DXC Technology

Managed Endpoint Threat Detection and Response (METDR)

G-Cloud 15

Service Definition Document

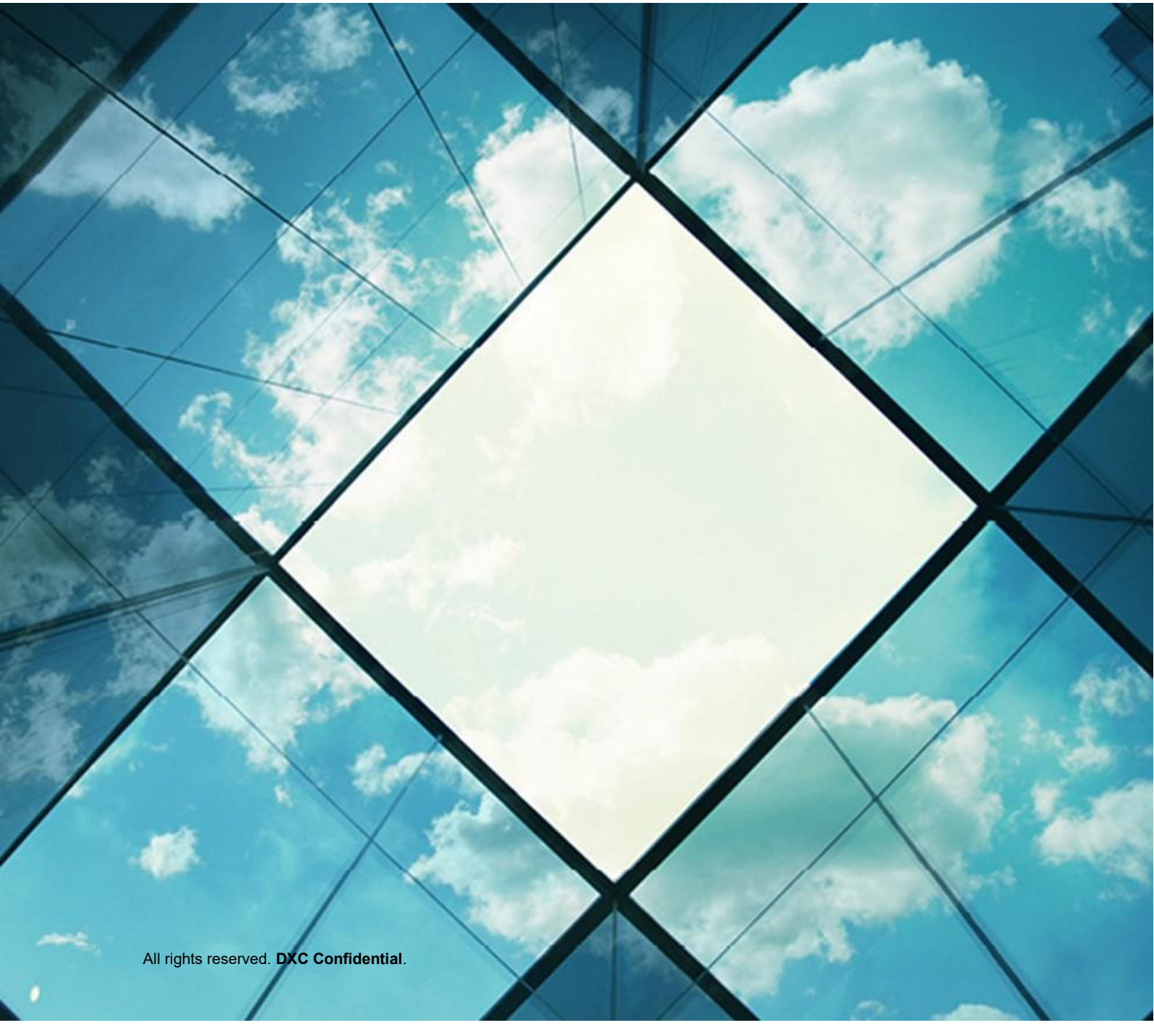

Table of Contents

1 Service Overview

Managed Endpoint Threat Detection and Response (“METDR”) proactively detects compromised Endpoint Devices (“endpoints”) in customer environments and assists in investigating and responding to compromise events. It is a cloud-based managed service powered by a third-party Software as a Service (“SaaS”) solutions, such as CrowdStrike and Microsoft Defender.

To detect and protect in-scope endpoints, METDR requires all customer-managed endpoints to have an Endpoint Detection and Response (“EDR”) agent installed.

EDR agents continuously collect endpoint activity data and send it to a cloud-based Management Console that serves as the data repository from which METDR manages, monitors, and reports on endpoints.

To analyse EDR agent data and compare it to predefined attack patterns, such as indicators of compromise (IOC) and indicators of attack (IOA), METDR uses behavioural-based detection, machine learning techniques, and threat intelligence. The service generates alerts and forwards those alerts to DXC’s Security Monitoring service, where they are monitored 24x7 and triaged, with response actions performed or recommended as required.

