KYOCERA

Kyocera solution datasheet

Managed Endpoint Detection and Response (M-EDR).

Protect your business against the latest cyber threats with our (M-EDR) Managed Endpoint Detection and Response solution.

Overview.

Our Managed Endpoint Detection and Response (M-EDR) demonstrates another pillar of Kyocera's portfolio to encompass maximum cyber security. Utilising detection and response toolsets, coupled with Kyocera's knowledge and 24x7 expertise, delivers a human overlay to automated technology-based detection, analysis and response.

The solution leverages a market leading EDR platform using detection tools to monitor system configuration. Monitoring and alerts identify issues, which are then reported to the security operations team.

Analysts review security information provided by endpoint sensors which are deployed to all managed endpoints within an environment.

Kyocera's M-EDR services are a single component part of our much wider cyber security portfolio. Designed to improve and maximise overall protection and available to our customers to meet today's dynamically evolving cyber security landscape.

Key features.

Our M-EDR solution is available in different packages depending on the individual drivers and customers' expectations. The base option behind this solution, which we call 'Visual', includes the following service features:

- Onboarding
- Automated technology-based detection and analysis
- Proactive threat hunting
- 24x7 managed detection and response
- Root cause analysis, process containment, and remediation
- Application of industry-leading cyber threat intelligence for threat detection
- Experienced and professional security operations team
- Health, status, and availability systems management using the security platform
- Optional tuning and configuration
- Service reviews, threat insights and cyber security recommendations.

All subsequent levels of service expand on this base level, building to a pinnacle service.

M-EDR service packages.

Our M-EDR solution provides a comprehensive set of service packages that leverage the component features of leading technology platforms to perform endpoint threat prevention, detection and response. This enables remediation of malicious threats or anomalous activities within the customer environment.

The service packages are facilitated through the monitoring of the endpoints and workloads where a licensed sensor is installed, and collection of raw data that originates from these endpoints and workloads. Kyocera will apply policies, filters and correlate logic to the raw logs and endpoint data to identify potential security related events.

This service includes management of the EDR sensors, data collection, event normalisation/prioritisation, correlation, insights, and reporting.

Kyocera provides targeted M-EDR to a defined and authorised number of endpoints/workloads. To deploy the service, these endpoints must be enabled with the EDR sensor with the assistance of Kyocera Security Operations Team.
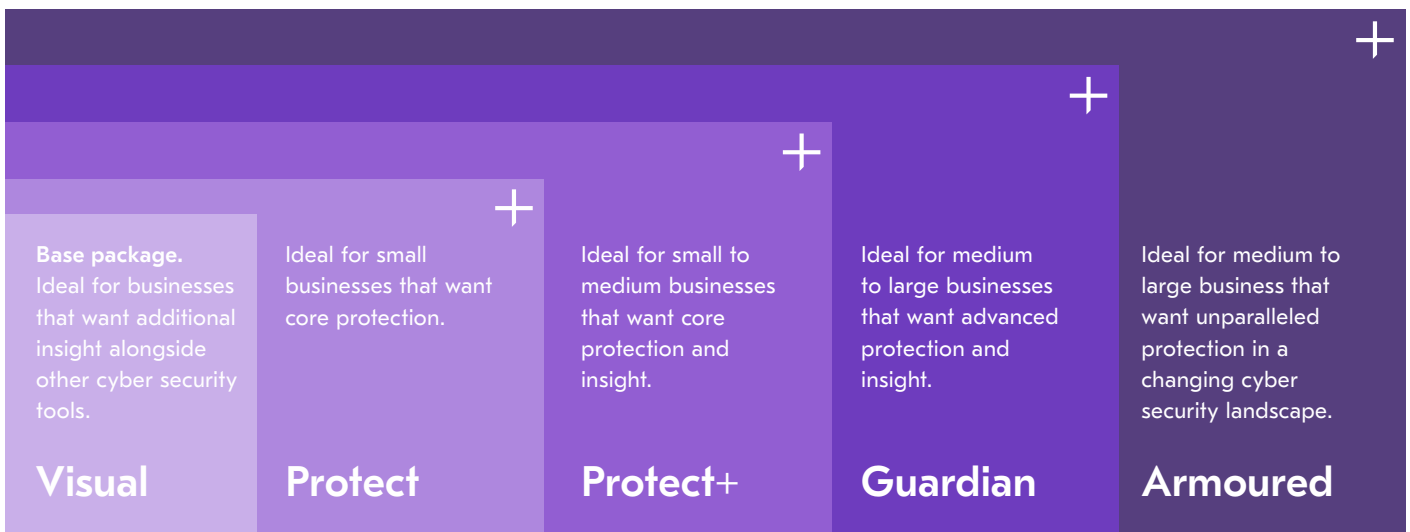
Kyocera offer five individual types of M-EDR package, each developed to be suitable for and tailored to different customer drivers and requirements. Our service solution varies based on selected requirements, the chosen service package, and help desk plan.

