|---|---|---|---|---|---|
| **Location** | Location | • Monitors a target's location<br>• Monitors sites where each activity was sent/received<br>• Passive location monitoring is based on CID<br>• Active collection is based on GPS | N/A | ✓ | ✓ |
| **Actions** | Camera snapshot | • Front and back cameras take photos<br>– No indication appears on the device<br>– Flash is never used<br>– Images do not appear in the device gallery<br>– **Note:** Images may be out of focus since the flash isn't used and the device may be in motion<br>• Photos are sent to the C&C servers<br>• Operator chooses the degree of image quality; size can be reduced to ensure faster transmission | N/A | × | ✓ |
| | Screenshot capture | • Screen capture is taken<br>• Image is sent to the C&C servers | N/A | × | ✓ |
| | Room tap<br>(mic recording) | • Microphone is activated to record surrounding sounds<br>– No indication that a recording is in process<br>– Recordings are not stored on the device<br>– **Note:** Recording quality is affected by the device model, surrounding noise, and microphone sensitivity; the latter varies between phone models and is set by the device vendor<br>• Data is sent to the C&C for playback and analysis | N/A | × | ✓ |

Cyber Technologies

# 7 SECURE TRANSMISSION

Collected data—historical data extraction, passive monitoring, and active collection—are, by default, sent in near real time to the C&C servers. The preferred transmission channel is Wi-Fi but, if unavailable, cellular data channels such as GPRS, 3G, and LTE are used.

The agent, which uses several compression and encryption methodologies, can exclude irrelevant, non-textual content from documents before transmitting them.

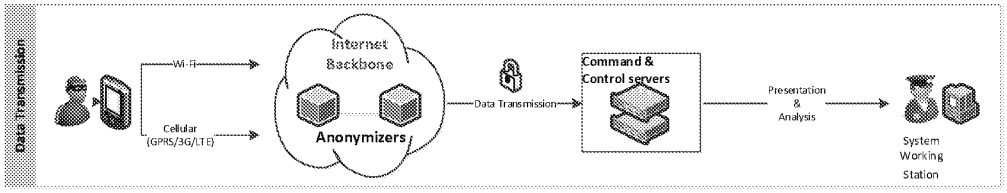
Due to Pegasus' tremendous capabilities, and the remarkable efforts invested in its design, the data usage is tiny—normally only a few hundred bytes. This guarantees that collected data is easily transmitted, and has minimal impact on a target's device and data plan.

Section *6.5 Collection Buffer* notes that if data channels are unavailable, then the agent continues to collect new information, stores it in a dedicated buffer and, when connectivity returns, transmits the data. Factors that can affect data transmission are noted below.

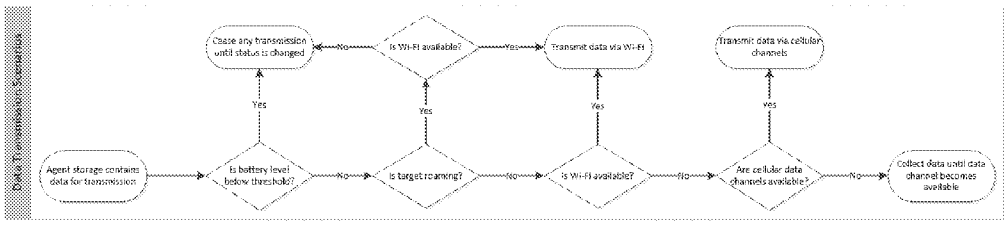
- **Low battery:** If a device's battery has only 5% remaining power, then all data transmission processes are stopped until the device is recharged.
- **Roaming device:**
  - Cellular data channels used by roaming devices are expensive; therefore, by default, data transmission is handled via Wi-Fi.
  - If Wi-Fi is unavailable, then transmission stops.
  - System operators can, however, choose to transmit data over cellular channels—though this can lead to high data-plan charges.
- **Dormant agent:**
  - The agent is set to dormant under the following circumstances:
    - Target enters a country whose expensive roaming charges could draw attention
    - Target enters a country with high with exposure risk.
    - There may be legal and/or contractual limitations on use in given countries
  - The agent continues to passively collect and then store data. Upon departure from the country-of-risk, collected data is transmitted to the C&C servers.

Communication between the agent and the central servers is indirect—it is handled via an anonymizing network—thus trace-back is infeasible.

The below image shows the Pegasus system's data transmission process.




Channels and scenarios for transmitting collected data are set out below.




## 7.1 Data-transmission Security

The connection between agent and servers is encrypted with strong algorithms and also mutually authenticated; transmitted data is encrypted with a unique and asymmetric encryption.

The encryption of data and transmissions is pivotal, but attention must be given to data, battery, and memory use—the target must be kept unaware.

It is inconceivable that a target would discover an active agent. The agent, installed deep in the device, is well beyond OS privilege controls and is untraceable by antivirus and anti-spy software.

## 7.2 Data Hashing

The authenticity of collected data is guaranteed; it is sent in encrypted form and is digitally signed to prevent tampering. Data is timestamped as follows:

- At creation
- Upon arrival at the C&C servers

## 7.3 Anonymizing Transmission Network

Agent invisibility and source security are the guiding principles of the Pegasus solution. An Anonymizing Transmission Network (ATN)—a network of anonymizers—is deployed at every client's site to ensure that it is impossible to trace back to an operating organization thus ensuring full deniability.

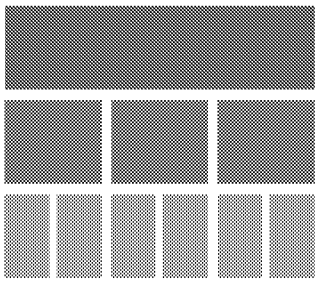
ATN nodes are spread worldwide and enable agent connections to be redirected along separate paths before reaching the C&C servers. This ensures that the identity of the communicating parties is obscured.

**Note:** Our 24/7 Support Center monitors security alerts arriving from all client systems; however, while the Support Center can see security alerts, they cannot view any collected target or operational-related data. Should there be a security incident, the client must immediately follow Support Center guidance and directions.

Cyber Technologies

# 8 MONITORING AND INVESTIGATION

Collecting intelligence on hundreds of targets and devices generates vast amounts of data that require visualization, presentation, and investigation.



Collected data is displayed in an easy-to-use, intuitive user interface (UI).

- Collected data is organized per case
- Each case consists of related targets
- Target profiles show installed agents; e.g., devices with Pegasus agents

The Pegasus system includes a set of operational and collaborative tools that help organizations transform data into actionable intelligence. Tool functionalities include the following:

| | |
|---|---|
| **Timeline investigation** | Review and analyze activities in chronological order to best understand the flow of events. |
| **Geographical investigation** | Review target and case activities on a map:<br>• View their historical locations<br>• Investigate their routine<br>• Simultaneously view and compare multiple target trails |
| **Data enrichment** | Enrich collected data with user input to help retrieve, filter, and analyze data:<br>• Add comments and tags<br>• Write summaries and conclusions<br>• Add translations |
| **Entity management** | Manage targets that are tagged per case, location, and/or subjects. For example,<br>• Operation [name]<br>• Country [name]<br>• Drugs<br>• Terror<br>• Serious crimes |
| **Advanced search and filters** | Search and filter to prove or strengthen a theory, or investigate events.<br>User categories such as case, target, topic, types of data (location, calendar records, email), terms, names, numbers, code words, dates and times, etc. |
| **Notification and action rules** | *Roadmap* feature that will define rules to,<br>• Generate notifications<br>• Issue actions |


## 8.1 Data Export

This section holds information on features, tools, and other systems used to export data from the Pegasus system.

**Third-party Systems**

Pegasus is an end-to-end system that provides its users with collection, presentation, and advanced investigation tools. Additionally, the system can export html files that may be integrated with compatible, third-party analysis systems.

**Export Authenticity**

Collected data maintains its integrity—it cannot be changed or altered by system users. Users can, however, add explanations and additional information by means of descriptions, tags, and comments. This leaves the data unchanged, but it does add a useful reference layer.

All exported data is 'sealed data'—including hashes—and is admissible in court.

**Report Generation**

Generated reports can be securely transferred to organization stakeholders. The system generates reports based on data filtered according to parameters:

- Timeframe
- Cases and targets
- Types and categories of collected data
- Tags
- Comments
- Free text
- Location

# 9 AGENT MAINTENANCE

Installed agents require maintenance in order to support new features, bugs fixes, and changes to settings and configurations.

Agents can be uninstalled when a target is no longer a focus-of-interest for an organization.

## 9.1 Agent Upgrade

New agent versions are regularly released—for first time installation or as an upgrade to an existing agent. Latest versions provide new functionalities, bug fixes, support for new services, and/or improvements to the agent's overall behavior.

The time required for an upgrade is short and the process simple—there is no target engagement and the target's device is completely unaffected.

