# OPSWAT MetaDefender Cloud

## Service Description for G Cloud 15

This Service Definition describes OPSWAT MetaDefender Cloud, a cloud-based cybersecurity service available via the UK Government G-Cloud 15 framework.

It is intended to provide public sector buyers with a clear understanding of the service scope, delivery model, security controls, resilience, and support arrangements.

Further technical and product information is available at www.opswat.com

## Service Overview

OPSWAT MetaDefender Cloud is a fully managed Software-as-a-Service (SaaS) platform designed to protect organisations from file-borne threats, including known malware, unknown threats, and zero-day attacks. The service enables secure file transfer, upload, download, and storage across cloud, SaaS, email, and web environments. It is designed to support public sector security, compliance, and resilience requirements.

## Service Description

MetaDefender Cloud provides multi-layered file security using complementary detection and prevention technologies. These include multi-engine anti-malware scanning, Deep Content Disarm and Reconstruction (CDR), adaptive sandboxing, threat reputation services, and Proactive Data Loss Prevention (DLP). Files are inspected and sanitised before being allowed into or out of an organisation's environment, reducing the risk of compromise or data leakage.

## Service Scope and Use Cases

The service supports a wide range of public sector use cases, including secure file uploads, email attachment scanning, protection of SaaS platforms, secure web gateways, and storage security for cloud repositories. MetaDefender Cloud can be deployed to protect inbound and outbound data flows and to support zero-trust security models.

## Service Delivery Model

MetaDefender Cloud is delivered entirely as a cloud-hosted service. OPSWAT is responsible for operating, maintaining, patching, and updating the platform. Customers access the service through secure APIs, ICAP-enabled devices, or supported native integrations. No customer-managed infrastructure is required.

## Service Constraints

The service requires internet connectivity and supported integration methods. There are no hardware or operating system dependencies for customers. Planned maintenance is performed by OPSWAT and communicated in advance where customer impact is expected.

## Availability and Service Levels

The service is designed for high availability using a resilient cloud architecture. Availability targets and service levels are defined contractually and vary based on the subscribed service and support tier. Service performance is continuously monitored.

## Resilience and Disaster Recovery

MetaDefender Cloud is hosted in secure, professionally managed cloud datacentres with resilient power, networking, and physical security controls. The service architecture avoids single points of failure through redundancy and automated failover. Backup, disaster recovery, and business continuity processes are in place and tested regularly.

## Security Governance and Compliance

OPSWAT operates a formal information security management framework aligned with ISO/IEC 27001 and SOC 2 Type II. Security governance includes defined roles, responsibilities, and escalation paths. Policies and controls are reviewed regularly to ensure ongoing compliance with regulatory and contractual requirements.

## Data Protection and Privacy

Customer files are processed solely for the purpose of threat detection, analysis, and sanitisation. Files are not retained beyond processing unless explicitly configured by the customer. Data in transit is protected using TLS version 1.2 or above. Role-based access controls restrict access to customer data and management functions.

## Vulnerability and Patch Management

OPSWAT maintains a formal vulnerability management process. Potential threats are identified using vulnerability scanning, threat intelligence feeds, vendor advisories, and security research. Patches and mitigations are prioritised based on risk and deployed following testing in controlled environments.

## Protective Monitoring

The service is subject to continuous protective monitoring to detect security events and anomalous behaviour. Monitoring outputs are reviewed and investigated by OPSWAT security

teams. Detected incidents are handled in accordance with defined incident response procedures.

## Incident Management

OPSWAT operates documented incident management processes with pre-defined procedures for common service and security events. Customers can report incidents via the support portal, email, or telephone depending on support tier. Incident reports are provided to affected customers as appropriate.

## Support and Customer Management

Support is available under Silver, Gold, and Platinum tiers, offering different response times and coverage levels. Support services are delivered through the OPSWAT support portal, chat, and telephone. Assigned customer success management is available under higher support tiers.

## End-of-Contract and Offboarding

At the end of the contract, customer access to the service is terminated. Configuration data and access credentials are securely removed in accordance with OPSWAT policies. Customers may request assistance with offboarding and transition activities prior to contract end.

## Further Information

Additional technical details, product documentation, and service information are available at www.opswat.com