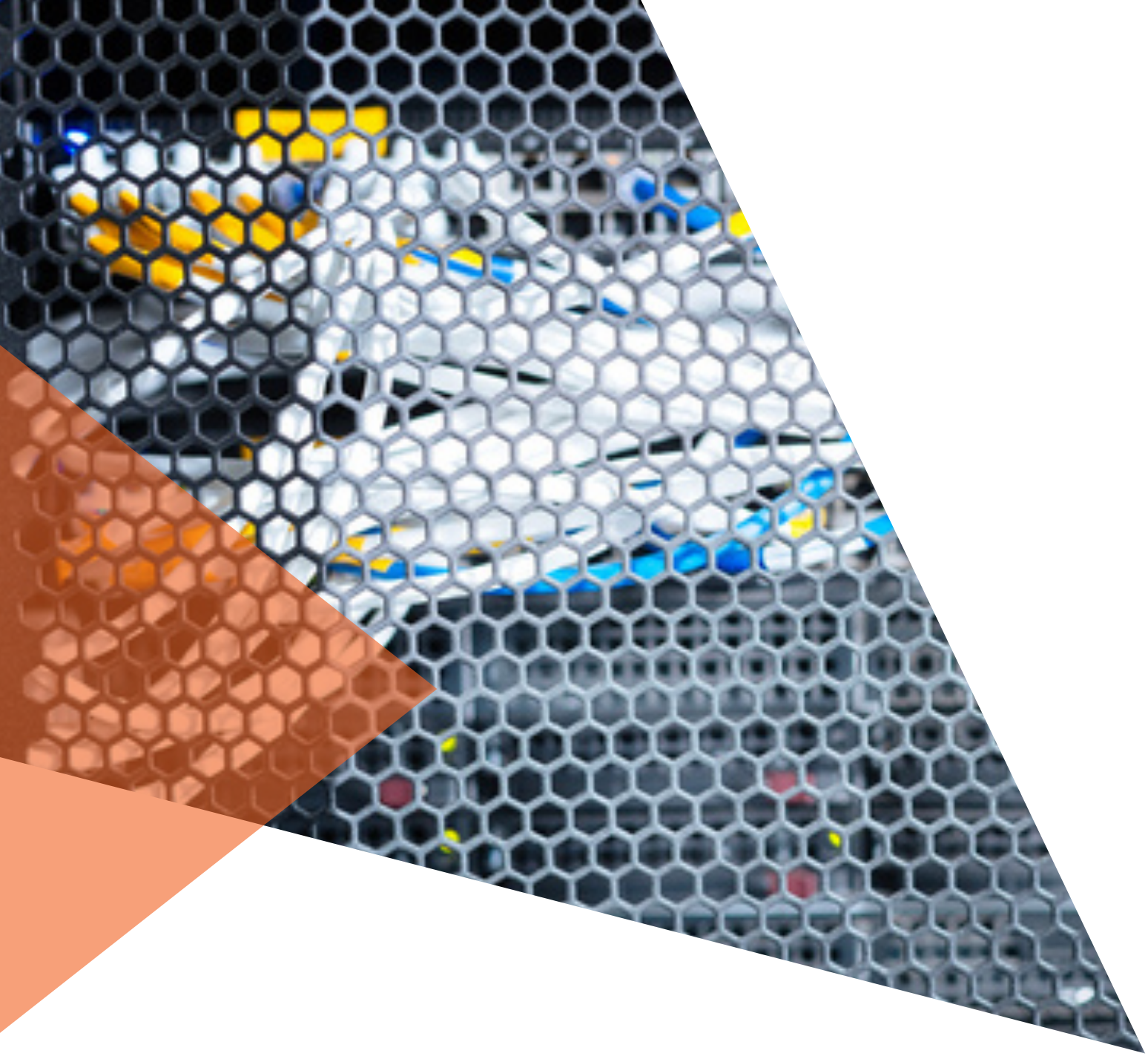


Huntsman Security

Enterprise SIEM

G-Cloud Service Description

Huntsman®

Defence-Grade Cyber Security

Commercial in Confidence

Document Date: 30 October 2025
Document Version: 1.7

Table of Contents

Huntsman Security / G-Cloud Enterprise SIEM

1 Introduction

Huntsman Security provides its Enterprise SIEM in a cloud-based (or optionally "on-premise") protective monitoring solution for organisations that operate both on-premise systems (i.e. in house) and/or cloud-based applications and server platforms.

