Integrity360

your security in mind

Managed Endpoint Detection and Response

Service Description for G-Cloud 15

Table of Contents

Document Purpose

This is document serves as a high-level description of the Managed Endpoint Detection and Response (EDR).

The aim is to describe, in simple terms, the service, the deliverables of the service and the associated benefits. This is described in a non-technical and vendor agnostic way. More detail can be provided when engaging with our team so that we can understand your specific requirements.

- Please visit: https://www.integrity360.com
- Phone: +44 20 3397 3414
- Email: info@integrity360.com

1. Scope of Service

1.1. Introduction

Threats come in many forms, ranging from attacking networks, and systems right through to applications. Ultimately the endpoint is often the main target, this is due to the fact that a compromised endpoint can give you access to all of the above and more. Securing the endpoint is a priority for any business in this day and age, ensuring the correct level of security is applied not just for users workstations but also servers, mobiles and cloud based hosts.

Integrity360's Managed EDR service provides a highly tailored solution based on industry leading technologies, coupled with relevant threat intelligence information and a 24/7 continuous monitoring service of all managed endpoints. Customers' critical assets (workstations, laptops, servers, virtual machines, mobile devices etc.) are monitored in real-time and when a threat is observed, Integrity360 will inform the customer (based on the severity of the threat) and take the necessary actions to isolate and perform remediation where necessary. Support is provided across the various product tiers covering features such as NGAV, Anti-Spam, Anti-Spyware, Device and Application Control, Host Web Filtering, EDR, to name a few. Integrity360's managed service builds on all the product tier offerings, providing a comprehensive managed endpoint security service for the customer.

Key use cases delivered within our service tiers include, but are not limited to the following:

1. **Installation, Configuration and On-going Maintenance** – The installation and configuration of the chosen endpoint security solution as well as on-going maintenance of the endpoint software and configuration.

2. **24/7 Management and Monitoring** – The management and monitoring of all endpoints in real-time, ensuring visibility of any threats found and reducing the overheads for the customer in relation to having an in-house security team.

3. **Technical Support** – Support for all Endpoint Protection features ranging from NGAV, Anti-Spam/Spyware, Host Web Filtering, Host Firewalls and our EDR service.

Please refer to the table below for a summary of the available packages included in the Integrity360 Managed Endpoint Security Service Tiers:

Service Name	Details	Included
Managed Endpoint Protection (MEPP)	24/7 Management & Monitoring	✓
	Weekly & Monthly Reporting	✓
	Response & Resolution SLAs	✓
	System Availability Checks	✓
	Remote Malware Clean-Up	✓
	Console & Client Upgrades	✓
	Comprehensive Web Portal	✓
	Support for Next-Generation AV, anti-spam, anti-spyware, device control and application control features	✓
Managed Endpoint Protection Plus (MEPP+)	All the features of the **MEPP** service tier	✓
	Support for additional Endpoint Security features	✓
	Host web filtering	✓
	Content control	✓
	HIPS	✓
	Host Firewall and encryption (*subject to platform licensing*)	✓
Managed EDR (MEDR)	All the features of the **MEPP** and **MEPP+** service tiers	✓
	Full configuration and support for EDR functionality	✓
	Security alert monitoring, triage, notification and investigation	✓
	Integrated Threat Intelligence	✓
	Proactive response within agreed rules of engagement	✓
	Ability to integrate with wider Integrity360's Managed Detection & Response (MDR) service (*optional service*)	✓

2. Service Features

Integrity360 endpoint protection provides best-in-class managed endpoint protection (EPP) and endpoint detection and response (EDR) services for malware protection and remediation. The combination of telemetry from the EDR agents and human monitoring by our SOC team ensures excellent 24/7 coverage for customers' network perimeter. The offering includes a proactive service that searches for advanced threats on different targets (endpoints, servers, etc.).

The underlying platform for Endpoint Protection can be selected from a range of leading industry vendors with whom we partner.

2.1. Managed Endpoint Protection (MEPP)

- Management of the Endpoint platform and endpoint clients/agents including setup, configuration, and ongoing maintenance and upgrades.
- Monitoring and triage of alerts, filtration and elimination of false positives and notification of alerts of interest to the customer, under 24x7 SLA. Notified alerts will be enriched with environmental context, criticality assignment, and remediation recommendations.
- Weekly and/or monthly alert summary reporting.
- Remediation of threats discovered, ensuring all endpoints are safe to use with minimal interaction from the customer.
- Adhering to strict response and resolution SLAs ensuring the customer's endpoints are and remain protected at all times.
- Technical support for NGAV, Anti-Spam, Anti-Spyware, Device and Application control features.

2.2. Managed Endpoint Protection Plus (MEPP+)

- All the features of the Managed Endpoint Protection service.
- Host Web Filtering support on the endpoint. An additional service that provides the ability to filter malicious and non-work related web traffic.
- Content Control within Host Web Filtering. The ability to control the content within web filtering, allowing the customer to tailor the filtering solution to their business needs.
- Host Intrusion Prevention System (HIPS). An additional service that monitors the endpoint for any abnormal changes being made. This feature allows the customer to create a baseline of what normal activity should look like on their endpoints and then monitors for any deviation outside of the norm. Actions can then be configured based on the activity detected ranging from alerting, logging and resetting connections.
- Host Firewall & Encryption. Management of the endpoint's firewall, rule maintenance and review as well as the management of data/hard drive encryption on the endpoint.
- Technical support for all the features that are part of the Managed Endpoint Protection service as well as Host Web Filtering, Content Control, HIPS, Host Firewall & Encryption.

2.3. Managed Endpoint Detection & Response (MEDR)

- All the features of the Managed Endpoint Protection and Managed Endpoint Protection Plus services.
- Full deployment, configuration and management of the EDR platform across in-scope endpoints.
- Alert monitoring, triaging and investigations in real time.
- Proactive response of all alerts based on the rules of engagement agreed with the customer

3. Service Level Agreements

Level	Impact Description	Response SLA Time	Response Service Window	Customer Response Notification/Escalation Contacts and Method
P1 – Critical	Critical attacks that can lead to a validated compromise and have a significant impact on operations.	Responded to within 15 minutes	24 x 7	Customer E-mail Customer Telephone
P2 - High	High risk attacks that can lead to a validated compromise and have some impact on operations	Responded to within 1 hour	24 x 7	Customer E-mail Customer Telephone
P3 - Medium	Medium risk attacks that can lead to service disruption and have little impact on operations.	Responded to within 8 hours (1 business day)	8 x 5	Customer E-mail
P4 - Low	Low risk attacks that can't lead to service disruption and have no impact on operations	Monthly Reporting Cycle	Monthly Reporting Cycle	Customer E-mail
Service/Feature request	Request for execution of tasks not related to service degradation	Responded to within 1 business day to assess implementation effort required	Resolved within 5 Business days	Business Hours
Informational	They are presented for informational /reporting purposes	Monthly Reporting Cycle	Monthly Reporting Cycle	Customer E-mail

4. Next Steps

Work with us to ensure that your business maintains a proactive security stance in a field where new threats emerge daily. Contact an Integrity360 advisor today to learn more about our services.

www.integrity360.com