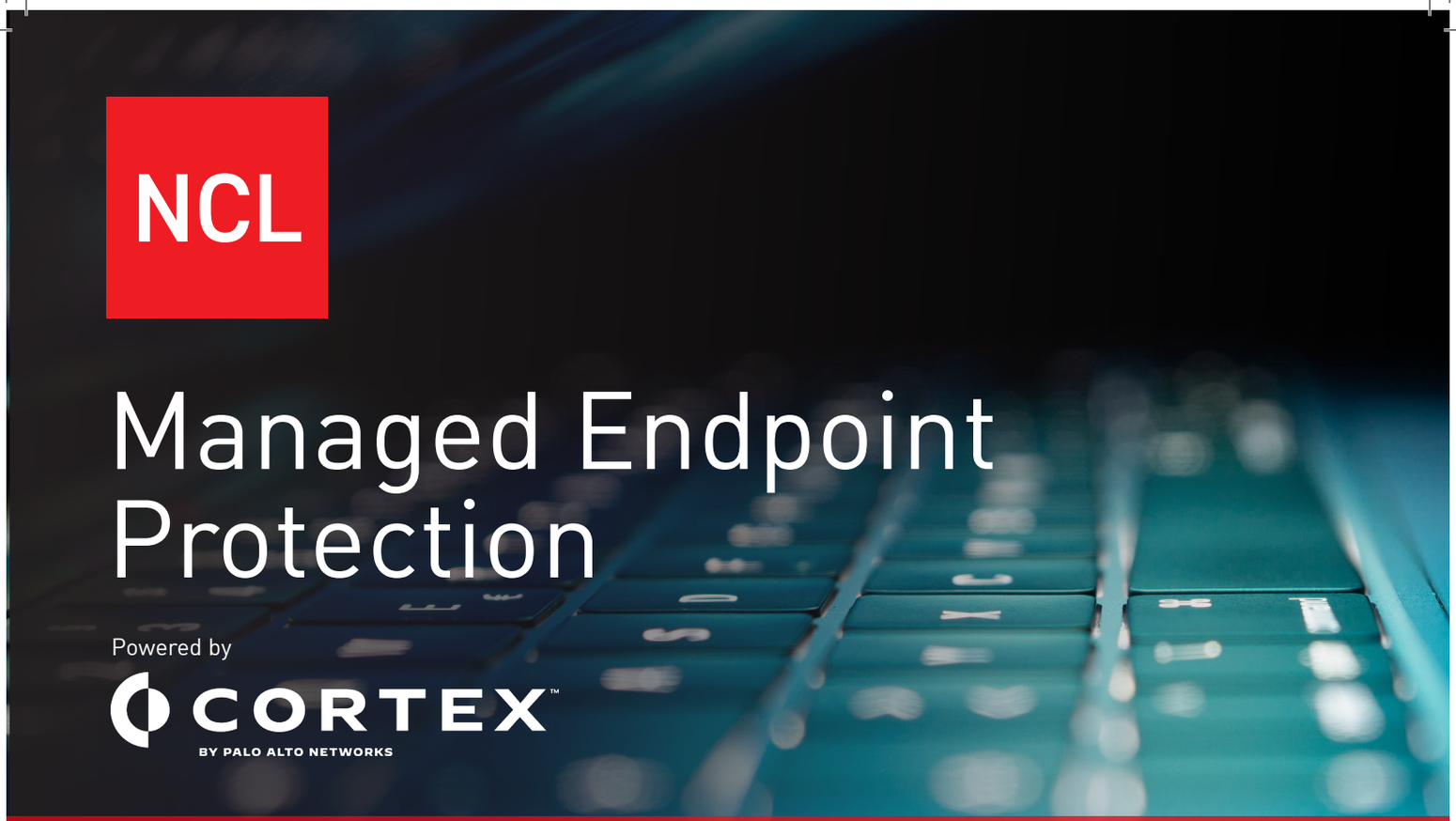


NCL

Managed Endpoint Protection

Powered by

CORTEX™
BY PALO ALTO NETWORKS

Protect your user and server endpoints from attack through AI-based proactive monitoring and behavioural based threat protection - all delivered from our UK

By analysing files before and after they execute, the service identifies the tell-tale signs of attacks, including zero-day malware, fileless and script-based attacks. Our protection techniques cover the MITRE ATT&CK™ Framework.