METDR consists of the following options:

- EDR Management, Monitoring, and Response
  - Requires Security Monitoring
- EDR Management only
  - DXC manages the EDR agent deployment and maintenance, but does not perform any monitoring or actions on events
- Incident Response and Threat Hunting
  - Add-on retainer for in-depth incident investigation and remediation of critical and widespread threats (e.g., data breach and ransomware).

2 Service Description

METDR is a cloud-based managed service that manages Endpoint Detection and Response (EDR) agents on customer devices, using behavioural analytics, machine learning, and threat intelligence to detect, investigate, and respond to threats. DXC provides 24×7 monitoring, incident management, reporting, and optional threat-hunting and incident-response capabilities.

- **Accelerated Detection & Response**: Reduces detection time from hours to minutes and containment from hours to seconds.
- **Reduced Operational Burden**: Offloads endpoint protection and response to DXC SOC.
- **Scalable & Customisable**: Supports both standard and custom delivery models for enterprise customers.

2.1 Service Features

Service features:

- System design and architecture for endpoint detection and response (EDR)
- 24×7 security monitoring and alert triage operations
- Threat detection using behavioural analytics and machine learning
- Managed configuration of EDR agents
- Incident investigation, containment, and remediation guidance
- Proactive threat hunting and analysis support
- Policy, allowlist, and denylist configuration management
- Standard and custom security reporting for customers
- Integration with DXC Security Monitoring services
- Support for CrowdStrike Falcon and Microsoft Defender platform capabilities

2.2 Service Benefits

Service benefits:

- Improves threat detection using behavioural analytics and threat intelligence feeds.
- Reduces business risk through continuous 24x7 security monitoring and triage.
- Accelerates incident remediation with targeted containment and response actions.
- Enhances threat visibility across endpoints with centralized cloud-based telemetry.
- Reduces deployment effort through lightweight, auto-updating endpoint agents.
- Streamlines policy management using console-based configuration controls.
- Improves operational efficiency with monthly summary and status reporting.
- Supports rapid threat hunting using predefined enterprise-wide query capabilities.
- Simplifies SIEM integration via standardized connector tooling.
- Reduces customer workload through fully managed EDR operations.

2.3 Value Proposition for UK Public Sector

- **Security and Compliance:** METDR provides robust, cloud-based endpoint protection that aligns with UK government security standards and data sovereignty requirements, helping public sector organisations safeguard sensitive data and maintain compliance.
- **Proactive Threat Detection:** The service offers 24x7 monitoring and rapid response to cyber threats, minimising the risk of disruption to essential public services.
- **Operational Resilience:** Advanced AI and behavioural analytics ensure critical services remain available, supporting the government's commitment to resilient digital operations.
- **Cost Efficiency:** By outsourcing security operations to DXC METDR, public sector bodies can reduce the need for large in-house teams, optimising resources and controlling costs.
- **Transparency and Assurance:** Regular reporting and alignment with public sector procurement standards provide clear oversight and build trust with stakeholders.
- **Scalability and Flexibility:** METDR scales to fit organisations of any size and offers customisable service options to match specific risk profiles and operational needs.

About DXC Technology

DXC Technology (NYSE: DXC) is a leading global provider of information technology services. We're a trusted operating partner to many of the world's most innovative organizations, building solutions that move industries and companies forward. Our engineering, consulting and technology experts help clients simplify, optimize and modernize their systems and processes, manage their most critical workloads, integrate AI-powered intelligence into their operations, and put security and trust at the forefront. Learn more on dxc.com.

Every day we deliver excellence for our customers and colleagues. We use the power of technology to deliver mission-critical IT services that move the world. Our customers entrust us to deliver what matters most. We are DXC.

An Employer of Choice

We inspire and take care of our people. We work to create a culture of learning, diversity and inclusion for all our people to grow and reach their full potential.

A Trusted Technology Partner

We understand technology and are committed to delivering excellence for our customers.

A Company that Cares

We are committed to improving the communities in which we live and work. We are good stewards of our company, our customers and the world.

Deliver Mission Critical

We deliver the mission-critical IT services that move the world.

Entrusted to Deliver

Every day, we earn our customers' trust by delivering transformative technologies to ensure the success, safety and well-being of businesses and people worldwide.

Delivery Excellence

Our delivery excellence gives planes flight, helps patients heal, and increases the scale and speed of commerce.

Deliver What Matters Most

We are proud of the work we do and the trust and confidence our customers place in us to deliver what matters most.

Learn more at

https://dxc.com/us/en/offerings/security

110 Pinehurst Road
Farnborough Business Park
Farnborough
GU14 7BF
United Kingdom

DXC.com

About DXC Technology

DXC Technology (NYSE: DXC) is a leading enterprise technology and innovation partner delivering software, services, and solutions to global enterprises and public sector organizations — helping them harness AI to drive outcomes at a time of exponential change with speed. With deep expertise in Managed Infrastructure Services, Application Modernization, and Industry-Specific Software Solutions, DXC modernizes, secures, and operates some of the world's most complex technology estates. Learn more on dxc.com.