- A system operator requests the upgrade and, once initiated, it is completed within minutes.
- If the target's device is turned off or has a poor data connection then the upgrade is delayed until the device is reactivated and/or the data connection improves.

Updates are crucial—they keep the agent functioning and operational, and improve and repair security issues that can arise due to the ever-changing smartphone and communication environments.

## 9.2 Agent Settings

Agent settings are initially defined during installation:

- Data to be collected
- Preferred channels of communication with the C&C server
- Frequency with which the agent communicates with the server

**Agent Uninstall**

When an intelligence operation is completed, or a target is no longer of interest, then the agent can be uninstalled; this process is quick and has zero-to-minimal effect[1] on a target's device.

If an agent is operational on a device and communicates with the C&C servers, then—regardless of the initial installation vector—it is simply and **remotely** uninstalled. Under certain circumstances, a physical uninstall is also possible.

1. System operator issues a request for agent uninstallation.
2. Uninstall command is sent to the device.
3. No trace whatsoever will ever be found on a device.

Uninstalling an agent doesn't affect any data collected to date. Prior to the removal process, all collected data is transmitted to the C&C servers where it awaits investigation and analysis.

[1] In some cases, uninstall may lead to device reboot; however, this will only occur after agent removal is completed.

Cyber Technologies

# 10 OPERATIONAL SECURITY

Q Cyber Technologies devotes extensive resources towards keeping our clients and products secure and, equally important, invisible to targets. The Pegasus architecture ensures no client trace-back or agent detection.

## 10.1 Self-destruct Mechanism

The Pegasus agent carries an automatic self-destruct mechanism that the system operator can choose to activate due to specific operational considerations.

If there is a chance of agent exposure then the self-destruct mechanism is automatically activated; then, when the risk has been removed, the agent can be re-installed. The agent has sensors that help detect security risks such as those noted below:

- **Anti-debugging—**agent continuously monitors debugging activities; e.g., device rooting, connections to forensic tools, and/or connection to an emulator.
- **Agent manipulation—**agent endlessly monitors its own code and performs checks for changes and/or abnormalities.
- **Device mirroring—**agent ceaselessly monitors the environment on which it is running and will immediately detect device duplication or changes.
- **Unresponsive agent:** If an agent is unresponsive or doesn't communicate with the servers for a set period of time[2], then the agent automatically performs uninstall to avoid remaining on an unused or unsupervised device.

## 10.2 Security Alerts Monitoring

Our Network Operations Center (NOC) monitors Pegasus security logs 24/7—if there is any suspicious activity or an alert, an immediate investigation begins.

- Support Center updates the client and shares known information.
- Nagios, the security monitoring system, is transparent and also available on client premises.
- NOC follows a protocol:
  - Verify which type of security alert was triggered.
  - Actions to be taken by the support team and client.

[2] Default period is 21 days but can be reconfigured for a shorter period of time.


# 11 AUDITING

Pegasus is a mission-critical system that supports covert, operational intelligence activities. System operators and analysts are well trained and understand the system's capabilities—especially the collection of highly-sensitive and critical data.

- System's auditing mechanism enables:
  - Compliance, where relevant, with country-specific regulations
  - Access to auditing tools that access correct system usage—from log in to log out
- Audited data is only available to persons who are designated as auditors by the system administrator.
  - They can review data and filter it according to date, user, or user action
  - Example: Review all actions performed by a given user on a specific date
- A user can only connect to one Pegasus workstation at a time.
  - Supports reliable and accurate auditing
  - Example: If a user connects to another workstation, then the initial connection automatically ends
- Audited information is stored in a protected database.
  - Data cannot be deleted or altered by any level of system user
  - This safeguards data integrity and viability
  - If required, audited information can be exported

# 12 ROLES, PERMISSIONS, AND ENTITIES

Pegasus is an intelligence system that collects, generates, and stores large volumes of critical data.

Q Cyber Technologies understands that gathered data can relate to high-profile and/or sensitive targets and, as such, our company provides a mechanism for managing the compartmentalization of data according to user permissions.

The system's highly-flexible permissions architecture makes organizational changes extremely easy to update. Users are allocated roles, tasks, and related permission levels. On the basis of these parameters, users can access permitted data and use specific sets of tools—all of which assist them in meeting both mission and organizational objectives.

## 12.1 Roles

Roles are characterized by predefined sets of activities, tools, modules, and permissions. New and existing users smoothly transition into and within the Pegasus system. Roles include,

| | |
|---|---|
| **Administrator** | • Creates and manages system users, their roles, and assigned permissions<br>• Gives users access to system modules, and the ability to conduct operations and view data |
| **Supervisor** | • Manages acquirer, analyst, and operator roles<br>• Views all operations performed by subordinates<br>• Approves and conducts critical operations; e.g., agent uninstall & data deletion |
| **Acquirer** | Dedicated user who deals with the entire life cycle of an agent on a target's device—installation and maintenance to uninstallation |
| **Analyst** | • Runs investigations and can only read, query, and analyze collected data<br>• Analysts add comments, tags, and descriptions to the data to aid in interpretation |
| **Operator** | • Conducts installations, deploys new agents, and changes existing settings<br>• Views data and issues active data collection requests |
| **Auditor** | • Dedicated user with only auditing-section permissions<br>• Can audit system usage and all user operations—from log in to log out |

**Authentication and Authorization**

The security and integrity of your Pegasus system is ensured.

- System access requires authentication—the log-in process demands the use of both a username and password.
- These identifiers are stored and transmitted in an encrypted manner.

Following successful authentication, users can then access data permitted to them based on their role and associated teams and cases.

## 12.2 Module Permissions

**User permissions** are based on their **role**, as well as to the **team** and **cases** to which they are assigned.

Cyber Technologies

| | Agent Life Cycle | Monitor & Investigate | Data Enrichment | Archive, Delete, Uninstall | System Admin | Audit |
|---|---|---|---|---|---|---|
| Acquirer | ✓ | | | | | |
| Analyst | | ✓ | ✓ | | | |
| Operator | ✓ | ✓ | ✓ | | | |
| Supervisor | ✓ | ✓ | ✓ | ✓ | | |
| Auditor | | | | | | ✓ |
| Administrator | | | | | ✓ | |

## 12.3 Entity Relations

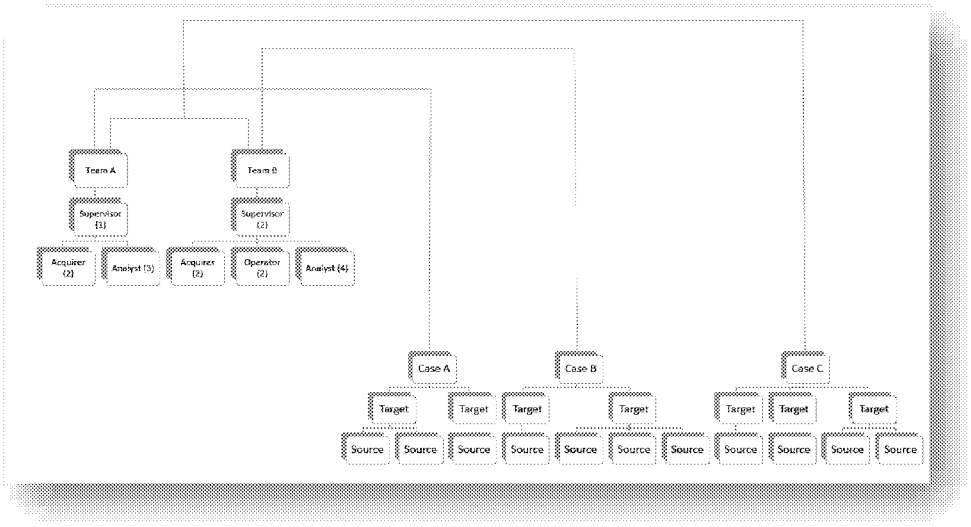
Pegasus organizes collected data according to mission cases—each case holds at least one target or person of interest.

A target may possess one or more devices. Your organization can collect data from all of them by installing an agent on each of a target's devices.

The system is designed to support compartmentalization. Access to case data is based on the roles held by the various team members—supervisor, operator, analyst, and acquirer.

