DXC TECHNOLOGY

DXC Technology

Managed Endpoint Protection

G-Cloud 15

Service Definition Document

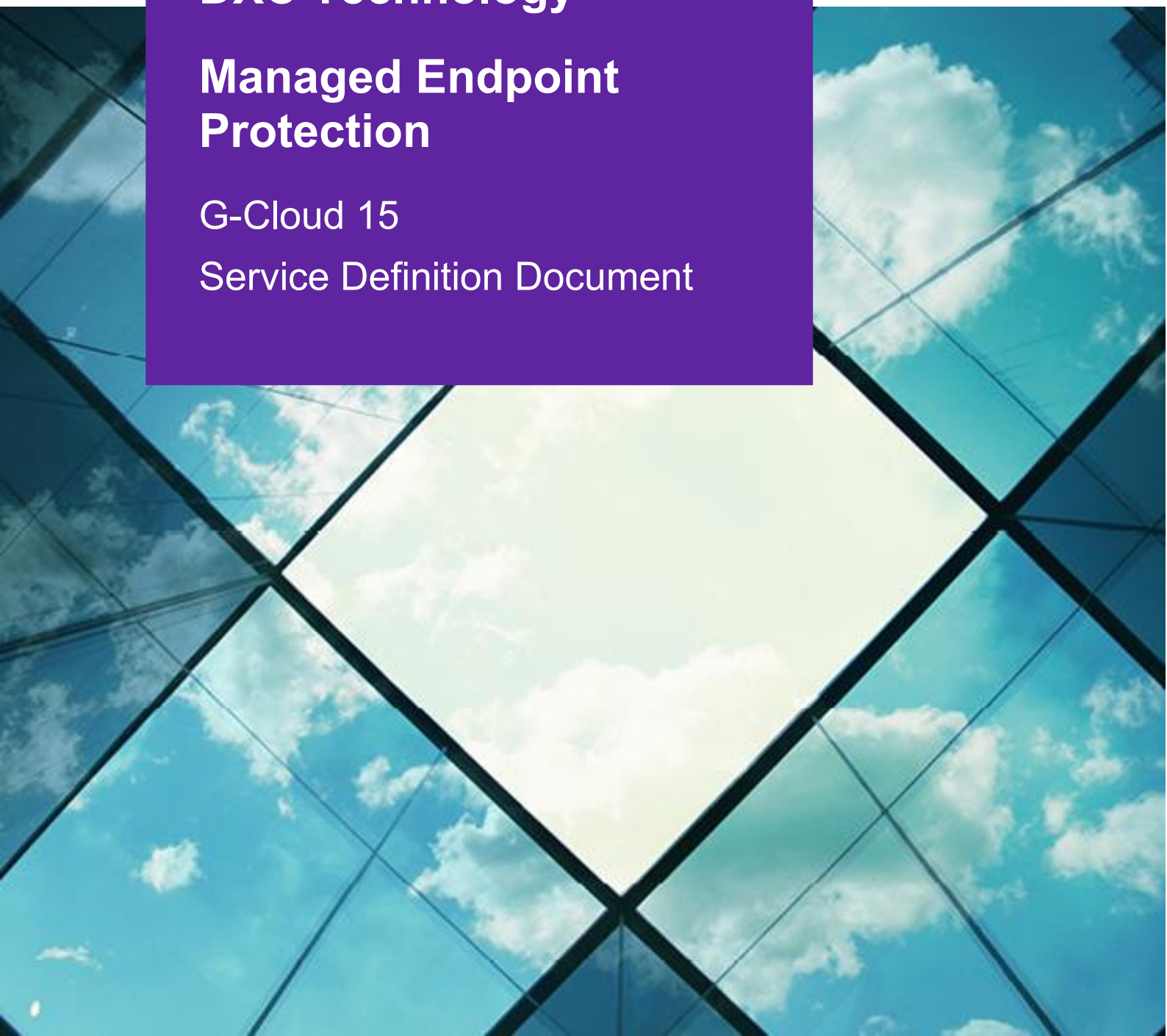


Table of Contents

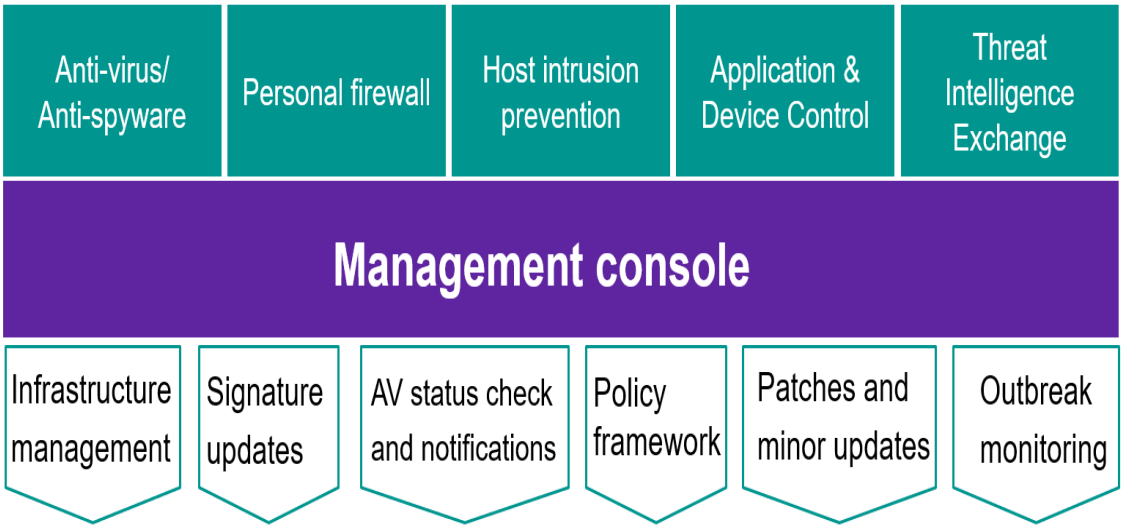
DXC Managed Endpoint Protection

1. Service Overview

Managed Endpoint Protection (MEP) is DXC's comprehensive managed service protecting desktops, laptops, VDI and servers from malware, ransomware, exploits and unauthorized access—combining prevention, detection, response, centralized policy management, continuous monitoring, and evidence-based reporting.

2. Service Description

2.1Service Features (Base)



- **Anti-Malware (AV/AS):** Real-time protection, scheduled scans, behavioural detection, ransomware mitigation, signature currency checks, automated remediation.
- **Personal Firewall:** Inbound/outbound application, port and protocol control with enterprise rulesets and exception workflow.
- **Host Intrusion Prevention (HIPS):** Behavioural & signature-based prevention, memory exploit mitigation, attack-surface reduction.
- **Application Control:** Allow/deny lists, script & binary execution control, optional workstation lockdown for high-risk users.
- **Device Control:** Governance of USB/Bluetooth/storage peripherals; data exfiltration reduction.
- **Adaptive Threat Protection:** ML-driven detection and dynamic containment for zero-day threats.
- **Advanced Threat Defence (Sandbox):** Dynamic/static analysis of suspicious files, automated reputations and response.
- **Endpoint Hardening Baselines:** CIS-aligned baselines (local admin, encryption, firewall, browser hardening), policy inheritance & drift detection.

- **Remote Response & Remediation:** Device isolation, kill processes, quarantine artifacts, runbooks, post-incident hygiene checks.
- **Operations & Governance:** 24×7 monitoring, incident triage, outbreak management, problem management, controlled changes.
- **Asset & Inventory:** Visibility to coverage, agent health, definition/update currency, protection components.
- **Threat Intelligence Integration:** Ingest sector-specific intelligence, enrich telemetry with reputations/IOCs, maintain customer-specific reputation knowledge base.

Operations Model & Integrations

- **Integrations:** SIEM/SOAR, ITSM/ticketing, CMDB, Identity (SSO/conditional access), PKI, UEM/MDM.
