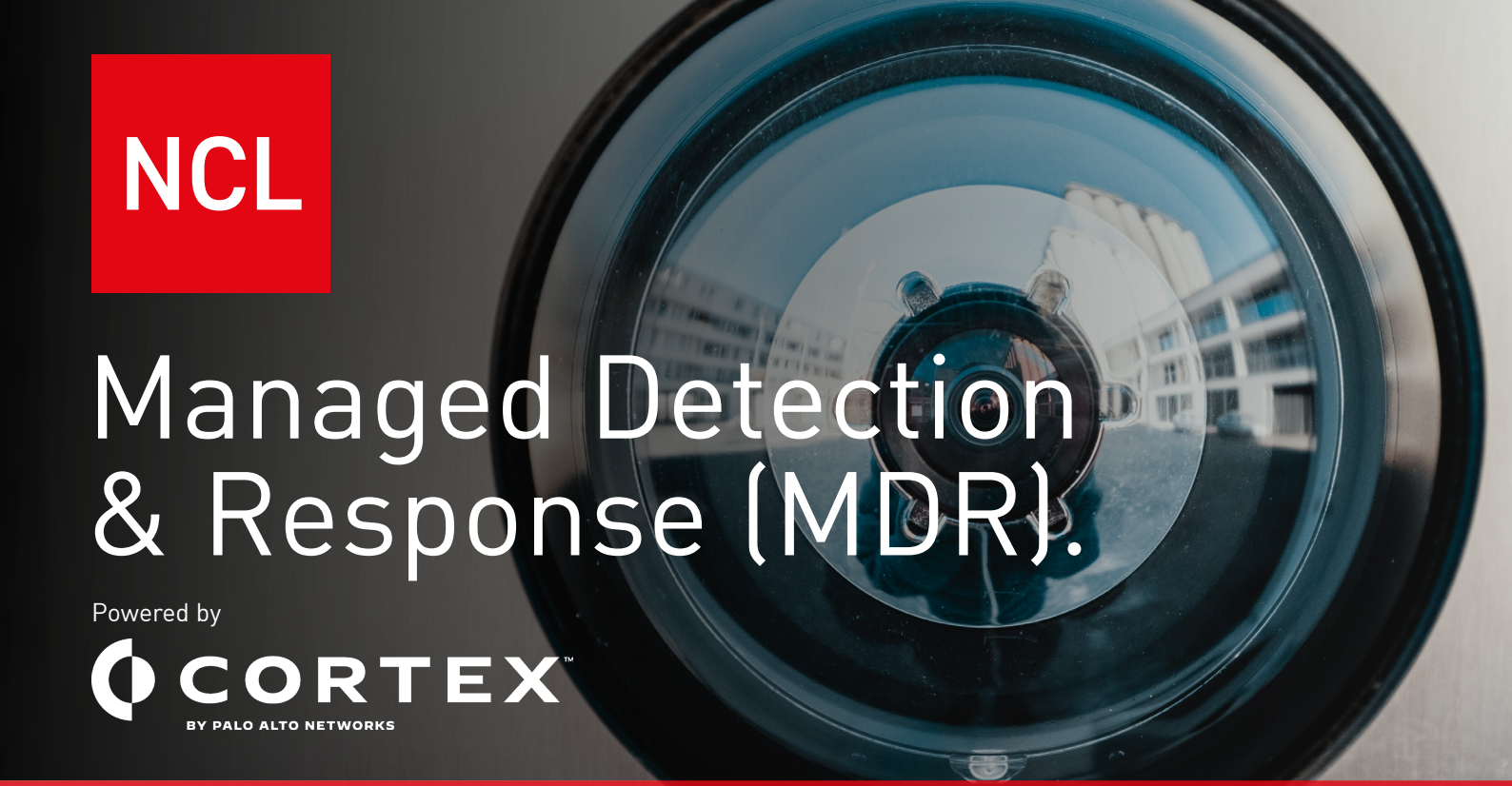


NCL

Managed Detection & Response (MDR).

Powered by CORTEX™ BY PALO ALTO NETWORKS

Real-time detection and response capabilities designed with one thing in mind – protecting your processes and digital assets from cyber threats, and all delivered from

paloalto® NETWORKS

Based on Palo Alto's leading Cortex cybersecurity solutions, our Managed Detection & Response (MDR) service is cloud native and monitors networks, users, devices and data to detect and respond to risks to your business, such as ransomware, suspicious activity, compliance or policy violations and data breaches.

Our solution optimises threat detection and investigation by automatically collecting and analysing the volume of log data from your information systems to identify vulnerabilities and threat or non-compliant activity. Once identified, workflow driven automated response activities can be completed to either isolate, stop or remediate the threat or vulnerability.