The below diagram sets out the following situations:

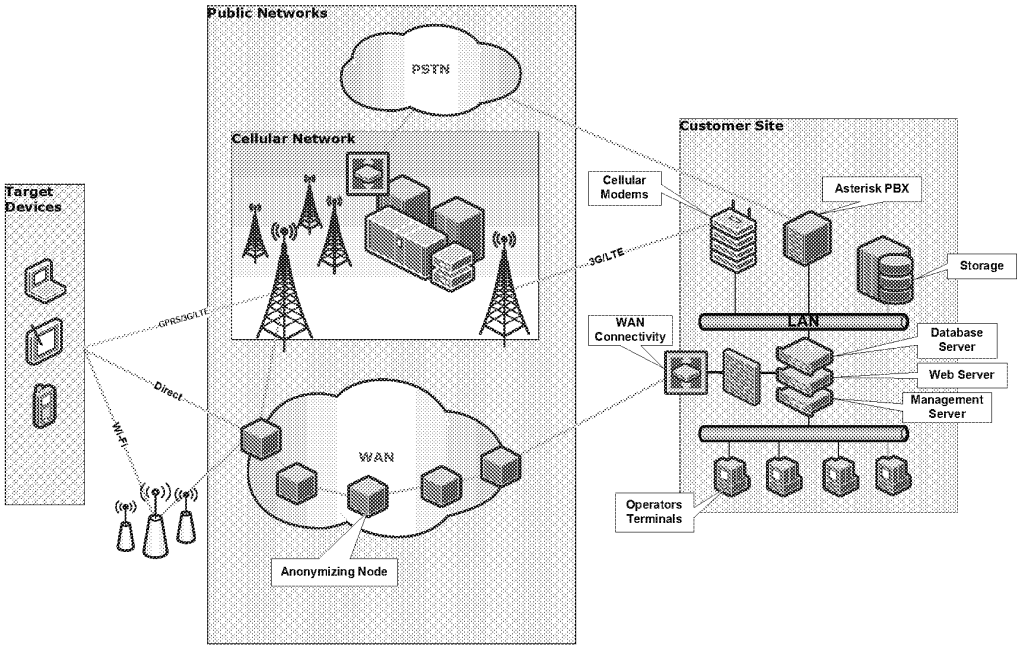
- Team A investigates Case A.
- Team B investigates Case B.
- Both Teams A and B investigate Case C.



Cyber Technologies

# 13 SOLUTION ARCHITECTURE

The Pegasus system's major architectural components are shown in the below image.




## 13.1 Client Site

Q Cyber Technologies is responsible for the deployment and configuration of Pegasus hardware and software at your site—we ensure that all is functioning correctly.

The below table outlines the main components that will be installed at your site.

| System Component | Description |
|---|---|
| **Web server** | Responsible for,<br>• Agent installation and monitoring<br>• Agent maintenance: remote control, configure, and upgrade installed agents<br>• Data transmission: receive collected data transmitted from installed agents |
| **Communications module** | • Responsible for interconnectivity<br>• Handles Internet connection to the servers |
| **Permissions-management module** | • Defines and controls features and content<br>• User access is permitted based on predefined criteria |
| **Data storage** | • Agent-collected data is stored on an external storage device<br>• Data backup has full resiliency and redundancy to prevent failures and downtime |

| System Component | Description |
|---|---|
| **Server security** | • All servers reside inside the client's trusted network<br>• Client deploys security measures<br>• Q Cyber Technologies also puts system-related security measures in place |
| **Hardware** | • System's standard hardware is housed in racks and installed on multiple, connected servers<br>• Responsible for advanced load balancing, content compression, connection management, encryption, advanced routing, and highly-configurable, server health monitoring |
| **Operator terminals (PC)** | • Main tool used by operators<br>• Used to activate the Pegasus system, initiate installations and commands, run investigations, and manage collected data |
| **Pegasus application** | • User interface that is installed on an operator's terminal<br>• Provides a range of tools—view, sort, filter, manage, and alerts—which are used to handle and analyze the volume of collected data |

## 13.2 Public Networks

The Pegasus system only requires hardware and software installations at your premises—there is no physical interface with local MNO.

However, since agent installations and data are transferred over public networks, Q Cyber Technologies ensures that the data is transferred efficiently and securely to your servers.

**Anonymizing Network**

The ATN is built from anonymized connectivity nodes spread over worldwide locations; they enable agent connections to be directed along varying paths before reaching the Pegasus servers. Anonymized nodes serve only a single client who can choose to manage their setup.

See Section 7.3 Anonymizing Transmission Network for more information.

## 13.3 Target Devices

Pegasus' architecture allows operators to issue new installations, and monitor, actively collect, and extract data from targets' devices.

**Note:** Pegasus is a mission-critical, intelligence system that maintains full redundancy in order to avoid malfunctions and failures. The system, which handles data and traffic on a 24/7 basis, is scalable to support client growth and future requirements.

Cyber Technologies

# 14 SYSTEM SETUP AND TRAINING

Q Cyber Technologies sets up the Pegasus system and trains your users before handing the system over to you.

## 14.1 System Setup

Pegasus is a turnkey solution whose system setup includes the following:

- Operating-environment
  - Client is provided with prerequisites that must be prepared
- Deployment:
  - Normally requires 15 work weeks
  - Q Cyber Technologies' personnel deploy Pegasus at the client's site
  - Setup includes hardware and software installations
  - Meeting end-user agreement particulars (e.g., adaptations) as well as client regulatory and technical environments

## 14.2 System Training

Once Pegasus is installed, Q Cyber Technologies personnel conduct a series of training sessions—these can take place at your site, another location, or at Q Cyber Technologies' headquarters.

The number of trainees in a session is in direct proportion to the number of operator stations.

Training content includes the following:

- Basic and advanced system usage
- Operational case management
- Web intelligence and social engineering
- System security
- Operational simulation exercises
- One-on-one, hands-on exercises

## 14.3 High-level Deployment Plan

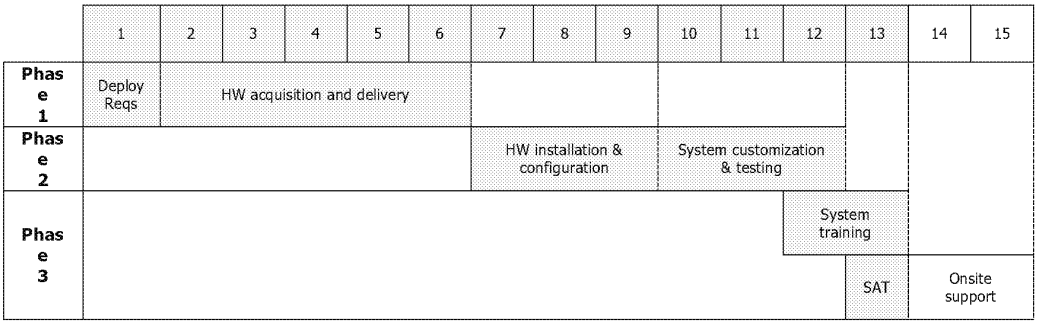
The deployment process—at your site—involves three phases:

- Phase 1 (P1): Preparations
- Phase 2 (P2): Implementation
- Phase 3 (P3): Training and Commissioning

| | | |
|---|---|---|
| **P1** | Preparations | • Analyze system deployment requirements together with the client<br>• HW and SW acquisition, delivery, and arrival to the client's premises |
| **P2** | Implementation | • HW & SW installation and configuration per the client's contract<br>• System customization and adaptation to local networks and devices<br>• System testing |
| **P3** | Training & Commissioning | • Detailed system training; including practicing real-life scenarios<br>• System Acceptance Test (SAT) by the client<br>• Onsite support for the first two working weeks of the system |

**Week**

Cyber Technologies




## 14.4 System Acceptance Test (SAT)

Q Cyber Technologies has extensive experience installing and implementing our Pegasus system.

The System Acceptance Test (SAT) covers the following:

- Sets out the scope of work
- Describes the approach and tests to be performed to validate agreed-upon system functions
- Verifies the system is fully functioning
- Validates that agreed-upon functionalities have been delivered and received by the client

The tests are divided into the following stages:

1. Functionality
2. Network and provider
3. Client-tailored

An official system hand over—from Q Cyber Technologies to you—is performed once the system has been deployed, tested, and used for demonstration checks.

Cyber Technologies

# 15 MAINTENANCE, SUPPORT, AND UPDATES

Q Cyber Technologies provides one year of maintenance, support, and upgrade services.