M-EDR service packages provide insights into areas of the ICT landscape that are vulnerable and not protected; they provide tailored services to maximise customers value utilising existing resources and skills sets. We do not include management or monitoring of any unsubscribed endpoint, workload, or intermediary log sources, and it does not include hardware, technology training for end users or engineering resources.

The fundamental philosophy behind our services is to prevent incidents before there is a need for response and remediation. With our insight reports and customer success journeys we work with customers to improve their overall cyber security position with a view to reducing or preventing threats.

Our five individual M-EDR service packages

Base package. Ideal for businesses that want additional insight alongside other cyber security tools.	Ideal for small businesses that want core protection.	Ideal for small to medium businesses that want core protection and insight.	Ideal for medium to large businesses that want advanced protection and insight.	Ideal for medium to large business that want unparalleled protection in a changing cyber security landscape.
Visual	**Protect**	**Protect+**	**Guardian**	**Armoured**

Kyocera aligns its service approach to the NIST Framework to ensure the maximum protection and aligned services for our customers.

		Visual	Protect	Protect+	Guardian	Armoured
Identify	Implementation	✓	✓	✓	✓	✓
	Configuration - Core Platform	✓	✓	✓	✓	✓
	Policy creation	✓	✓	✓	✓	✓
	Rule groups	✗	✗	✗	✓	✓
	IOCs & exclusions	✓	✓	✓	✓	✓
	Asset management	✗	✗	✗	✗	✓
	Platform updates	✓	✓	✓	✓	✓
	Platform access controls & auditing	✓	✓	✓	✓	✓
	Visibility	✓	✓	✓	✓	✓
	Base reporting	✓	✓	✓	✓	✓
	Base notification	✓	✓	✓	✓	✓
Protect	"AI", Policy response	✓	✓	✓	✓	✓
	Rules based action	✗	✗	✗	✓	✓
	Identity protect	✗	✗	✗	✓	✓
	Device control	✗	✗	✓	✓	✓
	Firewall control	✗	✗	✗	✓	✓
	Encryption control	✗	✗	✗	✓	✓
	Application control	✗	✗	✗	✓	✓
	BIOS control	✗	✗	✗	✓	✓
	OS control	✗	✗	✗	✗	✓
	File control	✗	✗	✗	✗	✓
	Threat hunting	✗	✗	✓	✓	✓
	Threat hunting quaterly insights	✗	✗	✗	✓	✓
	Vulnerability control	✗	✗	✗	✓	✓
	Headline vulnerability control	✗	✗	✗	✓	✓
Detect	Detections	✓	✓	✓	✓	✓
	Detection assign, comment	✓	✓	✓	✓	✓
	Vulnerability visibility	✗	✗	✗	✗	✓
	Vulnerability OS	✗	✗	✗	✗	✓
	Vulnerability third party	✗	✗	✗	✓	✓
	Identity Visibility	✗	✗	✓	✓	✓
	Device visibility	✗	✗	✓	✓	✓
	Network exposure (Domain IP)	✗	✗	✓	✓	✓
	Resource visibility	✗	✗	✓	✓	✓
	Encryption visibility	✗	✗	✓	✓	✓
	File visibility	✗	✗	✓	✓	✓
	Robotic process visibility	✗	✗	✓	✓	✓
	Threat intelligence	✗	✓	✓	✓	✓
	Detection enhanced detail	✗	✓	✓	✓	✓
	Actor profiling	✗	✓	✓	✓	✓
	Threat insights	✗	✓	✓	✓	✓
