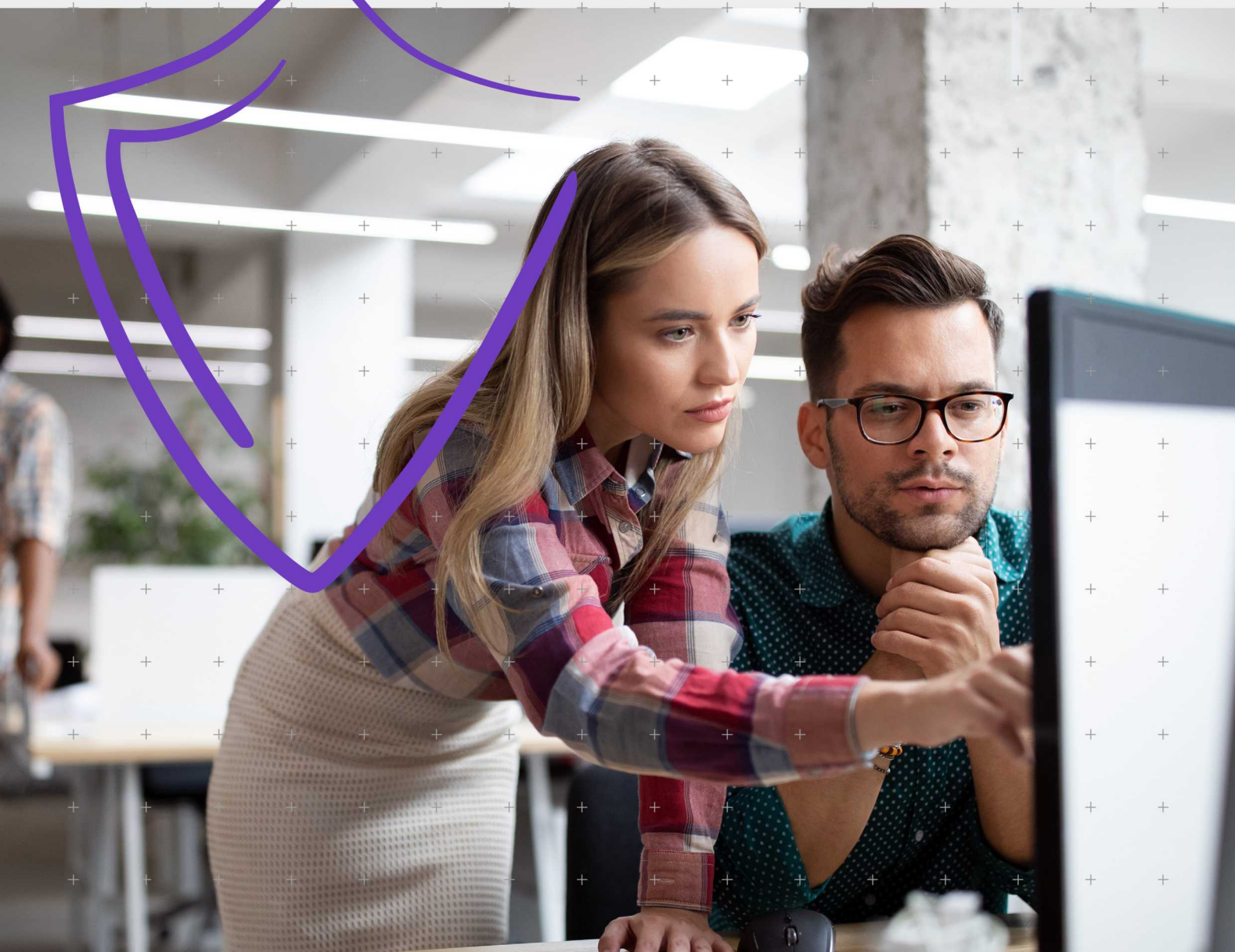
KYOCERA

kyoceradocumentsolutions.co.uk

Managed Endpoint Detection and Response (M-EDR).

M-EDR protects against ransomware, zero-day malware, fileless attacks, phishing and more.



Managed Endpoint Detection and Response (M-EDR).

Ensure your business has comprehensive protection. Now and for the future.

Our Managed Endpoint Detection and Response solutions protect businesses of all sizes from all current and future cyber threats. A fully managed cyber security service, it ensures that your IT teams are free to focus on more strategic business goals.

The best-in-class Endpoint Detection and Response solutions are fully managed, delivering a human overlay to technology-based, automated detection, analysis and response software.