## 15.1 Maintenance and Support

Requests for an onsite support engineer to help troubleshoot and to take on greater responsibilities will be evaluated per client.

| | |
|---|---|
| **SW upgrades** | • Periodic SW releases add new features and capabilities, and fix bugs<br>• New upgrades are coordinated with the client to minimize system downtime |
| **SW hotfix** | • Dedicated SW package to fix critical bugs (unrelated to periodic SW upgrades)<br>• SW hotfixes are provided when a new OS version is introduced for a specific platform; Redacted - Export Controlled |
| **Health-monitoring system** | • Connected 24/7 to the support team's NOC<br>• Monitored by a system configured to perform the following:<br>– Connect all major HW components and provide system's health status in real time<br>– Monitor SW components (e.g., tunnels and 3rd party services) and send alerts if a service is down or will be affected due to technical and/or white balance reasons<br>– Alerts for all security incidents relating to the system |
| **NOC 24/7 tier support** | • Tickets are submitted by phone, secured website, or email<br>• NOC representatives follow support procedures to ensure each ticket is handled according to the SLA |

| Tier 1 | Tier 2 | Tier 3 |
|---|---|---|
| Company-trained engineer provides support.<br>• Support includes:<br>– SW & HW installations<br>– Upgrades<br>– Basic troubleshooting<br>– Configuration changes<br>– Operation optimization | Field Service Engineer (FTE) provides proactive, best-effort support.<br>• Dedicated engineers inspect, examine, and resolve common technical issues<br>• If required, remote assistance is provided via remote desktop SW and a Virtual Private Network (VPN) | Technical support engineer provides support.<br>• Support activities include all those associated with Tier 1 and Tier 2 plus,<br>– In-depth system instruction<br>– Advanced diagnostics<br>– R&D-level troubleshooting |

## 15.2 Upgrades

Our Company releases major upgrades approximately every quarter; these upgrades include,

- New features
- New devices/OS support
- Bug fixes
- Client-tailored features

Cyber Technologies

# 16 ABBREVIATIONS AND ACRONYMS

| Abbreviation | Description |
|---|---|
| ATM | Asynchronous Transfer Mode |
| ATN | Anonymizing Transmission Network |
| BBM | Blackberry Messenger |
| C&C | Command and Control (server) |
| CID | Cell ID |
| CSV | Comma Separated Value |
| dBm | Decibel (referenced to milliwatts) |
| ESEM | Enhanced Social Engineering Message |
| FSE | Field Service Engineer |
| GB | Gigabyte |
| GPRS | General Packet Radio Service |
| GPS | Global Positioning System |
| GSM | Global System for Mobile Communications |
| GUI | Graphical User Interface |
| HW | Hardware |
| ID | Identity |
| IM | Instant Messenger |
| IMEI | International Mobile Equipment Identity |
| IMSI | International Mobile Subscriber Identity |
| **Redacted –Export Controlled** | |
| IP | Internet Protocol |
| ISP | Internet Service Provider |
| JSON | Java Script Object Notation |
| LAN | Local Area Network |
| LI | Lawful Interception |
| LTE | Long-Term Evolution (3GPP/4G) |


| Abbreviation | Description |
|---|---|
| MB | Megabyte |
| MCC | Mobile Country Code |
| MITM | Man In The Middle |
| MNC | Mobile Network Code |
| MNO | Mobile Network Operator |
| N/A | Not applicable |
| NOC | Network Operations Center |
| OS | Operating System |
| PBX | Private Branch Exchange |
| PSTN | Public Switched Telephone Network |
| R&D | Research and Development |
| SAML | Security Assertion Markup Language |
| SAT | System Acceptance Test |
| SD | Secure Digital |
| SIM | Subscriber Identity Module |
| SLA | Service Level Agreement |
| SMS | Short Message Service |
| SSID | Service Set Identifier |
| SSL | Secure Sockets Layer |
| SW | Software |
| UI | User Interface |
| URL | Uniform Resource Locator |
| VoIP | Voice over IP |
| VPN | Virtual Private Network |
| WAN | Wide Area Network |

# Exhibit 33

**UNREDACTED VERSION OF DOCUMENT PROPOSED**

**TO BE FILED UNDER SEAL**

# Mobile Endpoint

## Product Description

## Copyright and Disclaimer



We make no representation or warranty regarding the accuracy or completeness of this document and reserve the right to alter its contents at any time without notice. Functionality and specifications featured in this document are subject to change without prior notice and vary between configurations.

Please contact us for current product features and specifications. Any supply of the products featured in this document will be subject to the terms and conditions of the relevant contract.

## Confidentiality Notice

This document is confidential and contains proprietary information. This document may be used solely for the purpose for which it is provided, that being evaluating the possibility of acquiring a license to use our solution. If you do not have written permission to use this document, then immediately cease using it and destroy all copies.

The licensing, use, sale and implementation of all products is subject to the customer provision of a signed and stamped end-user certificate and an import and/or export license issued by the relevant authorities.

# Contents





# 1 Introduction

Our company assists government law enforcement and security agencies in monitoring threats and fighting crimes. Our leading-edge mobile endpoint solution with its advanced technology overcomes today's major challenges of intelligence collection to deliver valuable intelligence on time, every time.

With a proven track record of successfully and repeatedly meeting major technological challenges, the mobile endpoint solution overcomes encryption to extract intimate content from the target's mobile device. Our solution provides a robust system that meets rigorous demands of Tier 1 organizations for operational security, data visualization, scale of operations and regulations.

# 2 The Challenges

The challenges facing law enforcement and intelligence organizations fall into three main domains: technology race, discreet interception, and data magnitude.

**Technology race**

- Hidden by encryption
- Multi-faceted mobile world
- Endless technology sprint

**Discreet interception**

- Increased target awareness
- 24/7 Monitoring
- Overcome intelligence gaps
- Restrict classified information
- Deniability
- Mobile endpoint volatility
- Comply with regulations

**Data magnitude**

- Abundance of data
- Time-critical operation
- Fragmented data sources

## Technology race

### Hidden by encryption

In the world of communications, mobile systems and most mobile applications use high standards of end-to-end encryption to answer the user's demand for privacy and security of their mobile devices. Targets take advantage and hide behind encrypted mobile devices and applications when communicating with their

accomplices. The encryption makes it virtually impossible to reveal the full content of the targets communications and the data that is stored.

### Endless technology sprint

Device manufacturers introduce new mobile devices at an accelerated speed, alongside continuous version updates for operating systems and applications. It becomes a constant race for law enforcement organizations to keep pace with the ever changing technology and stay on the target for the entire investigation.

### Multi-faceted mobile world

The mobile market is extremely characterized by diverse and new emerging technologies.

The mobile domain is dominated by two major **operating systems (OS)**. One is a closed garden highly secured system whose source code is unavailable, while the other OS has many flavors implemented by various device manufacturers making it nearly impossible to sustain.
**New devices** are constantly emerging into the market, embedding new and different security capabilities, and on top of this there are a **multitude of mobile applications**. Each application has its proprietary method of operation and security mechanisms.

Altogether, the variety of devices, OS and applications create an extremely large matrix containing hundreds of possible combinations. Providing a robust technology that can collect data from targets holding various devices, OS and using a multitude of applications is a continuous, fragmented challenge.

## Discreet interception

### Increased target awareness

Technology providers answer their customers' demands for privacy and security by providing alerts for abnormal or critical events. As a result, targets are becoming increasingly aware and suspicious of any anomaly when using mobile technology in their day to day interactions. An optimal intelligence solution is required to be more sophisticated in order to remain constantly under cover.

### 24/7 Monitoring

Targets do not keep office hours – they operate around the clock. Receiving targets' critical data timely is of extreme value, and hence requires a solution that works continuously with no downtime.

### Overcome intelligence gaps

Unfortunately, specific intelligence needed at a specific time is not necessarily reflected in the data on the target's mobile device. The ability to track the target's exact current location, to voice record, and perform similar operational scenarios are all critical in resolving and preventing crimes.
A solution that enables silently taking control over the mobile device to acquire intelligence is invaluable.

### Restrict classified information

Intelligence case work contains highly sensitive information which needs to be discreetly protected. A top requirement is a system that can compartmentalize users into restricted groups to prevent unauthorized users from accessing critical information.

### Deniability

Today's world has become an increasingly monitored world with the vast internet traffic being monitored by web services and governments. Users' activities are monitored both for commercial and for political and government administration reasons. It is necessary for intelligence gatherers to be able to stay under cover and remain anonymous. A solution that is clean and untraceable is a high requirement.

### Mobile endpoint volatility

Mobile devices are frequently reset either due to battery drain, decline in performance, or as a result of the target's action.
Having successfully installed a mobile endpoint on a target's device is a great achievement, however, in some cases a device reset or other conditions might lead to losing the mobile endpoint installation. Innovative ways are required to be able to return to the target efficiently.

### Comply with regulations

Law Enforcement Agencies work under many national legal and regulatory frameworks. If these regulations are not strictly adhered to, evidence that is gathered may be inadmissible which can lead to a failure to convict.
Regulations usually state which data can be collected and for which time period, how data should be securely managed to guarantee that it was not tampered, how data should be filed in court, who can have access to view the data and how actions that are done to collect or handle the data should be audited.
A comprehensive top tier solution should meet all such regulations to allow the law enforcement team do their professional work quietly knowing that regulations are built into the system to make sure their conviction will not fail because of a technicality.

## Data magnitude

### Abundance of data

Mobile devices store tens of thousands of records and generate vast amounts of data by the minute. When backing up data even more digital content is created. This challenge becomes more intense when dealing with a multitude of endpoints and recurrent installations. Navigating this sea of data, monitoring its flow, removing duplicated records and detecting the relevant information is a daily challenge for the analyst.

