NCL

Critical Asset Protection.

Powered by CORTEX™ BY PALO ALTO NETWORKS

Special projects, merger and acquisition programmes, heads of development, senior executives - ensure your most important assets are protected by certified

This service provides a bespoke managed detect and response service combined with our security hardening expertise developed working with defence clients. This service is for users, data or systems that have a higher level of threat associated with them. For example: special projects, merger and acquisition programmes, heads of development, senior executives. Services may only be required for fixed periods of time and can be turned up or down on request.

paloalto® NETWORKS

This service has the benefits of our Managed Endpoint Protection service but is enhanced with bespoke audit, detect and response capabilities ensuring your most critical business assets and data has the optimum level of security.

Our security consultants will identify and help to implement secure device configurations for users and data. Activities include:

- Security hardening of user end point devices.
- Enhanced white-listing of applications and services based on user profile/ geo-location.
- Heightened policy enforcement.
- Drive encryption enforcement/validation.
- Notification of critical patches for operating systems and key software configured on devices.
- Custom audit, detect and response rules.

We work with you to define custom audit, monitoring and response actions and configure these into your devices and our tool-sets.

Features & Benefits

Features

- Bespoke detect and response rules specific to your critical asset's needs.
- Provide comprehensive audit of movement of your critical data and information assets.
- Block data movement inside and egressing your organisation unless explicitly authorised.
- Delivered from UK - based ISO 27001:2013 certified Security Operations Centre
- Security cleared staff
- Event and incident data securely retained

Benefits

- Control the location and movement of your intellectual property.
- Ensure your IP is only accessed by those authorised to do so.
- Identify and control who has access to your crown jewels.
- Focus protection effort where the risk probability or impact is greater.

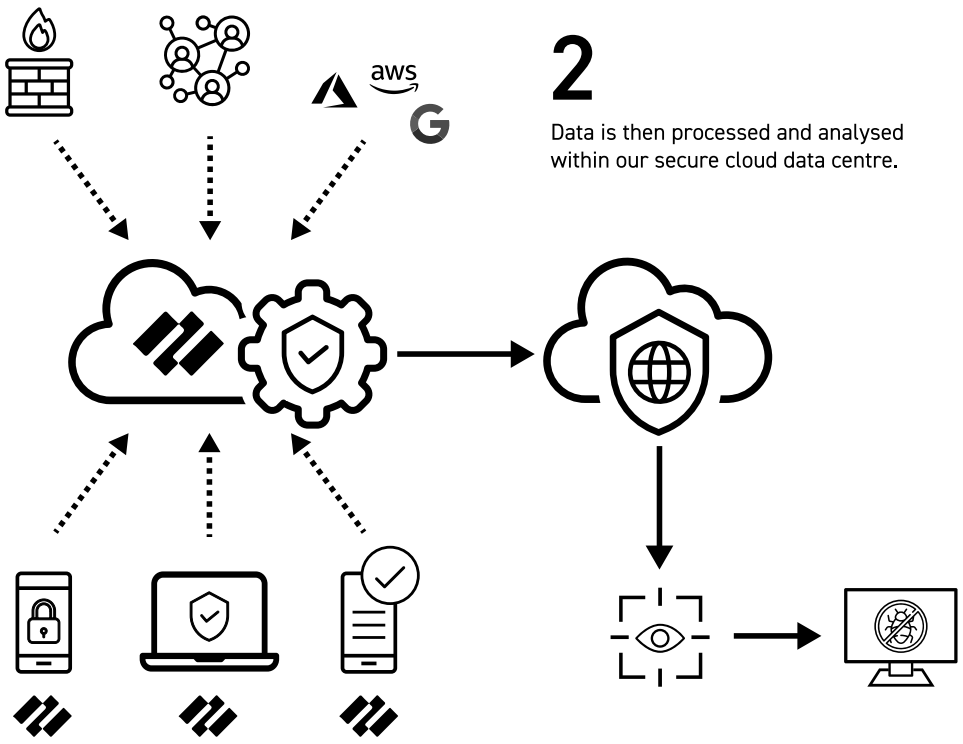
Service Delivery

For existing customers of our 'Managed Endpoint Protection' and 'Managed Detection and Response' services, Critical Asset Protection can easily be added. If you're not an existing customer, we can still create a bespoke Critical Asset Protection service for you.

1

The service is cloud based, with agents installed on endpoints and other sensors located at key points within your enterprise*.

Data from firewalls, the network and other 3rd party tools can be ingested using out-the-box integrationd or development.



2

Data is then processed and analysed within our secure cloud data centre.

3

Any threats, or suspicious activities are immediately presented to analysts within our UK-based SOC for validation and agreed response action.

4

When pre-agreed, rapid response through predetermined automated prevention/protection action can be enacted immediately upon determination.

*Subject to your change control, the service can be implemented in a matter of days and developed as more endpoints and sensors are added.

Service Levels, Reporting & Pricing

Service Levels

	Standard Package	Enhanced Package
Critical Asset automated audit, detection and Response	As required	As required
Analyst Support	Normal business hours	24 hrs/day, 7 days/week (on call)

Reporting

Reporting will be created based on the bespoke controls required in the service

Pricing

We offer a range of flexible pricing options dependent upon your preference. The services can be extended or augmented selecting options from the Service Catalogue.

- Day rate for specific engagement or addition to monthly service fee
- There is no start up fees, only a rate card or addition to your monthly fee.