- **Data Flow:** Endpoint telemetry → MEP management console → SIEM correlation → SOC analyst actions/automations.
- **Onboarding:** Discovery → Design/policy baselines → Build → Pilot → Rollout → Hypercare, with design guide, operations guide and runbooks.

Reporting & Dashboards (Included)

- **Weekly:** Coverage & health; detections/outcomes; definition currency; exploit-prevention compliance; firewall deployment; application/device control events; sandbox submissions/verdicts; exceptions.
- **Monthly:** Threat trends; top risks/assets; compliance posture; unknown files & reputations; incident themes; audit evidence pack.
- **Near real-time:** Web dashboards with drill-downs; ad-hoc reports for audits/regulators.

2.2 Service Benefits

Risk Reduction

- Multi-layered protection combining anti-malware, firewall, intrusion prevention, application and device control, and advanced threat defence significantly reduces the likelihood of successful attacks.
- Continuous monitoring and proactive threat hunting minimize exposure to zero-day vulnerabilities and advanced persistent threats.

Faster Response

- Predefined playbooks and automated workflows enable rapid containment and remediation of incidents.
- Centralized telemetry and integrated dashboards provide real-time visibility, accelerating decision-making and reducing mean time to detect (MTTD) and mean time to respond (MTTR).

Compliance Support

- Built-in alignment with ISO 27001, CIS Benchmarks, NIST Cybersecurity Framework, and UK-specific standards such as Cyber Essentials and GDPR.
- Regular compliance posture reporting and audit-ready evidence packs simplify regulatory audits and internal governance reviews.

Operational Efficiency

- Standardized security baselines and automated policy enforcement reduce manual effort and configuration drift.
- 24×7 managed operations by skilled security professionals
- Internal teams to focus on strategic initiatives rather than day-to-day endpoint security tasks.

Visibility and Control

- Executive dashboards and technical reports provide clear insights into endpoint health, threat trends, and compliance status.
- Granular reporting by geography, business unit, and device group supports informed decision-making and risk prioritization.