### Fragmented data sources

Data constantly pours in from a number of targets and devices – sometimes in different languages and using code names. When it comes to integrating personal data from different personal devices it is critical to view the data instantly and uniformly. Connecting data from different sources requires standardization and alignment to filter, sort, search and find the relevant content. A solution that can integrate its data paves the way to fast efficient productivity.

### Time-critical operation

As targets are on the move, collecting information about their actions in near real-time could determine the success or failure of the case. Decision makers expect to receive time-critical information without compromising on the operation's security and deniability.

# 3 Mobile Device Installations

The heart of any endpoint-based intelligence operation is installing a mobile endpoint on a target's device—each installation is carefully planned to ensure success.

The solution supports installation methods and capabilities that satisfy various operational scenarios. The following sections describe the different endpoint installation tools and techniques that are provided by the system.

The solution has worldwide global coverage and is MNO independent.

## 3.1 OS Detection

Due to the system's vast intelligence collection capabilities, certain intelligence pieces can be collected even prior to successful installation, and some of them can serve the operator's efforts to maximize the installation success rate. The operating system (OS) detection capability helps the operator decide which installation vector to use. The system will suggest the most effective and secure installation vector for the designated OS and thus help the operator overcome the multi front battle of the diverse mobile market.

## 3.2 Installation Vector Selection

Once the operator identifies the target's OS, they can select one of the system's multiple installation vectors.

The system will automatically suggest the most efficient and secure vector to match the current conditions, but the operator can override this suggestion and choose a different vector to suit the operational needs.

The system offers multiple vectors which require minimal user interaction—requiring no more than a single click.

### 3.2.1 Social Engineering

As targets today are extremely security-aware and no longer naive, special precautions must be taken to ensure the safety of an operation.

The solution offers tools for composing tailored, yet innocent looking messages—this is crucial as content credibility greatly affects whether a target clicks a link. The messages are designed to be sent at different times through various channels.

## 3.3 Installation Progress Tracking

During the installation process, the operator can keep track of the endpoint's installation status, to understand exactly what the status of each installation stage is and be in control on the entire operation. By viewing a clear status of the installation progress, the system operator can ultimately plan the operation.

## 3.4 Collect Intelligence during the Installation Process

During the endpoint installation process, even before the installation process is completed successfully, the system is already collecting intelligence from the target's device.

This enables the operator to gain valuable information about the target, such as the MSISDN, device information and more.

## 3.5 Redacted – Export Controlled

If a target was already previously installed, there are various means to stay on the target. In some cases, the endpoint will reinstall itself, while in other cases a silent reinstallation is possible. Otherwise, the system will help the operator to better prepare for future reinstallations by analyzing the target's installation history.

The system unifies and points out the most important information of the target's installation history to allow the operator to make the best decision regarding the next installation attempt, ultimately utilizing the ideal tool which the system provides to successfully reinstall the target.

### Challenges Met by Installation

The installation architecture provides an optimal solution for the following challenges:

- **Multi-faceted mobile world**
  Installs endpoints on the broadest combinations of commonly used devices and OS.
- **Hidden by encryption**
  Overcomes the highest standards of end-to-end encryption on mobile systems and most mobile applications.
- **Endless technology sprint**
  Our research teams are constantly working to ensure operation continuity.
- **Increased target awareness**
  Selects the most secure vector to install on the target's device and operates it silently.
- **Mobile endpoint volatility**
  Uses innovative ways to return to the target

# 4 Command and Control

## 4.1 Manage Communicating Endpoints

Once the endpoint has been successfully installed, the system provides an intuitive display of the live communicating endpoints.

Using this display, the operator can easily monitor and control live endpoints. Navigation is easy, keeping the most vital information at the center of attention at all times.

With minimal effort the operator is able to update, control or uninstall an endpoint.

Any update to an endpoint will automatically move it to the top of the list, bringing the update to the operator's attention, allowing the operational teams to easily monitor and maintain multiple endpoints simultaneously.

## 4.2 Endpoint Identifiers

As part of the endpoint management, the operator can access all metadata that is extracted from the endpoint, supporting the operator's future decisions.

The metadata is categorized into:

- Device information
- Endpoint information
- Activities information

Alongside the endpoint identifiers, the operator can find the relevant actions that are available for the endpoint, and can decide on the best action to be taken.

## 4.3 Send an Active Command

In order to acquire the most relevant intelligence, the system enables the operator to actively command the endpoint to collect specific types of information.

All commands are covertly activated without leaving any trace on the mobile device thereby giving maximum control over the target's device with the lowest risk.

This set of features allows the operator to decide exactly when and where to use the endpoint for creating active intelligence.

The active commands are:

1. **Locate target** – acquire the target's accurate location for a single point in time or continuously over a period of time, according to operational need.
2. **Take snapshot** – Connect a face to a target or take a look at the target's surroundings using the mobile device's front or back camera.

3. **Take a screenshot** – See exactly what the target is looking at on the screen, which application is open and what the target is currently doing with their mobile device.
4. **Room tapping** – Activate the mobile device's microphone and eavesdrop on the target and its environment's every word, anywhere in the world.

## 4.4 Request Historical Data

During the installation process, or later on at any given time, the operator can actively command the endpoint to collect all the historical data from the target's mobile device.

The endpoint dives deep into the mobile device's internal system to extract all the information that exists in the mobile device's storage from the beginning of time until the current moment.

The supported information types are:

- Call logs
- Instant messaging
- Emails
- Calendar events
- Contacts
- Browsing history
- Installed applications
- Connectivity history
- File lists and notes

## 4.5 Schedule a Command

For the operator to be able to obtain the most accurate piece of intelligence, even in situations where the endpoint has no communication whatsoever, the system allows active commands to be scheduled to support operational needs according to previously obtained intelligence.

Using this capability, any of the active commands above (locate target, take snapshot, screenshot and room tapping) can be scheduled to be triggered in a pre-defined time period, giving maximum flexibility and providing coverage even in the toughest operational scenarios when targets are taking the most extreme precautions.

## 4.6 Communication Template

As operational needs may vary, the system provides the operators with the ability to decide how they would like their endpoint to communicate. This can be configured to support any operational need.

## Challenges Met by Command and Control

The command and control architecture provides an optimal solution for the following challenges:

- **Overcome intelligence gaps**
  Send active commands or schedule commands according to operational needs.
- **Increased target awareness**
  Manage actively communicating endpoints covertly to avoid alerting targets.

# 5 Investigate

## 5.1 Activity Feed

The heart of an investigation is the activity feed. The activity feed orchestrates the entire timeline of events as they happen in the target's real life based on the data that is extracted from the target's mobile devices and other sources of information.

The feed displays all the activities that match the filter criteria selected by the operator to allow a quick and easy processing of the vast amount of data retrieved.

Using the integrated activity feed, operators can unveil discreet patterns between targets using multiple communication channels, which are almost impossible to detect from a single data type by the naked eye.

## 5.2 Modes of Use

To support all operational scenarios in the most optimal way, the feed is designed with two operation modes:

- **Live mode** – Supports on-going live operations, or any other need for instant updates. New activities extracted from the target devices are instantly pushed to the top of the feed, immediately available for the operator to see and analyze.
- **Investigate mode** – Supports a deeper investigation when there is a need to focus on a specific activity for further analysis. This mode only pushes in new activities when the user demands. A notification about new activities will appear and depending on the user's selection they will be pushed to the top of the feed for inspection and analysis.

## 5.3 Filters

As the system is designed to support both focused and broad investigations, a set of multi-layer filters helps the operator take a focused or broad view.

Each filter configured by the operator is stacked on top of the other filters giving the operator full control of the feed for both existing and new activities.

The available filters are:

- **Date/time** – See activities that happened during a specific time frame, filter out irrelevant noise, or take a look at the earliest activities found on the target's device.
- **Activity type** – Inspect only specific activity types for better focus. The system supports the selection of one or more activity types.

- **Case/target** – Select a single target, multiple targets, a whole case, or even multiple cases, to see the hidden connections between different targets or cases, or to focus on one important target.

## 5.4 Free Search

The vast amounts of extracted data can reach hundreds of thousands of activities for a single target. This makes it virtually impossible to manually locate any important piece of intelligence.

The system's search engine enables the operator to use any keyword to search all the extracted data.

On top of the extracted data, the system automatically searches inside the operator's enrichment activity, such as tags and comments, for maximum efficiency and time saving.

Once the system retrieves the search results, a set of controls is available to help the operator navigate the various search results so nothing is left unseen.

## 5.5 Activity Location

To provide additional value to the operator, the system not only extracts existing intelligence, but also fuses relevant intelligence pieces together to create an entirely new mapped picture.

Every activity that is performed by the target and is therefore extracted by the endpoint, has a location attached.