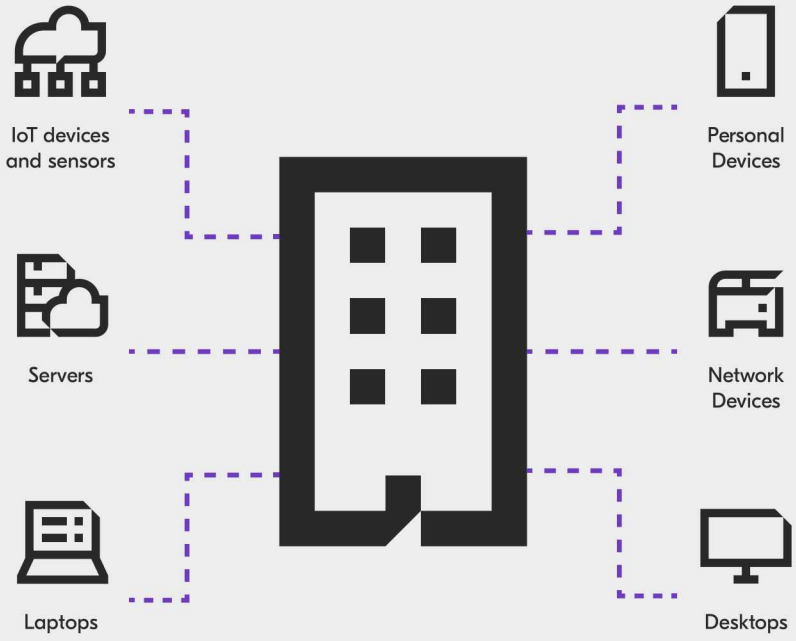
Our team monitors and manages system configuration, policies and alerting provided to the security operations teams. The solution also provides 24x7 proactive threat detection capability and enables the Kyocera teams to provide analysis and response (remediation) activities.

Industry analysts review security information provided by the managed endpoints and other monitored systems within the customer environment. Multiple threat intelligence feeds to quickly respond and remediate at the root cause.

What is an endpoint?

Put simply, an endpoint is any device connected to a network.

Now, you're probably thinking of laptops, phones and PCS, right? However, even your company fridge and microwave could be an endpoint and posing yet another threat gateway to your business.



Managed Endpoint Detection and Response solutions.

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

Visual.

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
+ Application of industry-leading cyber threat intelligence for threat detection
+ An experienced and professional security operations team
+ Optional tuning and configuration
+ Health, status, and availability systems management using the security platform
+ Root cause analysis, process containment, and remediation
+ Service reviews, threat insights and cyber security recommendations.

Each subsequent solution builds on this base level, leading to the pinnacle of cyber security...

Why Managed Endpoint Detection and Response?

We align with leading cyber security best practices and frameworks to ensure we deliver a portfolio of services that meet the ever-changing threat landscape.

NIST Cyber Security Framework is one the most well-known frameworks and follows the five functions/pillars of the cyber security program.

We align our services against these defined pillars to ensure maximum protection and referenced architecture.

Our solutions provide insights into areas of the ICT landscape that are vulnerable and not protected while providing tailored services to maximise existing resources and skill sets.

The fundamental philosophy behind our services is to prevent, before the need to respond and remediate. Through our insight reports and customer success journeys, we work with customers to improve their overall cyber security position with a view to preventing or reducing threats.

The key benefits of Managed Endpoint Detection and Response:

Reduced complexity.

The burden of threat-hunting is taken away from the end user and a root cause analysis of any attack is provided so businesses understand why cyber criminals attacked and how to prevent a recurrence.

Stay ahead.

New software security threats emerge daily, putting your data at risk... Get ahead of any new threats and stop attacks before the breach to save on recovery costs and a loss of reputation.

Maximum security.

Behaviour-based protection and proactive response tools to safeguard your system, allowing the cyber security team to address the root cause of the issue, kill or quarantine the threat, and remediate or roll back the system as needed.

Better protection.

Protect against all types of attacks, from commodity malware to ransomware and other sophisticated attacks. All from one solution that prevents silent failure.

Our solutions are built on the following NIST Cyber Security Framework foundations.

Identify.

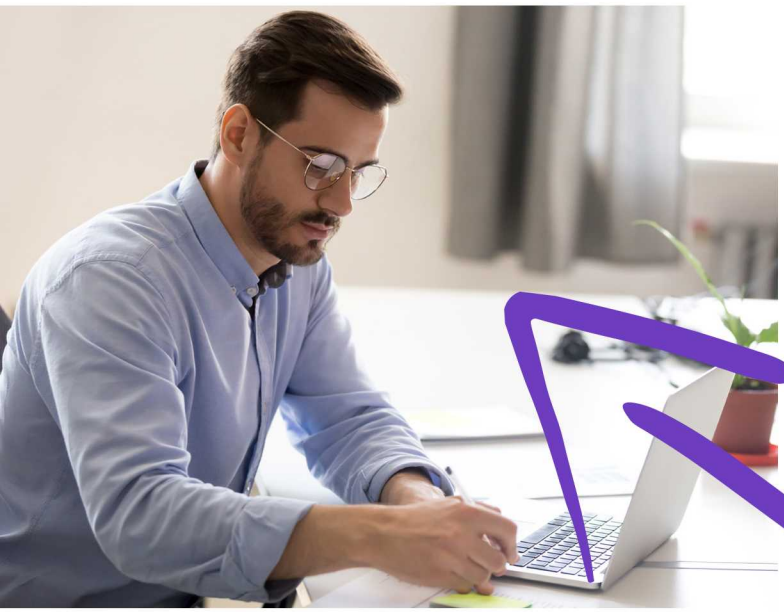
The identity process sets out to baseline and set the core configuration of the environment. This is often built during the onboarding phase and tweaked as the system and team learn the Identify steps that represent an important step in the protection of systems. The customer can feed into the Identify phase during onboarding, questionnaires, and service operating model steps.