This solution is available on the UK Government's "Digital Marketplace" through the G-Cloud framework.

Organisations may have logging and monitoring capabilities in place for platforms within their core in-house/on-premise IT environment to provide visibility to security teams or management of security events at platform or application level.

Huntsman's Enterprise SIEM allows this same level of monitoring and visibility to be extended to encompass those elements of IT operations delivered through cloud platforms (IaaS/PaaS) or applications (SaaS).

Similarly, hosting providers (G-Cloud or otherwise) may undertake a degree of security log collection and monitoring at the platform or infrastructure level (i.e. pertaining to the specific IaaS or PaaS services they provide in the cloud) or for a specific application.

The solution allows monitoring of the application operations at the user/client end, or any supporting systems such as on-premise gateway components, customer data stores or user systems.

2 Service Overview and Description

The solution leverages the tried-and-tested **Huntsman® Enterprise SIEM** to provide a complete and comprehensive threat detection, investigation and response (TDIR) capability, which can be deployed within the existing, internal server estate of the organisation or within a new or existing cloud platform. This allows:

- Integration of existing, on-premise and cloud (G-Cloud or otherwise) log sources.
- Incorporation of application layer logs from databases, intranet/extranet web applications and client-server applications where user integration at a record or transaction level needs to be monitored for potential misuse.
- Security monitoring to ensure that threats, compliance issues and misuse become immediately visible to the organisation itself.

The solution delivers:

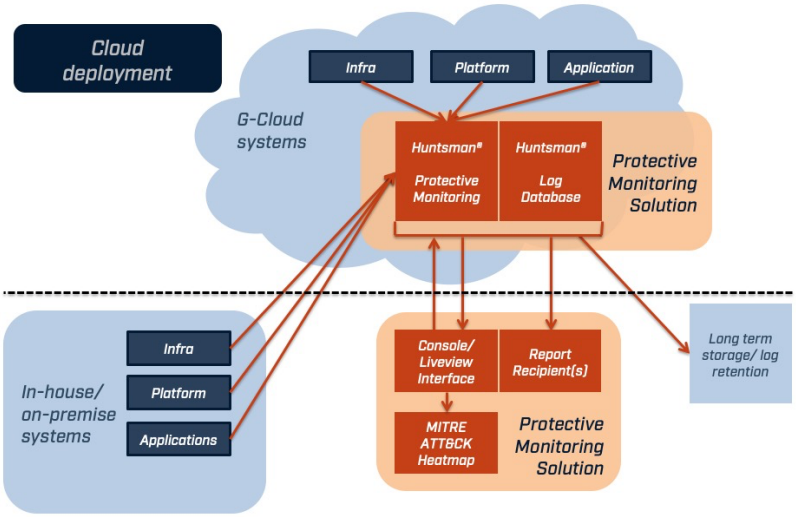
- Real-time alerting on security and compliance breaches
- High speed data processing
- Full log collection from all platforms, network infrastructure and applications
- Single console view, operation and compliance reporting for the entire organisation
- MITRE ATT&CK® Heatmap threat display
- Drilldown analysis for rapid investigation of alerts.
- Scheduled and automated compliance reporting
- Full support for workflow with an in-built incident management system