The endpoint is able to determine exactly where the target was when they received that crucial phone call, text message or any other piece of intelligence, and displays it in a user-friendly way to the operator.

## 5.6 Enrichment and Collaboration

Data collaboration is a powerful force multiplier. Since several operators may be analyzing the data that was collected by the system, it is crucial that system operators are able to collaborate in order to increase efficiency and save valuable time.

The system provides several enrichment and collaboration capabilities:

- **Tags** – Operators can tag any activity that may require further investigation, may have great significance, or mark it for whatever reason the current operation needs. All tagged activities can be easily reached later on by different operators.
- **Comments** – Operators can add a comment to every activity for translation, decryption of a code, or any other important statement that is worth sharing with other operators. Comments are searchable using the search engine making it a powerful tool for collaboration.
- **Sharing activities** – Operators are able to share an activity with other operators who have permission to view the activity to point out important information.

## 5.7 Aggregate and Deduplicate Data

As targets may be installed over and over again during an operation, the same stored intelligence is collected over and over again.

In order to avoid unnecessary duplications and yet centralize all the most important information in a relevant place, the system has a state of the art deduplication mechanism, which is capable of distinguishing between activities that have been updated, or are just plain duplicates.

The relevant intelligence is aggregated and cleaned, even between different installations of the same target, providing continuity in a target's investigation.

## 5.8 Data History

The target can create certain types of activities along the way for example, a contact may be updated or a Wi-Fi password may be changed.

The system unifies vital pieces of intelligence and displays the history of events, allowing the operator to get a unique view of the target's behavior and unveil the secrets even the most sophisticated targets are trying to hide.

## 5.9 Dedicated Views

The system provides dedicated views–tailor-made for specific activity types in addition to the activity feed. This capability allows the operator the flexibility to see these activities in the most convenient way for each activity.

While the *activity feed* helps the operator understand the true order of events, *dedicated views* allow the operator to focus on a specific activity type, and dig deeper.

## 5.10 Reporting

Whether it is for management review, or for court submission, the system provides maximum flexibility when designing the reports. The report generator exports the data according to the pre-defined filter in the Investigate module and also enables various sorting possibilities and enrichments to the report. Reports are available in either HTML or CSV format.

Each report is bundled with all the necessary intelligence, including the activities and enrichments, and also includes downloaded attachments which can be opened from within the HTML report.

### Challenges Met by Investigation

The investigation architecture provides an optimal solution for the following challenges.

- **Abundance of data**
  Provides a variety of filters to navigate and find the needle in the haystack
- **Fragmented data sources**
  Unifies the different data sources into a single friendly display
- **24/7 Monitoring**
  As data pours in around the clock it is brought to the attention of the operator
- **Time-critical operation**
  Provides access to time-critical information to develop the target investigation in a timely manner

# 6 Operation Security and Permissions

Different organizations have different needs, so the system supports a dynamic and very flexible authorization, compartmentalization and permission mechanism.

The main purpose of this mechanism is to enable organizations to restrict access to both intelligence data and the operations that are available to specific users in order to meet the organization's operational security needs and also to comply with regulations.

## 6.1 Operation Security

A key security aspect is the architecture's built-in Health Monitoring System infrastructure. Every product component and instance is monitored for two main reasons: the ability to both receive real-time alerts (used to improve operational and business continuity), and log historical events (allows investigation of past incidents).
Great effort is taken to constantly develop and update Operational Security (OPSEC) alerts as they effectively protect both client confidentiality and Company assets. The related alert may lead the Company to recommend taking preemptive action such as agent removal from a target's device.

It is crucial to note that all product monitoring is handled with a focus on client confidentiality; no sensitive target information is accessible to Company employees.

## 6.2 Roles

The system supports six different user roles. Customers can assign their users with the relevant user roles to meet operational needs while restricting access to classified cases, targets and system operations.

- **Acquirer** – Enables users to perform installation of new targets and issue active commands. The content collected from the targets is not available to users in this role.

- **Analyst** – Enables users to view and analyze content collected from installed targets, enrich the intelligence and export it in case of need. Users in this role cannot install new targets.
- **Operator** – Enables users to perform mobile endpoint installation of new targets, issue active commands, view and analyze content that is collected from the targets, enrich and export the data.
- **Supervisor** – Enables users to perform installation of new targets, issue active commands, view and analyze content that is collected from the targets, and enrich and export the data. On top of the above, the supervisor can also create new communication templates and delete existing targets from the system when they are no longer needed.
- **Administrator** – Enables the creation of new users, user groups and cases, and the assignment of users to user groups and cases. This role has no access to any intelligence data.
- **Auditor** – Enables users to audit the usage of the system, see all the actions that were performed and comply with regulations. This role has no access to any intelligence data.

## 6.3 User Groups

The system assigns specific user groups to different cases. Any user can be assigned to one or more user groups and each user group can be assigned to one or more cases.

This allows organizations to create compartmentalization and restrict specific user groups from accessing classified information and targets.

## 6.4 Cases

Each case in the system can host multiple targets, and each target can be assigned to multiple cases.

A user can only see information about cases that are assigned to the permitted user group.

### Challenges Met by Operation Security and Permissions

The architecture of administration and permissions provides an optimal solution for the following challenges.

- **Restrict classified information**
  Restricts access to intelligence to specific user groups by creating compartmentalization
- **Deniability**
  Provides the optimal anonymity in a monitored world and continuity of operations

# 7 Evidence Gathering

## 7.1 Warrant Management

The Warrant Management mechanism enables law enforcement agencies to comply with the legal parameters of warrants.

Legal warrants often define the time period for the collection of data, as well as the types of data that are permitted to be collected.

Warrant system settings are defined by the operator for each target. Based on the warrant settings, the system permits the operator to retrieve only data that is allowed by the warrant. If required, warrant system settings can be updated during the operation, for example, if the time period of the warrant has been extended. Warrant initial settings and changes are audited and can be presented to a court of law.

## 7.2 Data Authenticity

The system runs an automated process to ensure the authenticity of the data in the system. All data is digitally signed by the system so when data is prepared for a court of law, it includes a digital indication per record. This digital signature confirms that the origin of the data is only from the system and has not been modified since it was digitally signed.

The authenticity of collected data is guaranteed; it is sent in encrypted form and is digitally signed to prevent tampering.

### Challenges Met by Evidence Gathering

The architecture of evidence gathering provides an optimal solution for the following challenge:

- **Comply with regulations**
  Warrant settings define restrictions on data collection, and the system can ensure that the collected data is authenticated and digitally signed.

# 8 Executive Summary

The mobile endpoint solution offers the following benefits:

- **Global coverage**
  Monitor—from any location—targets' devices connected to the Internet.
- **MNO-independent**
  Comply with local laws and regulations, without the need to interact with local MNO.
- **High OPSEC standard**
  The solution is designed with OPSEC in mind so it is protected with numerous OPSEC mechanisms during installation, the agent's lifetime, and exfiltration.
- **Near real-time**
  Track your target in near real-time to monitor actions and events as they unfold.
- **Extract historical data**
  Dig into your target's historical data to find evidence or detect intentions.
- **Operate target devices**
  Activate an environmental tap to listen to a target's environment, take camera snapshots and more, to collect high value intelligence.
- **Provide data evidence that meets legal requirements**
  As defined by court warrants, data is collected and authenticated for presentation to a court of law.
- **Ongoing capability**
  Proven ability, over the years, to continuously provide new capabilities for intelligence gathering.

| | |
|---|---|
| **Installations** | • **Plan and install** mobile endpoints.<br>• **Maximize installation success rate** using built-in tools.<br>• **Ongoing tracking** of installation progress and endpoint communication routines.<br>• **Upgrade, maintain** and, when needed, **uninstall** existing mobile endpoints.<br>• **Transmit collected data** via the most secure and efficient pathways to the Command and Control (C&C) servers. |

| | |
|---|---|
| **Cases** | Presents all active cases and their target content. The Installation Management page:<br>• **Groups** all device and agent information into topics<br>• **Provides a clear view** of the installation status<br>• **Provides easy access to related actions** – the user can flip the relevant card to expose the action options and easily navigate to other sources of the same target. |
| **Investigate** | System operators and analysts study the collected data and turn it into actionable intelligence. Features include:<br>• **Live mode presents near real-time monitoring** of data received by the system as sent by a target's device; critical when dealing with sensitive targets or during operational activities.<br>• **Collaboration** – mark and share interesting intelligence between system operators.<br>• **Timeline view** – allows you to create in a single view a sequence of events from unrelated data sources.<br>• **Continuous tracking** – every action made by the target has its location attached to it.<br>• **Search and filter** – search by text and keywords, filter by activity types and dates.<br>• **Enrich** – add tags to bookmark relevant information and add comments for future reference.<br>• **Export** – collected data can be exported to various formats for further analysis and inspection and submission to a court of law. |
| **Commands** | Activate these extraction methods:<br>• **Active data collection** - Activate environmental tap to listen to a target's environment, take camera snapshots, retrieve files, and locate the target.<br>• **Historical data extraction** - extract all existing data on a target's device. |

| | |
|---|---|
| **Administration** | Manage all system administration tasks:<br>• **Permissions:** System administrator sets up and manages operators, groups, and their related roles to control user access to given targets, cases, and data.<br>• **Auditing:** Tracks all user activities and operations in the system from log in to log out. A system is in place to ensure the integrity of all audited data, ensuring no changes or deletions take place. |

## 8.1 Support and Research

Law enforcement and security agencies are forced to deploy a cutting-edge cyber solution to ensure they remain at the forefront of the race.