Future-Ready Options

- Optional threat intelligence integration enhances detection capabilities with sector-specific indicators and global reputation data.
- Flexible architecture supports integration with SIEM, SOAR, ITSM, and identity platforms, enabling scalability and adaptability to be evolving security needs.
- Advanced analytics and automation capabilities prepare organizations for emerging threats and regulatory changes.

2.3Operation-Level Agreement (to be used as SLs only if required):

Incident Priorities

Priority	Business Impact	Operational Impact	Security Impact
Major	• Significantly impacts business operations • Directly impacts revenue	• Multiple resilient Devices or systems fail	• Security breach • Critical systems compromised • Sensitive data lost
High	• Impacts Customer business operations • Indirectly impacts revenue	• Single infrastructure system or management Device fails	• Non-critical systems compromised • Non-sensitive data lost
Medium	• Impacts business operations • Unlikely revenue loss	• Specific system Device feature is unavailable or malfunctions	• Moderate security risks and concerns

Low	• No business impact	• No operational impact	• False/positive • No security impact

Key Performance Indicators – Time to Own

Priority Category	Time to Own (TTO)	KPIs
Priority 1	15 Minutes	• > 95% - Green • 90% - 95% - Yellow • < 90% - Red
Priority 2	60 minutes	
Priority 3	4 hours	
Priority 4	24 hours	

TABLE – KPI – Time to Own

Key Performance Indicators – Definition Compliance

KPIs	Compliance for Servers	Compliance for Workstations
Green	>98%	>95%
Yellow	97%-98%	94% - 95%
Red	<97%	<94%

TABLE 5 – KPI – Definition Compliance

Key Performance Indicators – Definition Updates

KPIs	Update Compliance
Green	>97%
Yellow	95%-97%
Red	<95%

TABLE 6 – KPI – Definition Updates

2.4KPI Definitions

Time to Own (TTO)

- Time to own is defined as the time counted since a ticket arrives to the MEP queue till that ticket is assigned by an analyst.

Definition Compliance

- Every Anti-virus vendor releases new definition files on a regular basis. These definitions are downloaded to a Master Repository and then deployed to the environment supported by MEP. When a machine fails to update for several days (typically, 5 days) from the Master Repository, it is considered to be non-compliant.

  Note: This metric will only affect those systems that have been online in the last 24 hours and have not been in maintenance during that period.

Definition Updates

- Endpoint Security ensures that the Master Repository is downloading the definitions from the Anti-virus vendor site at least every 24 hours. That means that the

environment is protected against the latest threats discovered by the vendor during the last day. A daily check is performed to ensure that the definition has been updated in the Master Repository. This metric will measure the number of days per month when a definition update happened in a day/24 hours. For example, there was no update on the 18th of April. That was the only occurrence where the update failed during April.

- Failures: 1
- Total number of days: 30
- Update Compliance: (30-1)/30*100 = 96.67%

2.5Delivery Organizations

Managed Endpoint Protection is globally delivered by MSS MEP delivery team and provides several delivery Global Delivery Centre (GDC)/Best-shore solution. An on-shore solution is also available as an option.

Offshore / Nearshore: Bulgaria.

Onsite: UK.

2.6 Service Constraints

To ensure a smooth and effective delivery of Managed Endpoint Protection, the following prerequisites and considerations apply:

- **Supported Platforms:** The service is designed for modern, supported operating systems across desktops, laptops, servers, and virtual environments. This ensures optimal security and compatibility with advanced protection features.
- **Reliable Connectivity:** Continuous protection and policy enforcement require stable network connectivity for telemetry, updates, and centralized management.

Customer Responsibilities:

Scope Clarity: Hardware repair, custom application development, and OS patching are outside the scope of this service. However, DXC can coordinate with your existing teams to ensure seamless integration and governance.

Customization Options: Bespoke reporting, unique workflows, or specialized integrations can be delivered through a structured change request process, ensuring flexibility without compromising service quality.

3 Value Proposition for UK Public Sector

DXC Managed Endpoint Protection delivers unique advantages for UK public sector organizations:

- **Compliance with UK frameworks:** Full alignment with Cyber Essentials/CE+, GDPR, NCSC guidelines, ISO 27001, and CIS benchmarks.
- **Data sovereignty and residency:** UK-based delivery and storage options to meet government assurance and regulatory requirements.
- **Cost optimization:** Leveraged delivery model reduces total cost of ownership while maintaining resilience and security assurance.

- **Operational resilience:** 24×7 monitoring, outbreak playbooks, remote isolation, and rapid remediation ensure continuity of citizen services.
- **Audit and assurance readiness:** Monthly and quarterly evidence packs for internal audits, regulators, and governance boards.
- **Sustainability and green IT:** Cloud-enabled management reduces infrastructure footprint and supports government sustainability goals.
- **Innovation and futureproofing:** Integration with threat intelligence, advanced analytics, and automation to address evolving cyber threats.
- **Workforce enablement:** Secure remote working capabilities and compliance-driven endpoint posture for hybrid environments
- **Risk transparency:** Executive dashboards and compliance scorecards tailored for UK public sector governance frameworks
- **Rapid onboarding and scalability:** Proven methodology for onboarding large, distributed environments with minimal disruption.

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/cyber-defense