	Workflow	✓	✓	✓	✓	✓
	Standard workflow	✓	✓	✓	✓	✓
	Custom workflow additions	✗	✗	✗	✗	✓
	Custom alerting	✗	✗	✗	✓	✓
	Intelligence reporting	✗	✗	✓	✓	✓
	Personalised reporting	✗	✗	✗	✓	✓
Respond	Response policy - standard	✓	✓	✓	✓	✓
	Detection & incident response	✗	✓	✓	✓	✓
	Response custom scripting	✗	✗	✗	✗	✓
	Containment	✓	✓	✓	✓	✓
	Custom containment policy	✗	✗	✗	✗	✓
	Quarantine	✓	✓	✓	✓	✓
	Sandbox quarantine	✗	✗	✗	☺	☺
	Sandbox deep analysis	✗	✗	✗	✗	✓
	Dedicated security analyst response	✗	✗	✗	✗	✓
	Advanced response reporting	✗	✗	✗	✗	✓
	Threat graph standard	✗	✓	✓	✓	✓
	Threat graph +	✗	✗	✗	☺	☺
Recover	Host/workload recovery support	✗	✗	✗	✗	✓
	Dedicated security analyst recover	✗	✗	✗	✗	✓
	Express support	✗	✗	✗	✗	✓
	Advanced recover reporting	✗	✗	✗	✗	✓
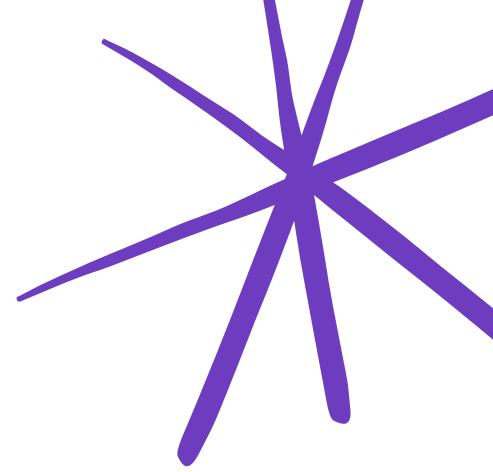
M-EDR services.

Identify

The identify process section of the NIST cycle sets out to baseline the core configuration of the environment.

Deployed during onboarding the team observe and learn the patterns, then adapt at this step to ensure the protection of the system.

The customer can feed into the identify phase during onboarding through the use of questionnaires and service operating model steps.

Please refer to Onboarding section of this document for further information.

Protect

The protect process lays down the control layer of the protection, it sets the controls in which the system pulls from the policies defined in the identify phase. Looking at vulnerabilities and active threat hunting the phase is critical to the prevent element of overall protection.

Set out in the identify process, the customer receives critical information, advice, and insights about their ICT landscape. This would be delivered to the customer quarterly or as and when relevant.

If the customer has subscribed to 'Threat Hunting' hunted threats will be logged as incidents should an indicator of attack (IOA) be detected within the environment. They will be available to the customer with alerts set out in 'Identify' and via the 24x7 portal.

See Proactive Threat Hunting Section of this document for further detail on our capabilities.

Detect

24x7 detection identifies attacks in your environment and prevents the spread of any malicious behaviour.

Using the insights from 'Protect' coupled with the rules, policies and understanding developed in Identify, our advanced security analysts can detect a wide range of attacks in your environment. Focusing on Indicators of Attack that may involve memory injections, executables, file changes, and registry modifications or malicious/unusual actions as well as traditional signatures and hashes, we have unparalleled detection capability.