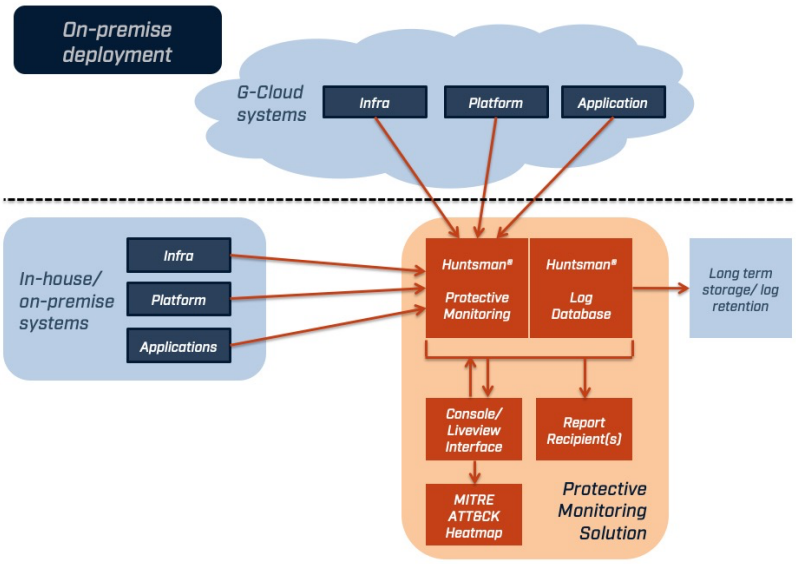
- Granular, role-based access
- In-house monitoring, reporting and alert investigation
- Full compliance support for GPG13 with the provision of alerts, queries, reports and dashboards "out of the box" with support for the latest NCSC Security Operations and Management guidance[1].
- Operational and compliance dashboards

2.1 Solution

Various deployment models are possible – within a cloud (IaaS or PaaS) deployment or even as an "on-premise" solution to monitor cloud and on-premise (e.g. user or gateway) systems.

Operation is the remit of the internal security teams to minimise external reliance and safeguard any data/operational information.





[1] https://www.ncsc.gov.uk/topics/monitoring

2.2 Benefits

- Real-time detection of security or compliance breaches.
- Rapid deployment of a functioning system.
- Complete overview through correlation of audit data from all internal and external (Cloud) devices.
- Full customer control of the threat detection and investigative processes including workflow support for handling, tracking and reporting of incidents.
- High level of (customisable) automation through all phases of the compliance lifecycle from detection, analysis, investigation and reporting.
- Representation of threats and alerts against the MITRE ATT&CK® framework for ease of understanding, investigation and response
- GPG13-based Status Dashboard giving a single console view of the organisation's compliance status aligned to more recent guidance from NCSC on "Security Operations and Monitoring".
- Supports deployment on-premise or within a cloud PaaS/IaaS environment as a virtual appliance.
- Suitable for both externally connected and air-gapped networks
- Fully scalable from small/limited scope monitoring requirements to whole enterprise monitoring
- Long term data retention (both in operation and at end-of-contract/termination) under full control of the customer organisation
- Additional compliance standards are supported (such as GDPR, PCI-DSS, ISO27001, FISMA, etc.).

3 Information Assurance / Compliance

The **Huntsman® Enterprise SIEM** solution is deployed on the customer's existing network/platforms or within a new or existing cloud IaaS or PaaS environment as two virtual machine appliances.