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.

Detect.

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.



Respond.

On potential signs of compromise, M-EDR utilises EDR at the endpoint to move or otherwise isolate questionable activities. M-EDR service utilises several techniques should a detection occur, depending on the severity and type:

+ Kill a process
+ Shutdown, restart endpoint
+ Kill network connections
+ Reverse shell on endpoint
+ Download files to endpoint (exe, patch, etc.)
+ Upload logs from endpoint
+ Run a script or PowerShell
+ Ban a process
+ Quarantine files
+ Contain endpoint

Recover.

As a part of the Recover activities our analysts can provide detail of the incident including IOA, points of entry, activities and compromised systems and files. Should a recovery of a system be required, we can provide (subject to your package) a dedicated security analyst that will talk you through best practices for recovering workloads and/or endpoints.

The detail of any recovery is subject to the type of attack and therefore it is not possible to define this element in detail. However Kyocera 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.

Why do you need Endpoint Detection and Response?

The evolving threat and sheer volume of security alerts mean it can be hard for IT teams to keep up particularly when using legacy anti virus technology which is reliant on existing knowledge of threats and relevant definition file. This can put critical business operations at risk and potentially cause irreparable damage.

Finding the right skills, and retaining experienced cyber security professionals has become a major obstacle for businesses of all sizes; especially when a 24/7 security resource is needed.

Whereas antivirus only provides detection and response to malware on an infected endpoint using a variety of different techniques, EDR incorporates Next Generation AntiVirus and other endpoint security functionality. This provides full protection against a wider range of potential threats via AI learning in the cloud.

Have you got full visibility? Or are you vulnerable?

Imagine you're a CEO, chances are that you're aware of the increasing number of cyber incidents in recent years, but they always seem a little far from home, they would never happen to you, right?

One Friday afternoon, just after lunch one of your employees clicks the link on the innocuous-looking link on an email they received, apparently from a legitimate source They've just fallen victim to a classic phishing email and just like that, from an employee's action on a single endpoint, your entire network is infected with ransomware.

You're now given 48 hours to pay the ransom in order to gain access to your newly encrypted files. The problem is it's already Friday afternoon and the technical support team for your Endpoint Detection and Response system has clocked off for the weekend...

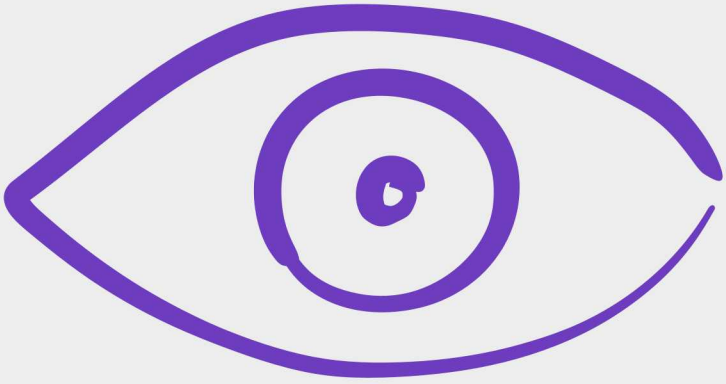
By Monday morning the ransom has been paid, but they've still not released the encryption key for your files. Now not only have you paid the ransom and incurred a significant financial loss, but you're also losing time, only adding to the total losses associated with clicking a link on a single email...

Now imagine an alternative scenario where you're using one of our Managed Endpoint Detection and Response solutions... Our team of experts are on hand to provide assistance, even though it is late on a Friday afternoon (they're available 24/7 in case you were wondering).

Rather than the threat going undetected and the ransomware gaining access to your systems, our software automatically detects the malicious intent, either killing or quarantining it.

You are now able to roll back or remediate the system as needed, ensuring no damage is caused. Then you will be sent a detailed report, providing insight into how and why the attack occurred, allowing you to understand the reasons behind it and educate your team accordingly.

In this scenario, you are now free to enjoy your weekend in peace!



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