Our research teams are constantly searching for new ways to deliver the customer a unique ability for collecting intimate intelligence from targets. Research is constantly ongoing to keep pace with ever-changing technology and agile market trends.

Our support teams work around the clock to ensure the system is operational 24/7 maintaining the invaluable flow of intelligence at all times.

For over a decade, the Company has been providing Tier 1 agencies worldwide, a proven operational solution to fight terror and crime effectively. Our top tier solution is an industry benchmark when it comes to bridging the technology gap in today's cyber battlefields.

# Exhibit 35

**UNREDACTED VERSION OF DOCUMENT PROPOSED**

**TO BE FILED UNDER SEAL**

# BILL OF MATERIALS (BOM) FOR SYSTEM INSTALLATION HARDWARE

The below list includes all required hardware. If an item is replaced by another product, the replacement item will be equivalent to or better than that listed in the BOM.

Disclaimer: This list may change if network, regulation, system, and/or country feature-support changes.

| Item Description | Manufacturer | Qty | Device Model |
|---|---|---|---|
| PowerEdge R730xd Server | | | |
| PE R730/xd Motherboard MLK | Dell | 1 | DELL-R730XD-22643-1 |
| Intel Xeon E5-2643 v4 3.4GHz,20M Cache,9.60GT/s QPI,Turbo,HT,6C/12T (135W) Max Mem 2400MHz | | | |
| Intel Xeon E5-2643 v4 3.4GHz,20M Cache,9.60GT/s QPI,Turbo,HT,6C/12T (135W) Max Mem 2400MHz | | | |
| R730/xd PCIe Riser 2, Center R730/xd PCIe Riser 1, Right | | | |
| PowerEdge R730xd Shipping EMEA1 (English/French/German/Spanish/Russian/Hebrew) Bezel | | | |
| Chassis with up to 24, 2.5" Hard Drives DIMM Blanks for System with 2 Processors Performance Optimized | | | |
| 12 X 8GB RDIMM, 2400MT/s, Single Rank, x8 Data Width 2400MT/s RDIMMs | | | |
| Standard Heatsink for PowerEdge R730/R730xd | | | |
| iDRAC8 Enterprise, integrated Dell Remote Access Controller, Enterprise 2 X 300GB 15K RPM SAS 12Gbps 2.5in Hot-plug Hard Drive | | | |
| 16 X 1TB 7.2K RPM Near-Line SAS 12Gbps 2.5in Hot-plug Hard Drive PERC H730 Integrated RAID Controller, 1GB Cache | | | |
| Performance BIOS Settings | | | |
| Dual, Hot-plug, Redundant Power Supply (1+1), 750W C13 to C14, PDU Style, 10 AMP, 2 Feet (.6m), Power Cord PowerEdge Server FIPS TPM 2.0 | | | |
| Intel Ethernet i350 QP 1Gb Network Daughter Card Intel Ethernet I350 QP 1Gb Server Adapter | | | |
| No Media Required No Operating System | | | |
| OpenManage Essentials, Server Configuration Management | | | |
| Electronic System Documentation and OpenManage DVD Kit, PowerEdge R730/xd OEM Order | | | |
| No Installation Service Selected (Contact Sales Rep for more details) Not Selected in this Configuration | | | |

| Item Description | Manufacturer | Qty | Device Model |
|---|---|---|---|
| Asset Service - System Shipbox Label (Model, Svc Tag, Order Information, Basic Config Details) ReadyRails Sliding Rails With Cable Management Arm<br>RAID 1+RAID 5 for H330/H730/H730P (2 + 3-22 HDDs or SSDs)<br>Enterprise Order - EMEA. Base Warranty<br>1Yr Parts Only Warranty (Emerging Only)<br>INFO 1Yr ProSupport and Next Business Day On-Site Service (Emerging Only) 3Yr ProSupport and Next Business Day On-Site Service (Emerging Only)<br>3Yr Data Protection - Keep Your Hard Drive Consolidation Fee ESG<br>EX-Works | | | |
| PowerEdge R730 Server<br>PE R730/xd Motherboard MLK<br>Intel Xeon E5-2650 v4 2.2GHz,30M Cache,9.60GT/s QPI,Turbo,HT,12C/24T (105W) Max Mem 2400MHz<br>Intel Xeon E5-2650 v4 2.2GHz,30M Cache,9.60GT/s QPI,Turbo,HT,12C/24T (105W) Max Mem 2400MHz<br>R730/xd PCIe Riser 2, Center R730 PCIe Riser 3, Left R730/xd PCIe Riser 1, Right<br>PowerEdge R730 Shipping EMEA1 (English/French/German/Spanish/Russian/Hebrew) | Dell | 3 | DELL-R730-E5-22650-1 |
| Bezel<br>Chassis with up to 8, 3.5" Hard Drives DIMM Blanks for System with 2 Processors Performance Optimized<br>2400MT/s RDIMMs<br>12 X 16GB RDIMM, 2400MT/s, Dual Rank, x8 Data Width 2 X Standard Heatsink for PowerEdge R730/R730xd<br>iDRAC8 Enterprise, integrated Dell Remote Access Controller, Enterprise<br>2 X 300GB 15K RPM SAS 12Gbps 2.5in Hot-plug Hard Drive,3.5in HYB CARR PERC H730 Integrated RAID Controller, 1GB Cache<br>Performance BIOS Settings DVD+/-RW, SATA, Internal<br>Dual, Hot-plug, Redundant Power Supply (1+1), 750W C13 to C14, PDU Style, 10 AMP, 2 Feet (.6m), Power Cord No Trusted Platform Module | | | |

| Item Description | Manufacturer | Qty | Device Model |
|---|---|---|---|
| Intel Ethernet i350 QP 1Gb Network Daughter Card Intel Ethernet I350 QP 1Gb Server Adapter<br>Emulex LPe16002B, Dual Port 16Gb Fibre Channel HBA, Low Profile No Media Required<br>No Operating System<br>Electronic System Documentation and OpenManage DVD Kit, PowerEdge R730/xd OEM Order<br>No Installation Service Selected (Contact Sales Rep for more details) Not Selected in this Configuration<br>Asset Service - System Shipbox Label (Model, Svc Tag, Order Information, Basic Config Details) ReadyRails Sliding Rails With Cable Management Arm<br>RAID 1 for H330/H730/H730P (2 HDDs or SSDs)<br>Enterprise Order - EMEA. Base Warranty<br>1Yr Parts Only Warranty (Emerging Only)<br>INFO 1Yr ProSupport and Next Business Day On-Site Service (Emerging Only) 3Yr ProSupport and Next Business Day On-Site Service (Emerging Only)<br>3Yr Data Protection - Keep Your Hard Drive Consolidation Fee ESG<br>EX-Works | | | |
| Dell 18.5in LED KMM DKMMLED185-001 | Dell | 1 | DKMMLED185-001 |
| Mounting braket for Dell 185FPM & LED KMM Consul | Dell | 1 | 185FPM |
| Dell DMPUIQ-VMCHS-G01 for Dell SIM for VGA, USB | Dell | 8 | DMPUIQ-VMCHS-G01 |
| Dell DAV2108 8-port analog, with 1 local user | Dell | 1 | DAV2108 |
| NetApp EF5600-FC Dual Controller x 2 25X1.6TB SSD Non-FDE,DE5600,0E,-C Battery,E5400,E5500,E5600,0E,-C<br>EF560A,48GB Controller,16Gb FC,4-ports,0E,-C Blank,Dsk Drv Filler,DE5600,0E,-C<br>SFP,10Gb iSCSI/16Gb FC,Unified,E-Series,0E,-C Cable,SAS HD to miniSAS,SAS2,1m,0E,-C Cable,miniSAS,1m,0E,-C<br>Pwr Cord,In-Cabinet,2m,C14-C13,E-Series,0E,-C ESM,SBB-2,0E,-C | NetApp | 1 | EF5600<br>X-48619-00-0E-C X2 EF-X564802A-0E-C X2 X-35610-00-0E-C X12<br>X-48895-00-0E-R6-C X8 X-26002-00-0E-R6-C X2 X-20004-00-0E-R6-C X2<br>DOC-EF5X0-SYS-0E-C X1 X-52197-00-0E-C X1 |