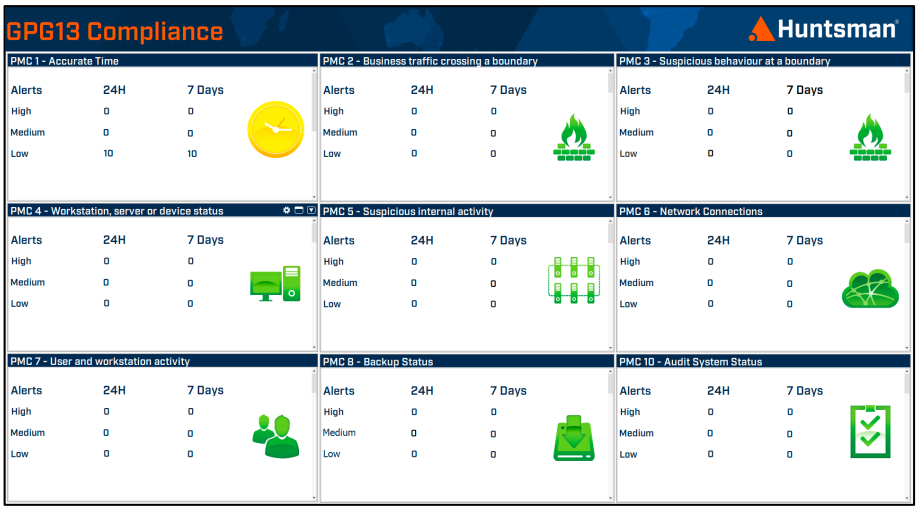
A full access control model for collected data is included to enable role-based and fine-grained access control to users, incident analysis and other stakeholders. An extensive audit trail of all user/analyst activity is retained.

Long term data storage (e.g. for compliance purposes) is within the customer's own, existing storage.

NCSC formerly advocated the use of GPG13 for security monitoring. This was superseded by updated guidance on Security Monitoring and Operations[2] as well as the requirements in the Cyber Assessment Framework (CAF)[3].

A complete set of related queries/reports is included "out of the box" to allow comprehensive compliance reporting. Alerts are also predefined to ensure that the Customer security/operations teams are aware of issues and can respond within defined service levels.

The fully interactive GPG13-aligned compliance status dashboard is provided for access by any Console user.



Huntsman® Enterprise SIEM is deployed and accredited in environments at all security classifications.

SC and DV cleared engineers are available to install and configure the software, including the building of interfaces for bespoke applications. Huntsman Security engineering support is also available to assist with solution design.

No customer organisation information/log/incident data is held, managed or accessed by Huntsman Security.

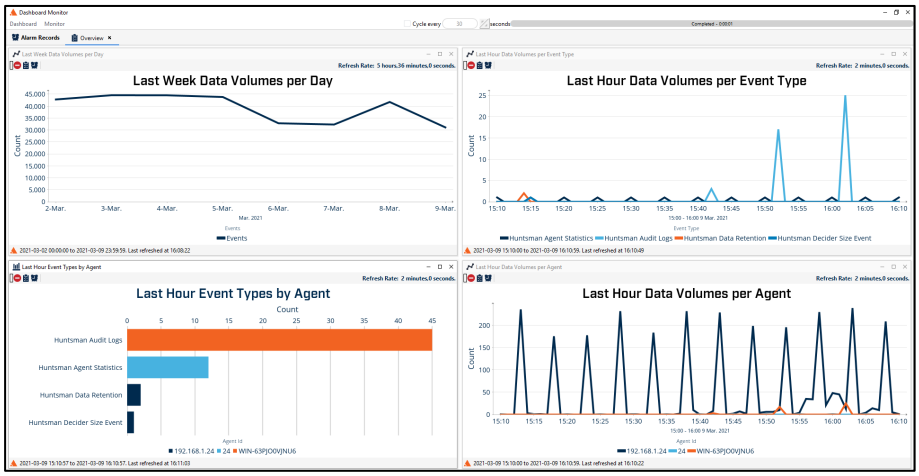
[2] https://www.ncsc.gov.uk/topics/monitoring