Our software agents provide response options to quickly contain threats while allowing analysts to collect additional endpoint information and further their investigations. Threat containment options include:

- Endpoint isolation – disabling network access expect to our management console for investigation and remediation
- Terminate processes to stop any running malware
- Blacklist files to stop further execution
- Quarantine malicious files
- Retrieve files from endpoints for further analysis and investigation
- Directly access endpoints to view, delete, move, or download files
- Enforce configuration through centrally managed policies

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 then we will provide remote analyst support to your incident. management team.

MITRE | ATT&CK™

Protection that covers the entire MITRE ATT&CK™ Framework

Features & Benefits

Features

- AI-based endpoint analysis
- Detection of common and advanced attacks
- Ransomware and malware protection
- Remote control corrective action
- SOC based centralised Management
- Integration with cloud-based WildFire® malware prevention
- Delivered from UK - based ISO 27001:2013 certified Security Operations Centre

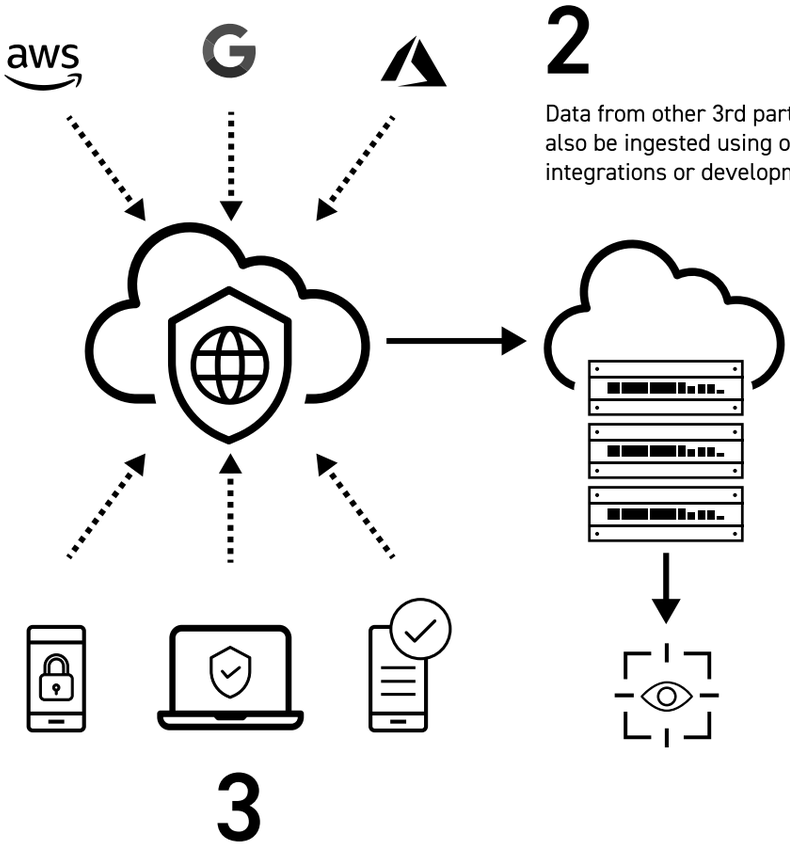
Benefits

- Reduced meantime to detect and to respond
- Minimise cost, time and effort in dealing with attacks
- Centralised management of end point security configuration
- Reduce impact of attack

Service Delivery

1

Our Managed Endpoint Protection Service is cloud based with agents installed on enpoints (laptops, desktops, tablets and servers) within your enterprise.*



2

Data from other 3rd party tools can also be ingested using out-the-box integrations or development.

3

Data is processed and analysed within our secure cloud data centre and presented to analysts within our UK based SOC for validation abd agreed response action.

