pwc

G-Cloud 15

Compromise Discovery Services

January 2026

Contents

Transforming Business using the Cloud

Enabling business and enterprise transformation using cloud is a complex, strategic consideration facing many private and public sector organisations. We have worked with many Central and Local Government clients to support the implementation of their business objectives using cloud technology.

Cloud technology and services have the potential to reduce cost, remove technology bottlenecks, and facilitate rapid business innovation. As a result, for most organisations globally, adopting cloud technology has become a question of "when and how" rather than "if".

Opportunities for enterprises include a combination of one or more of the following:

- Implementing private and/or hybrid clouds for infrastructure and applications
- Smarter use of public cloud infrastructure for optimising existing business functions
- Using cloud for implementing new business services or digital operations
- Reducing cost by moving to consumption-based pricing models that only charge for the actual IT capacity and services used.

Migration or adoption of cloud must be properly choreographed for success. We understand the realities and the business and technical risks that should be fully considered, understood and mitigated before such a move. Critical considerations include:

- **Alignment of business and technology objectives.** This is essential to fully realise the targeted benefits of any cloud transformation or any refinement of existing cloud services. There can be a tendency to adopt cloud systems to fit current ways of working, rather than adopt and standardise processes where possible. The trade-offs between business, customer and technology requirements must be considered to make informed design decisions
- **Availability and reliability of services**. The avoidance of operational downtime to mitigate in lost revenue, unnecessary operational cost or reputational damage that can disrupt business operations
- **Decentralised support structures.** The need to tailor and revise the approach to operational security to cover the support structures employed by cloud service providers that will have a different risk profile for sensitive information
- **Data handling practices.** Data classification and data-handling practices that reflect the data flow within a cloud environment must be understood and tailored accordingly to protect customer data

- **Data privacy.** Compliance with GDPR to understand where and how information can be stored or processed. The cloud model enables data to bounce swiftly around the world by using available server capacity in various geographic locations, but this must be within the bounds of what is permissible. This is ever more of a concern as organisations review their front office, back office and out of office experiences

- **Future Technology Trends.** Cloud applications are the stated direction of travel for the major application vendors, but any upgrade path must also cater for the future technology needs of the organisation and seek to minimise technical debt where possible.

A careful assessment of an organisation's needs and different cloud service provider's controls is required, enabling concerns to be addressed and the correct path to the cloud to be selected.

As a trusted advisor PwC provides the framework, and the wealth of private and public sector experience, to consider the combination of Business, customer experience and Technology activities outlined above. There is no single answer that covers each and every client organisation; we tailor our frameworks to client circumstances to better support them:

- As a partner through the complete lifecycle of strategy to execution

- With point business issues encountered during implementation or running the business.

Compromise Discovery Services

This section describes in more detail the service features and benefits included within this service definition document.

Compromise Discovery Services

Proactive assessment to identify evidence of malicious activity, both current and historical, by analysing telemetry from endpoints and external threat sources.

Compromise Discovery Services Features	Compromise Discovery Services Benefits
• Dedicated and experienced threat hunters proactively searching for advanced threats • Threat detection across the endpoints • End-to-end visibility across the IT environment • Supplemented with our own global threat intelligence feeds • Includes hygiene indicators such as outdated, commonly exploited applications • Industry leading technology layered with our advanced threat detection • Direct access to investigative and forensic specialists • Executive and technical report including prioritised recommendations • Managed Detection Response services including Orchestration and Automation (SOAR) • 24x7 Managed Cyber Defence with Palo-Alto Cortex-XDR, XSOAR, and Sentinel	• Identification of previously unknown, hidden threats, to allows effective remediation • View of threat activity and bad behaviours from legitimate users • Helps gain a state of confidence in your security infrastructure • Deep investigative and forensic analysis translated into business risk advice • Insight into critical areas of vulnerability • UK wide delivery capability • Real time, threat hunting services • SIEM orchestration and automation (SOAR) managed services and advisory • Managed Cyber Defence (MCD) SOAR services

Our view on the service features and benefits within this service definition document are presented below. There is often one common denominator in targeted cyber-attacks: **digital evidence was present in the environment long before the victim became aware of the issue.**

Our experience responding to intrusions around the world shows that targeted threat actors often maintain remote access to an environment for 6 –18 months before being detected. Unfettered access can linger for years and sometimes is never detected.

By drawing on the threat detection capabilities and skillsets in our team, we can identify the presence of threat activity in clients' IT estates, as well as other unwanted activity. Artefacts of these active threats can be detected from two key sources:

- **Endpoint** threat detection
- **External** threat detection.

We have developed sophisticated and robust detection, triage, and analysis techniques for each. Without the collection of artefacts from **endpoint** and **external** sources, a comprehensive view of an attacker's activity (live and historic artefacts from endpoint data; potential exfiltration and command and control activity from endpoint data; sinkhole activity from external data) cannot be constructed.

1. Endpoint Threat Detection

With your IT teams, we agree on how to deploy a software agent most effectively and rapidly to your user and server systems and on a representative test population. This agent enables us to:

- Sweep every system for evidence of historical malicious activity (e.g. historical data exfiltration or lateral movement)
- Monitor real-time activity on the systems to detect any ongoing malicious activity
- Conduct targeted deep-dive analysis on specific systems to support investigative requirements
- Identify IT security weaknesses and areas of high risk.

2. External Threat Detection

We use PwC's proprietary malware domain sinkhole infrastructure solution to monitor for connections from client IP ranges through to malicious malware command and control domains we have been able to acquire.

When we identify malicious threat activity across endpoints, we seek to expand on that activity, to provide evidence-backed insights into the threat actor's capability, intent, and potential attribution.

Supporting research and technical data is included as appendices as part of our final deliverable.

Where our attribution can be taken further, to the level of personas or organisations, we will often document this detail or provide additional information via verbal or in-person briefings.

Core deliverables

- Comprehensive executive and technical report
- Identified threat overviews
- Spreadsheets of validated event data
- Recommendations