[3] https://www.ncsc.gov.uk/collection/cyber-assessment-framework

4 Solution Outputs

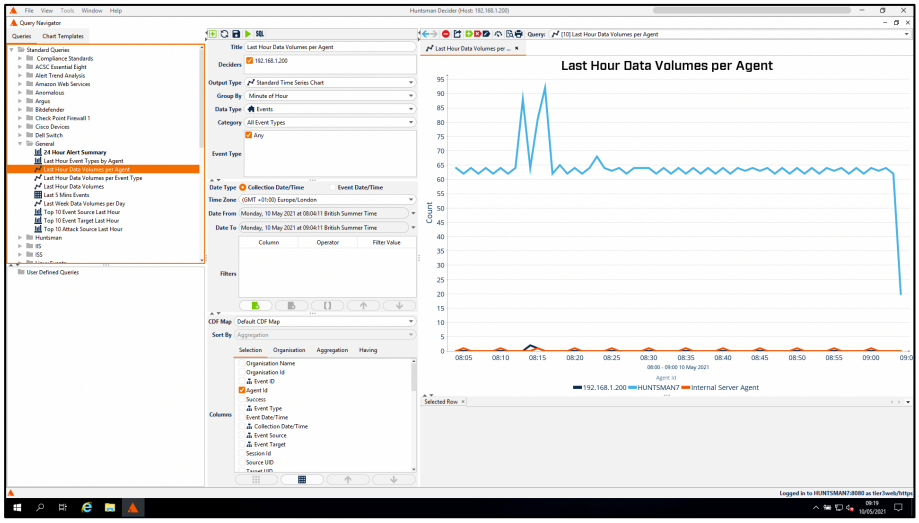
Customer security operations teams can access security information in several ways:

Operator Dashboard



Real-time visualisation with multiple dashboards and the flexibility to create custom dashboards.

Liveview (Query Navigator Interface)



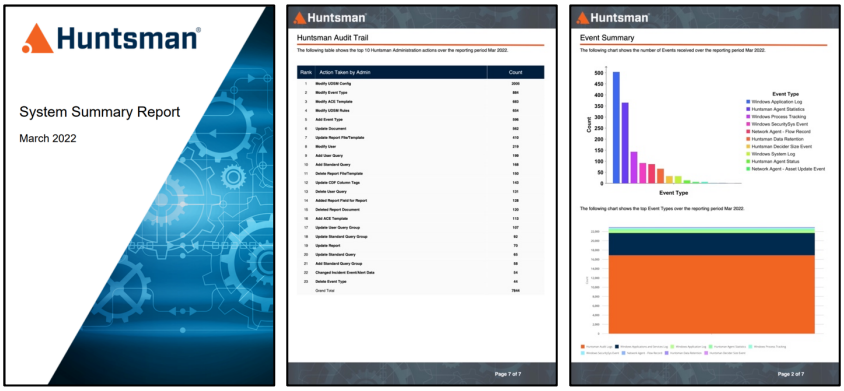
Event log and alert query interface used by customer operators for investigative purposes.

Graphical and textual information formats with full filtering, drill down and analytical capabilities.

MITRE ATT&CK® Heatmap Threat Display

MITRE ATT&CK® Heatmap represents threats against the framework to enable operators to see patterns of attack throughout the lifecycle and assess priorities for mitigation based on attack progress.

Automated and Ad-hoc Reports



800 out of the box reports providing stakeholders with focussed information.

Archive Data Retention

All data is extracted/archived in a machine-readable format. Data is stored on the customer's own storage facilities and always remains under their full control.

5 Deployment, Configuration, Operation

Deployment of the Enterprise SIEM solution is straightforward and is minimised through the pre-installation preparation activities and a virtual appliance deployment. Huntsman Security engineers will undertake the initial activation so that a functioning compliance system is available almost immediately.

Once installed and configured, all operations and monitoring (e.g. responding to alerts) remain a customer responsibility to give full control over the security alert decision-making and investigation process.

5.1 Customer Pre-requisites

The Customer environment, both the platforms to operate the virtual machine solution and the user and data source/monitored systems, is within the management of the Customer.

Ongoing operation and investigation processes are undertaken by the Customer's own security analysts/operations team.