We'll take care of security while you're taking care of business.

M-EDR services.

Respond

On potential signs of compromise, M-EDR utilises EDR at the endpoint to move or otherwise isolate questionable activities.

Our M-EDR service utilises several techniques should a detection occur, depending on the severity and type:

- Kill a process
- Kill network connections
- Upload logs from endpoint
- Ban a process
- Download files to endpoint
- Shutdown, restart endpoint
- Reverse shell on endpoint
- Run a script or PowerShell
- Quarantine files
- Contain endpoint

By subscribing to our M-EDR (at any service) package level, all customers provide authorisation and direction to remediation of known malware, attacks or detections. These include intrusions of any criticality affecting customers endpoints/workloads accessible to the Kyocera Security Operations Team. Further information is detailed in the operational process of the service.

Broadly governed under the posture approach, there are three distinct action levels, Active, Measured and Cautious. The Kyocera Security Operations Team will assess the situation and take the most appropriate action to protect your ICT systems based on the allocated posture level.

If a system is found to be labelled in the cautious posture Kyocera will seek approval where possible and it is in the customers best interest to respond in a timely manner to ensure that action can be taken by the Kyocera Security Operations Team.

Recover

The Kyocera Security Operations Team has established an intensive incident investigation process that provides for a consistent methodology of incident response analysis across all customer organisations.

As part of the recover activities our analysts can provide detail of the incident including IOA, points of entry, activities and compromised systems and files. This information will be dependent on the type of attack and approach of the attacked. Should a recovery of a system be required Kyocera can provide (subject to your chosen service package) a dedicated security analyst that will talk you through best practises of recovering workloads and/or endpoints.

The procedure of any recovery is subject to the type of attack and therefore it is not possible to define this element in detai. However our Kyocera Security Operations Team will work with the customer to provide as much information as possible to deliver an outcome whereby the customer may recover the affected hosts/endpoints.

We'll take care of securitywhile you're taking care of business.

Proactive Threat Hunting (Protect).

Kyocera will proactively search customers' environments with queries based on threat intelligence and research done on new and emerging threats and focus on indicators of behaviour and indicators of attack identified by research.
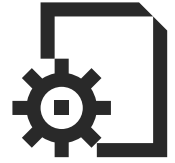
Tasks in this stage will include:

- Triage initial findings and expand investigation scope from hunting query searches to hunting lead ingestion.

- Where appropriate escalate the threat hunting investigation to an incident where standard incident processes would be adopted.

- Where not a direct incident, notify the customer regarding hunting findings within customers environment, which shall constitute confidential information of each of the parties via insight and customer success reporting.

- Threat Intelligence/insight report which details which hunting queries were created and provides a global overview of the threats for which the hunting queries were built.

Cyber-attacks are becoming more sophisticated and therefore active threat hunting is very important to improve overall protection. Any attacker who is on a known endpoint and/or with known identity/credentials will be very difficult for AI/technology to detect malicious action.

Through active threat hunting, human overlay and indicators of attack actions can be explored in more detail so that malicious behaviour can be detected.

Onboarding.

The Kyocera onboarding stage is an important step to successful delivery of the selected service. To start, Kyocera will conduct a live onboarding meeting, attended by our professional services and security operations resources.

Our onboarding playbook is used as a template, a guide for our activities rather than a rigid standard to onboarding, to accommodate the exact environment and requirements of a build. Tasks at this stage include:

Remote onboarding call

Conduct remote onboarding meeting to provide an overview of M-EDR to the customer and gather relevant M-EDR data to aid deployment activities.

Understand the customers current cyber security strategy and approach

- Understand the customers current security toolsets
- Understand the customers business activities
- Understand the customers personnel structure and responsibilities

Security questionnaire

Review the security questionnaire (provided in advance) to understand the customer's

- ICT environment including endpoints and workloads
- Administrative processes
- Service processes
- Current detection and response capabilities

Open Q&A

Provide a Q&A session to answer any customer questions specific to the selected M-EDR package.