| Item Description | Manufacturer | Qty | Device Model |
|---|---|---|---|
| Blank,Dsk Drv Filler,DE5600,0E,-C Cable,miniSAS,1m,0E,-C<br>Pwr Cord,In-Cabinet,2m,C14-C13,E-Series,0E,-C Cable,OPT,50u,2GHz/KM,MM,LC/LC,2M,R6<br>Cable,Ethernet,ACP,RJ45,CAT6,2m,R6<br>Enclosure,2U-24,DE5600,Empty,2PSU,0E,-C+Rail Kit SSD,1.6TB,Non-FDE,DE5600,0E,-C<br>Enclosure,2U-24,DE5600,Empty,2PSU,DM,0E,-C<br>OS Enable,Per-0.1TB,SANTRCTY,Ultra-Stor,0E,-C OS Enable,Per-0.1TB,SANTRCTY,Ultra-Stor,0E,-C OS Enable,Per-0.1TB,SANTRCTY,Ultra-Stor,0E,-C Non Returnable Disk Plus,e<br>Non Returnable Disk Plus,e SupportEdge Standard Part Replace 4hr SupportEdge Standard Part Replace 4hr | | | E-X30030A-0E-R6-C X2 X-35610-00-0E-C X11<br>X-20004-00-0E-R6-C X2 X-52197-00-0E-C X1 X6553-R6 X8<br>X6561-R6 X2<br>E-X5681A-0E-R6-C X1 E-X4059B-0E-C X12<br>E-X5681A-DM-0E-R6-C X1 E-X4059B-0E-C X13<br>OSSANTRICITY1CAP30EC X192<br>OSSANTRICITY1CAP30EC X208<br>CS-NRD2-E X1 CS-NRD2-E X1 CS-A2-4R X1<br>CS-A2-4R X1 |
| Digi PortServer TS 16 port rackmountable RJ-45 Serial to Ethernet Terminal Server | Digium | 2 | TS 16 |
| Cisco 4331<br>IP Base License for Cisco ISR 4330 Series<br>U.S. Export Restriction Compliance license for 4 Performance on Demand License for 4330 Series<br>4-port Layer 2 GE Switch Network Interface Module AC Power Supply for Cisco ISR 4330<br>POWER CORD<br>Security License for Cisco ISR 4330 Series 4G Flash Memory for Cisco ISR 4300<br>4G DRAM (1 x 4G) for Cisco ISR 4300 | Cisco | 3 | ISR4331-SEC/K9 SL-4330-IPB-K9 X3 FL-4330-HSEC-K9 X3 FL-4330-PERF-K9 X3<br>NIM-ES2-4 X3 PWR-4330-AC X3 CAB-ACE X3<br>SL-4330-SEC-K9 X3 MEM-FLSH-4G X3 NIM-BLANK X3 SM-S-BLANK X3<br>SISR4300UK9-316S X3<br>CON-3SNT-ISR4331S X3 |

| Item Description | Manufacturer | Qty | Device Model |
|---|---|---|---|
| Blank faceplate for NIM slot on Cisco ISR 4400 Removable faceplate for SM slot on Cisco 4000 Cisco ISR 4300 Series Universal | | | |
| Cisco 3850<br>Catalyst 3850 48 Port Data IP Base<br>Catalyst 3K-X 350W AC Secondary Power Supply<br>Cisco Catalyst 3850 2 x 10GE Network Module Europe AC Type A Power Cable | Cisco | 2 | WS-C3850-48T-S S3850UK9-163 X2<br>PWR-C1-350WAC/2 X2 |
| 50CM Type 1 Stacking Cable<br>Catalyst 3750X and 3850 Stack Power Cable 30 CM 350W AC Config 1 Power Supply<br>3YR SNTC 8X5XNBD Cisco Catalyst 3850 48 Pt Data | | | C3850-NM-2-10G X2 CAB-TA-EU X4<br>STACK-T1-50CM X2 CAB-SPWR-30CM X2<br>PWR-C1-350WAC X2<br>CON-3SNT-WSC388TS X2 |
| Catalyst 2960-X 48 GigE 4 x SFP LAN Base<br>3YR SMARTNET 8X5XNBD Catalyst 2960-X 48 G | Cisco | 2 | WS-C2960X-48TS-L CON-3SNT-WSC248TS X2 |
| Cinterion EHS6T-ETH ( Penta-band 3G & dual-band 2G ) Modem | Gemalto | 10 | MC55i |
| Optiplex 7050 MT<br>– OptiPlex 7050 MT : Mini-Tower<br>– Windows 10<br>– Intel Core i7-6700<br>– 16GB<br>– UK/Irish (QWERTY) Dell KB212-B QuietKey USB Keyboard Black<br>– 256 SSD Hard Drive<br>– Dell Optical (Not Wireless), Scroll USB (3 buttons scroll) Black Mouse<br>– 3Yr ProSupport and Next Business Day On-Site Service (Emerging Only) | Dell | Per contract | DELL-7050-MT |
| Dell 24" Monitor 60.4cm(23.8") Black EUR | Dell | Per desktops x2 | DELL-U2417H |

| Item Description | Manufacturer | Qty | Device Model |
|---|---|---|---|
| | | per desktop | |
| APC NetShelter SX 42U Deep Enclosure 1200X600 with Roof and Sides Black | APC | 2 | AR3300 |
| Rack PDU 2G, Metered, ZeroU, 32A, 230V, (36) C13 & (6) C19 | APC | 4 | AP8853 |
| PDU Cord Retention Kit for Full-Height & 48U, Basic & LCD-Metered PDU (1 per PDU | APC | 4 | AP9569 |
| Horizontal Cable Organizer 1U w/brush strip | | 10 | AR8429 |
| SEH UTN-250\2500 Professional USB Device Management | SEH | 1 | |
| Cat7 patch cord,0.5m,Blue | | 20 | |
| Cat7 patch cord,1m,BLue | | 40 | |
| Cat7 patch cord,2m,BLue | | 30 | |
| Cat 7 patch cord,3m,Grey | | 30 | |
| Cat 7 patch cord,5m,BLACK | | 20 | |
| Cat 7 patch cord,10m,Grey | | 10 | |
| 24 port Cat 6 patch Panel | | 4 | |
| duplex patch cord,10m - Patch cord Fiber OM3 LC LC 10m | | 8 | |
| duplex patch cord,10m - Patch cord Fiber OM3 LC LC 3m | | 8 | |
| Console Cable 6ft with RJ45 and DB9F | | 2 | |
| Blank plate 1U(10 per pack total 5 packs) | APC | 50 | AR8136BLK |
| Power Cord, C13 to C14, 5m | | 20 | |
| Power Cord, C13 to C14, 3m | | 40 | |
| Power Cord, C13 to C14, 1m | | 20 | |
| Universal shelf | | 3 | |
| APC Smart-UPS SRT 5kVA Output HW Kit | APC | 4 | SRT001 |
| power cable 3 meters for ups + Sicon 32A | APC | 4 | |
| APC Smart-UPS SRT 192V 5kVA | APC | 4 | SRT5KRMXLI |

| Item Description | Manufacturer | Qty | Device Model |
|---|---|---|---|
| APC 6kVA RM Battery Pack | APC | 4 | SRT192RMBP |
| Office Home & Business 2016 32-bit/x64 English | Microsoft | Per desktops | |
| VMware vSphere 6 Essentials Plus Kit for 3 hosts (Max 2 processors per host) | VMware | 1 | VS6-ESP-KIT-C |
| Production Support/Subscription VMware vSphere 6 Essentials Plus Kit for 1 year | VMware | 1 | VS6-ESP-KIT-P-SSS-C |
| Veeam Backup & Replication Enterprise for Vmware and Hyper-V per Socket License | Veeam | 8 Sockets 6/2 | |
| Microsoft Windows Server 2016 Standard Edition (WinSvrSTDCore 2016 SNGL OLP 2Lic NL CoreLic) | Microsoft | 32 | 9EM-00124 |
| Microsoft Windows CAL 2016 (WinSvrCAL 2016 SNGL OLP NL UsrCAL) | Microsoft | 3 | R18-05123 |
| MS SQL 2017 Server Standard core 2 socket License | Microsoft | 2 | 7NQ-01158 |
| Nagios XI (Enterprise version with 100 Nodes license) | Nagios | 1 | |
| BIG-IP Virt Edit.Appl Security Manag 200Mbps V16 | F5 | 1 | F5-BIG-ASMVE200M-V16 |
| Level 1-3 Premium Service for BIG-IP Virtual Edi | F5 | 1 | F5-SVC-BIG-VE+PREL13 |
| BIG-IP Virtual Edition IP Intelligence License 1 | F5 | 1 | F5-SBS-BIGVE-IPI11YR |