To facilitate the solution activation, the following activities need to be completed:

- IP address information is made available for the virtual appliance infrastructure
- A suitable virtual environment for the appliances to be installed on must be identified (cloud-based or on-premise)
- Adequate data storage for the volume of data the customer intends or expects to gather/retain short and long term must be provisioned
- Appropriate change controls must be raised for the installation of the virtual appliance infrastructure, agents to be installed on monitored servers (for agent-based collection)
- Network connectivity between components must be facilitated (including network and host firewall rules)
- Access provisioned (including credentials) to systems for both software/agent installation for data collection, and to Consoles for configuration and management
- A list of platforms, log sources, security controls, and applications that require monitoring to be drawn up
- A technical point of contact to be nominated

A detailed checklist of actions and pre-requisites will be provided to facilitate the activation.

5.2 Backup and Disaster Recovery

All event and log data collected can optionally also be retained in its *Original Log File* form for compliance or backup purposes on existing customer storage systems. Longer-term event data retention is also stored on customer systems; hence both short and long-term data can be included in existing customer backup arrangements. The Huntsman® virtual machine data and configuration may also be included in these arrangements to provide a complete DR solution.

5.3 Deployment and on-boarding

The following activities will be undertaken. In this list the elements that are the responsibility of Huntsman and the Customer are indicated.

Activity/Delivery	Huntsman	Customer
Completion of the pre-install information checklist	Recipient	Completion

Activity/Delivery	Huntsman	Customer
VM server and storage provisioning		Provision
Virtual appliances – simply requires VM server	Supply	Receive
Training (up to 6 delegates)	Deliver	Attend
Engineer support for application/user on-boarding	Provide	
Configuration of initial users and user roles for – alerting, dashboards	Action	Inform
Definition of initial reporting schedule and report recipients	Action	Inform
Addition of standardised log sources	Action	
Configuration of archive retention mechanism to customer's own storage	Action	Verify
Extra support (see Rate Card) may be commissioned if required	Action	Request

5.4 Training

- User and Administration training will be provided for up to 6 customer operators.
- Customer technical, engineering or security staff can observe the on-boarding, configuration and log definition process to aid their understanding of the solution.

5.5 Operation / Service Management

The following operations will occur subject to access and availability and within the allocation of engineering days. In this list the elements that are the responsibility of Huntsman and the Customer are indicated.

Activity/Delivery	Huntsman	Customer
Scheduled reports automatically despatched to defined recipients	Configure	Receive
Automatic alerting (to customer LiveView operators)	Configure	Supply
All operation/response/alert/event interaction and investigation undertaken by customer security personnel		Operate
9-5.30 (working day) support provided for faults.	Provide	
Additional services available as required (see Rate Card)	Action	If req'd

Deployment and configuration services are included in the on-boarding - up to 5 days for size bands 1 to 4 and 10 days for size bands 5 to 10. Additional services can be purchased if required.

"Additional services" include configuration changes, additional log source interfaces, report template creation, dashboard customisation and system check-ups.

5.6 Reporting and Alerting

In this list the elements that are the responsibility of Huntsman and the Customer are indicated.

Activity/Delivery	Huntsman	Customer
Correlation alerts to be generated in line with GPG13		Receive/ Respond
Reports will be despatched on a set schedule to agreed stakeholders by email	Configure	Receive
Ad hoc reports can be generated by the customer operators at any time		Configure
All queries, alert response and investigation is undertaken by the customer operator		Operate
Hold/store customer data	No	Yes

No reports/data/raw information or alerts will be passed to, or held by, Huntsman Security.

5.7 Support and Service Levels

The table below shows the operations that are the responsibility of Huntsman and the Customer.

Activity/Delivery	Huntsman	Customer
9-5.30 support will be provided for faults	Provide	Receive
Normal day to day operation will be fully under the control of the customer		Operate
Software updates, new standard log sources, new standard queries/alerts/dashboards, new standard reports	Provide	Action
Undertaking of routine platform/system/database housekeeping	Define	Action

5.8 Long term data retention

- Log and event data, as well as generated alerts will be held within the main virtual appliance data store
- A flat-file archive will be configured to extract data after a set period of time (by default 90 days). This data will be exported in a readable form to a customer owned/controlled storage area for long term retention and backup.