Discuss package options

Discuss M-EDR package service operating model including:

- Communication plan
- Security stages
- Sensor update approach
- Incident playbooks

Onboarding timescales

Onboarding timescales will depend on detailed discussion with the customer and the project team. The onboarding timetable normally looks like the following (an example illustration and part of our onboarding playbook).

Step	Time
01. Contract executed	Day 0
02. Welcome email sent	48 hrs
03. Questionnaires sent	72 hrs
04. Onboarding call/meeting	1-3 days
05. Operating model template sent	1-2 days
06. Customer fills our operating model template	1-2 days
0.7 Sensors deployed and check in	TBC
08. Configuration begins	1-3 days
09. Operational	TBC
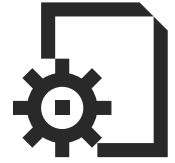
Onboarding.

Service activation

Service activation is performed during Kyocera core hours Monday to Friday 08:30 - 17:30 UK time (excluding bank holidays)

Activation may be performed at other times for an additional fee and with reasonable advance notice to Kyocera Professional Services and Project Teams.

Kyocera will use up to the first 30 days (subject to project plan) post-activation to identify a baseline policy and countermeasure of the customer environment and tune the service. Tuning is a process of factoring out some of the expected noise of the customer's environment and optimising the service to provide better visibility and anomaly detection.

This is part of Kyocera's three stage programme for technology and service adoption.

Activation stages, policies & countermeasures

Depending on the customer scenario, Kyocera aim to move through the three-stage activation programme within a given window.

Kyocera will work with the customer to determine any conflicting security tools that may need removing or reconfiguring as part of the service. Based on onboarding certain asset groups may remain in a stage as part of the end service.

Stage 01. →	Stage 02. →	Stage 03. →
Cautious	**Measured**	**Active**
Deploy, learn, and visualise providing insight into the environment that the Kyocera team can learn, understand, and discuss with the customer. a. Prevent "high"detections b. Investigate, analyse and remediate with approval	First stage prevention for known indicator of attack (IOA) and elements where false positives are the least likely. Advanced configuration and policies are deployed to implement second stage prevention, alerts, and insights. a. Prevent critical, high and medium detections b. Investigate, analyse and remediate based on pre-defined playbook	Full protection, maximum prevention, threat hunting and investigation through a tailored configuration, policies, and human understanding. a. Prevent all severity detections b. Investigate, analyse and remediate and reboot based on pre-defined playbook
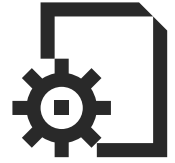
Onboarding.

Service baseline

During service onboarding, questionnaire and customer meetings, Kyocera will determine if the baseline security practises of the organisation are in place.

This includes but not limited to:

• Basic port blocking
• Privilege access control

If it is found that baseline security does not exist, then there may be an extended onboarding stage 1 and 2 cycle to ensure and provide the customer time to remediate their key practises and approach.

Where this is the case the project team may decide to take the service and remain at stage 1 and 2 for a longer period. This is project and customer specific and will be dealt with on a customer-by-customer basis and may result in reduced or removal of SLA commitments during this period.

Kyocera policies and asset groups

Asset group	Playbook posture	Assignment criteria	Sensor update policy	Always comms first
Workstations	Active posture	OS	Auto	No
VIP Workstations	Active posture	Machine name convention	Auto	No
Servers	Measured posture	OS	Defer 14 days	No
Critical servers	Cautious posture	CSV	Defer 14 Days	Yes

Service approach.

Advanced endpoint protection (Sensor)

Through service onboarding, Kyocera will provide a sensor (for the customer to deploy or alternatively for Kyocera to deploy at an additional charge) to enable the necessary capabilities and functionality for M-EDR. This sensor will be wholly managed by the Kyocera Security Operations Team, including policies for Prevention, Detection, Alerting, and Response capabilities.