*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 Support	Normal business hours	24 hrs/day, 7 days/week (on call)
Service Desk	Normal business hours	Normal business hours

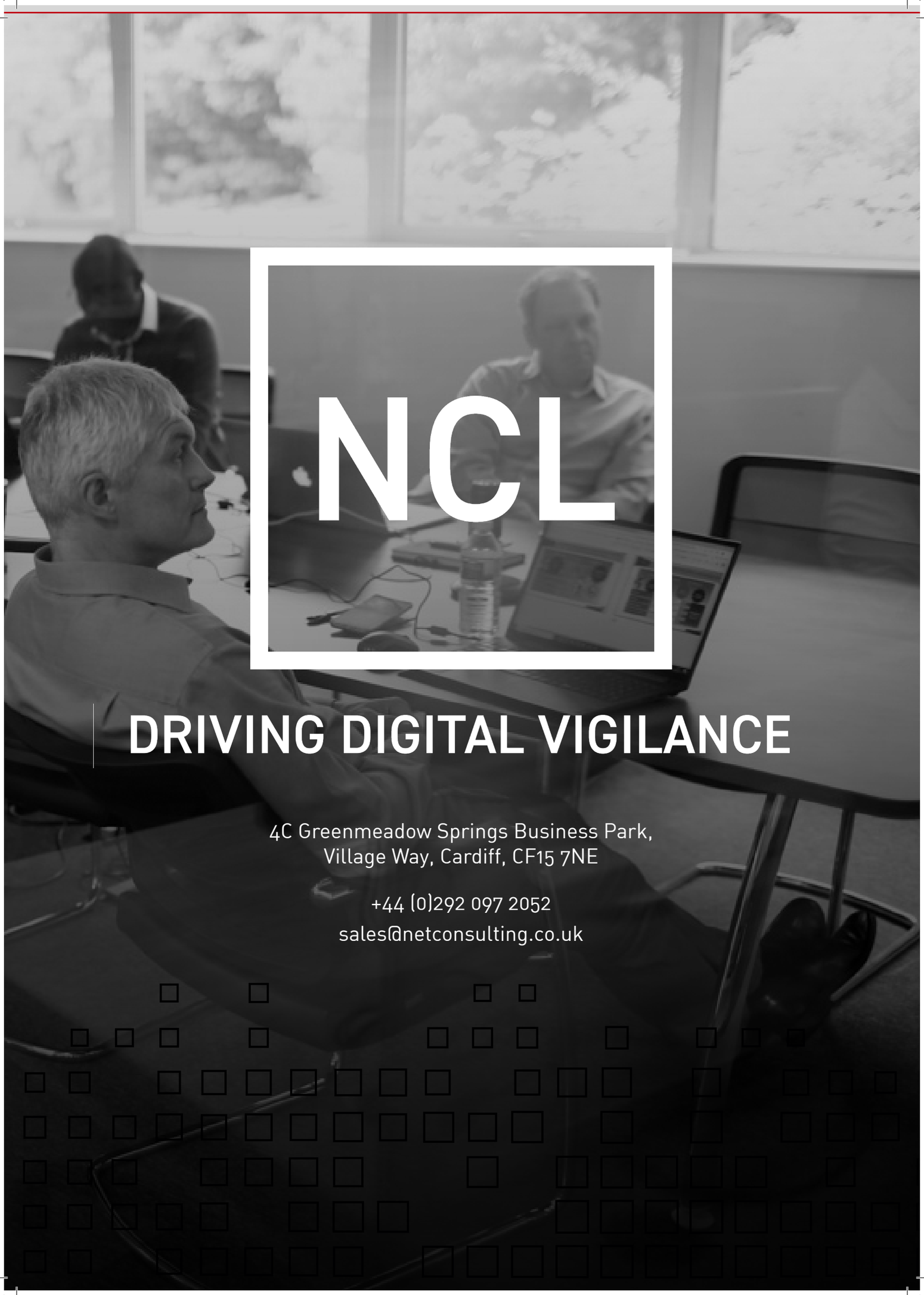
Reporting

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 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.

+44 (0)292 097 2052 sales@netconsulting.co.uk



DRIVING DIGITAL VIGILANCE

4C Greenmeadow Springs Business Park,
Village Way, Cardiff, CF15 7NE

+44 (0)292 097 2052

sales@netconsulting.co.uk