5.9 Technical/Platform requirements

The **Huntsman® Enterprise SIEM** solution requires the following for installation:

- 1 x virtual machine with 4 x 2.6GHz processors (or higher), 16GB RAM, 150GB disk space
- 1 x virtual machine with 4 x 2.6GHz processors (or higher), 32GB RAM, 150GB disk space
- 3TB - 35TB provisioned disk space for the log database

Long term archive storage of log data can be held on any existing storage system/file repository.

The LiveView console software (for customer operational users) runs on Windows or Linux and requires 600Mb of disk space and 1Gb RAM. This will be installed on existing customer desktop/laptop systems.

5.10 Customer responsibilities

Customer responsibilities are defined in the appropriate tables above. Huntsman Security will work with the customer to on-board and enable the solution to facilitate and support the customer's own use and operation of the Enterprise SIEM.

This includes:

- Provision of pre-install information and technical details
- Provision of a suitable platform environment for the Huntsman virtual infrastructure
- Provision of information to support the installation/deployment
- All ongoing operation of event, alert and incident processes and management

5.11 Decommissioning and off-boarding

The decommissioning and off-boarding process is handled by Huntsman Security with input from the customer. The nature of the solution makes cessation of the service straightforward.

The following steps will be performed by a Huntsman Security engineer on a day to be agreed:

- Data collection will be disabled
- All data will be extracted to a readable archive file for local customer storage
- The customer will confirm that the data in the readable archive is correct and complete
- A backup of the database contents can be taken if required
- The virtual appliance will be deactivated and deleted. This is to be confirmed by the Customer to Huntsman Security (a pro forma letter will be provided to confirm this).

5.12 Additional, optional services

Additional services can be specified/procured at any time in line with the rate card.

Service Type	Description
Check-up	Undertaken by an experienced Huntsman Security engineer this periodic check-up is for the purpose of ensuring that system operation, housekeeping and processes are optimised and running as expected and that any potential issues are identified.
Complex log source definition	Where complex or bespoke log/data sources are in scope Huntsman Security can provide engineering support to configure the solution to incorporate these and enable operators to make sense of this information.
Advanced configuration (e.g. clustering)	Where the solution operates in a live/real-time service environment, or where clustering and resilience are key (e.g. across sites) then Huntsman Security can advise on suitable architectures, configurations and deployments.
Customising alerts and reports	Where there is a requirement for complex alerts or reports that are unique to the customer then a Huntsman Security engineer can be engaged to produce these as a professional services engagement.

5.13 Service Constraints

The **Huntsman Security Software Licence** governs appropriate use of the intellectual property and confidentiality associated with the software.

The **Support & Maintenance Agreement** defines the support services available as part of this service.

5.14 Huntsman Security service portfolio

The following optional services and assistance are available on request as professional services; please refer to the **Rate Card**. These are in addition to solution on-boarding.

Specialist Services	• Deployment in on-premise and cloud-based deployments and configuration of ancillary, support or dependant systems • Design advice/authority for protective monitoring operations and configuration of the solution to enable this with minimal effort (i.e. maximising automation) • Business analysis relating to the need for monitoring, security event and incident handling and escalation/management • Solution design and development • Transition management for security operations functions • User role definition and creation for operations teams / stakeholders
Service Integration and Management Services (SIAM)	• Enterprise security monitoring architecture • Project management during deployments • Service and systems integration • Software Support, Engineering and Helpdesk services
Information Management and Digital Continuity	• Log and event data archiving, long term retention and storage management

6 Pricing, ordering, commercial and Invoicing

6.1 Pricing

See pricing document for details.

6.2 Flexibility

Huntsman Security's solution has been designed to accommodate customers with a variety of requirements across small or large environments. The solution gives customers a fully functioning deployment and supports the requirement for individual customers to adapt the solution to their unique environment.

Where the scale, size, throughput or service needs are beyond that provided by the **Huntsman® Enterprise SIEM** then Huntsman Security can offer its enterprise architecture and licencing arrangements, however this sits outside the Digital Marketplace.