The sensor will provide next generation anti-virus/anti-malware, along with heuristic and behavioural detection and prevention for advanced threats. Kyocera provides initial policies based on our experiences of your sector, size, and environment. Those policies are applied immediately on deployment and are monitored for tuning or tweaks which may be necessary based on specifics of the customer systems.

Log/data collection

Within our M-EDR, we will deploy and configure sensors on customer's devices for collecting logs, as initially scoped with customer. Kyocera will provide configuration through a consolidated sensor installer, and work with the customer on any customer log aggregator/forwarder devices to apply appropriate filters to the raw log data if required.

Logs/data are collected and forwarded to the elected technology platform for processing, analysis, and management.

Coverage of all log sources so that logs are appropriately sent to the sensors and log collection areas are the responsibility of the customer. Kyocera will work with the customer to ensure any unknowns are highlighted. This includes, but is not limited to, any intermediary log sources. If changes to customers existing network architecture are required for service implementation, Kyocera will communicate these changes during onboarding.

Communication

Kyocera seek to streamline communication to maximise protection whilst providing the customer maximum visibility.

Alerting

Alerting is segregated into different categories traditionally defined as advisory, low, medium, high, and critical. When an alert is detected, the customer will be notified where appropriate by Kyocera Security Operations Team as defined in the onboarding process and within the service levels.

In some cases, for example low or advisory alerts, these will be logged and included in insight or service review reporting for the customer visibility and will also be available live time in the customer portal.

Where the alerts are of critical or high nature and the onboarded, processes indicate to do so the team will reach out via phone/email to the customer to inform them of a situation and or actions taken.

Where the customer service package includes Kyocera will also perform additional analysis to determine whether a security event indicates a security compromise. Following the application of remedial actions, Kyocera will provide a description of the event(s), and any contextual information identified during the investigation.

Service approach.

Reporting

Standard reporting is included with all levels of M-EDR, providing visibility on alerts and incidents raised by the technology and/or Kyocera Security Operations Team.

Depending on the service package and the technology modules selected, the customer reporting may also include other insights and alerts, for example, login activity and patch status.

Reporting is reliant on appropriate data and logs from the customer, and if such data is not available, Kyocera will be unable to produce the listed reports.

Kyocera standard reporting is there to provide key insights and updates to customers in most cases. Custom/personalised reporting is available under select packages and will be defined during the onboarding process from the Kyocera catalogue of available reports.

As standard the service packages include one or selected reports below.

Standard reporting

- Per incident or advisory email (see how we communicate)
- Monthly overview of incidents, advisories and KPIs/metric

Personalised reporting

- Per incident or advisory email
- Monthly overview of incidents, advisories and KPIs/metric
- Monthly tailored insight report
- Quarterly landscape report and service overview

KPIs/metric are defined as the following in both standard and personalised reporting.

KPI
- Incident, advisory and request - Response SLA
- Average time to triage
- Average time to remediate

Metric — Sensor health within environment
- Endpoint split
- Total
- Active vs inactive
- Configuration health and deployment

Metrix — Detections
- Low, medium, high, critical

Metric — System remediations

Kyocera seek to ensure reporting provides value to the customer within the standard reporting approach of the organisation. Kyocera under the right service package can tailor reporting based around the services it provides to the customer requirements.

Kyocera Document Solutions has championed innovative technology since 1959. We enable our customers to turn information into knowledge, excel at learning and surpass others. With professional expertise and a culture of empathetic partnership, we help organisations put knowledge to work to drive change.

KYOCERA Document Solutions (U.K.) Limited

Eldon Court
75-77 London Road
Reading
Berkshire RG1 5BS

Tel: 03330 151855
e: info@duk.kyocera.com

kyoceradocumentsolutions.co.uk

A Kyocera Group UK Company

Annodata Ltd.
The Maylands Building, Maylands Avenue
Hemel Hempstead
Hertfordshire HP2 7TG

Tel: 03330 151856
e: sales@duk.kyocera.com

kyocera-annodata.co.uk