Where more complex or subtle threats are encountered, or where manual intervention or procedure is required, our UK-based security analysts provide their skills and knowledge to efficiently augment the response activity. This allows them to use their knowledge and experience to focus on the exceptions – where human intelligence is the value.

Real-time threat intelligence feeds ensure that behavioural and other indicators of compromise are constantly updated in the service.

Where immediate threats are identified, these are notified as security incidents following the defined process. Where agreed, remediation action can be either automatically or analyst enacted to minimise threat impact. Where remote or automated response cannot be undertaken, we will provide remote analyst support to your incident management team.

The visibility, situational awareness and ability to respond of your organisation is improved through the provision of incident root cause data, actions taken and context relevant reports and dashboards.

Features & Benefits

Features

- Malware detection and exploit prevention
- Identification and blocking of zero-day threats
- Advanced and Persistent Threat (APT) protection
- Proactive vulnerability detection and threat hunting
- Rapid response through predetermined automated prevention/protection action
- Flexible policy-based controls for different user group needs
- Integrates cloud, network and endpoint solutions for full enterprise cover
- Threat intelligence integrated into detection and response actions
- Ongoing advisory, optimisation and maintenance of the solution for undisturbed business
- Delivered from UK - based ISO 27001:2013 certified Security Operations Centre

Benefits

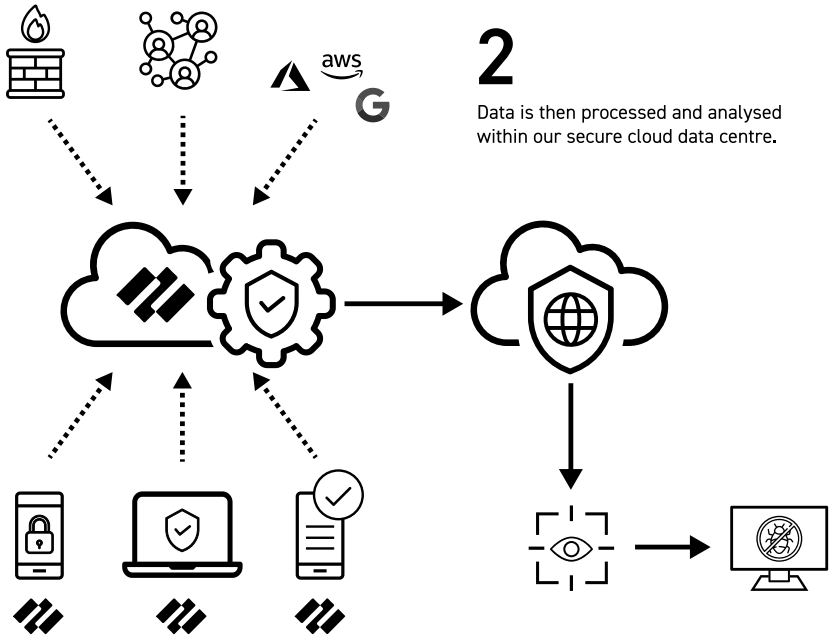
- Reduced probability of compromise/ incident
- Faster identification of compromise when it occurs
- Minimise impact of compromise through quicker more informed response
- Provides proactive defence – reducing impact of any attack
- Supports in meeting compliance standards or regulation
- Underpins legal and forensic investigations
- Informs evolution of your policies as your business changes
- Tailored service levels to meet your risk appetite and budget
- Turnkey solutions for rapid on-boarding
- Helps you manage cost (compliance, legal, incident response and recovery)

Service Delivery

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
Automated Detection, Alerting & Response	24 hrs/day, 365 days/year	24 hrs/day, 365 days/year
Analyst Response	Normal business hours	24 hrs/day, 7 days/week (on call)
Analyst Support	Normal business hours	24 hrs/day, 7 days/week (on call)
Service Desk	Normal business hours	Normal business hours

Reporting

Daily	Weekly	Monthly
Notification of significant activity i.e. high priority incidents created or updated.	Email summary of activity in period, incl: • Number of events processed • Number and type of incidents by category (malware, phishing etc) and priority. • Summary of incidents, responses and status • Identification of encrypted drives on endpoints • Summary status of sensors, endpoints and last contact	Email summary of service management activity expressed as point in time and monthly trending, incl: • Number of service fulfilment requests • RFCs received/in-progress in period and status • Service levels and key performance indicators – trending of key measures/ metrics over 12 month period • Annotated relevant contextual information • Summary of threat hunting/ Digital investigations/other-ad-hoc investigations undertaken and status • Data storage volume consumed vs available including trending growth • Recommendations for improvement

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.