6.3 Ordering

On receipt of an order Huntsman Security will provide a technical questionnaire to determine the architecture and capture key information to allow the VM to be provisioned.

A complete Call-Off Order Form signed by both the Customer and Huntsman Security is a prerequisite to progressing an order and scheduling the deployment.

6.4 Invoicing

Commissioning and set up will be invoiced on receipt of the order.

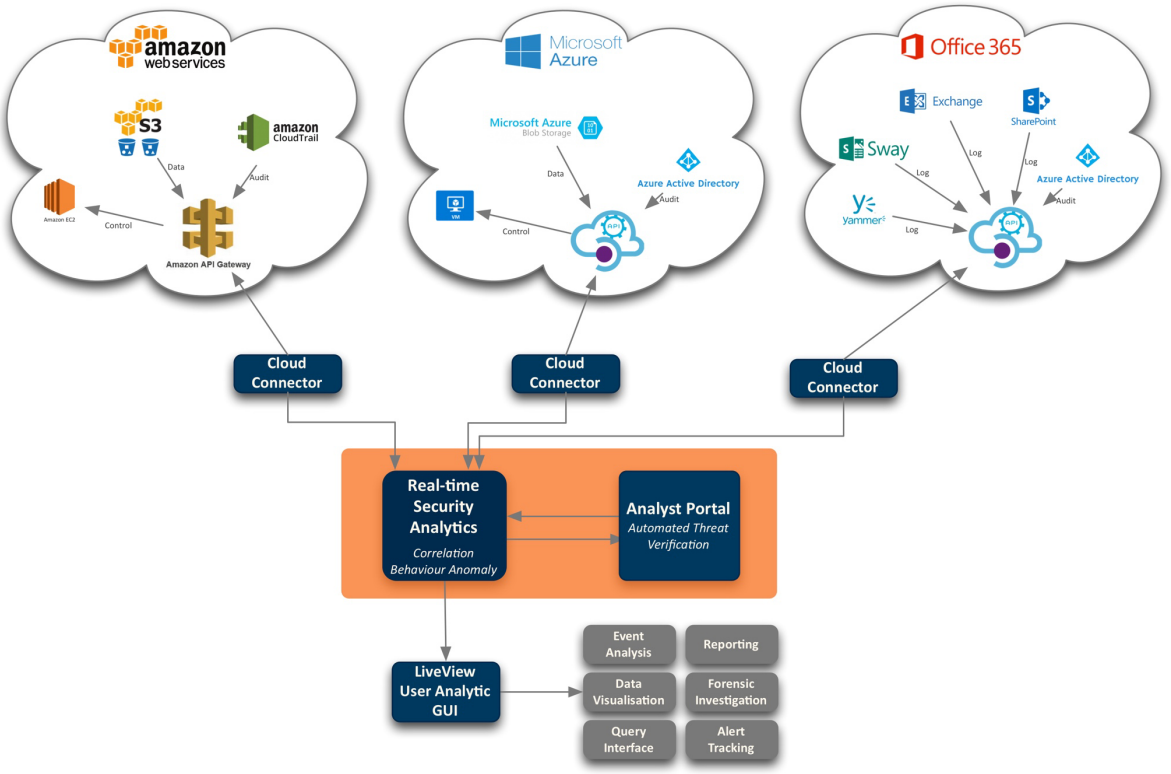
Ongoing subscription costs will be invoiced quarterly in advance.

6.5 Termination

Termination of the service requires 3 months' notice. At the point of termination, the remainder of the service period will be invoiced immediately.

Huntsman Security engineering will arrange a site visit to ensure that all customer data is extracted to a local storage location and to remove/delete the software/VM. See "Decommissioning" above.

7 Example Cloud Deployment



* * * *

http://www.huntsmansecurity.com

support@huntsmansecurity.com

Australia	+61 2 9419 3200
UK	+44 845 222 2010
Japan	+81 3 5953 8430