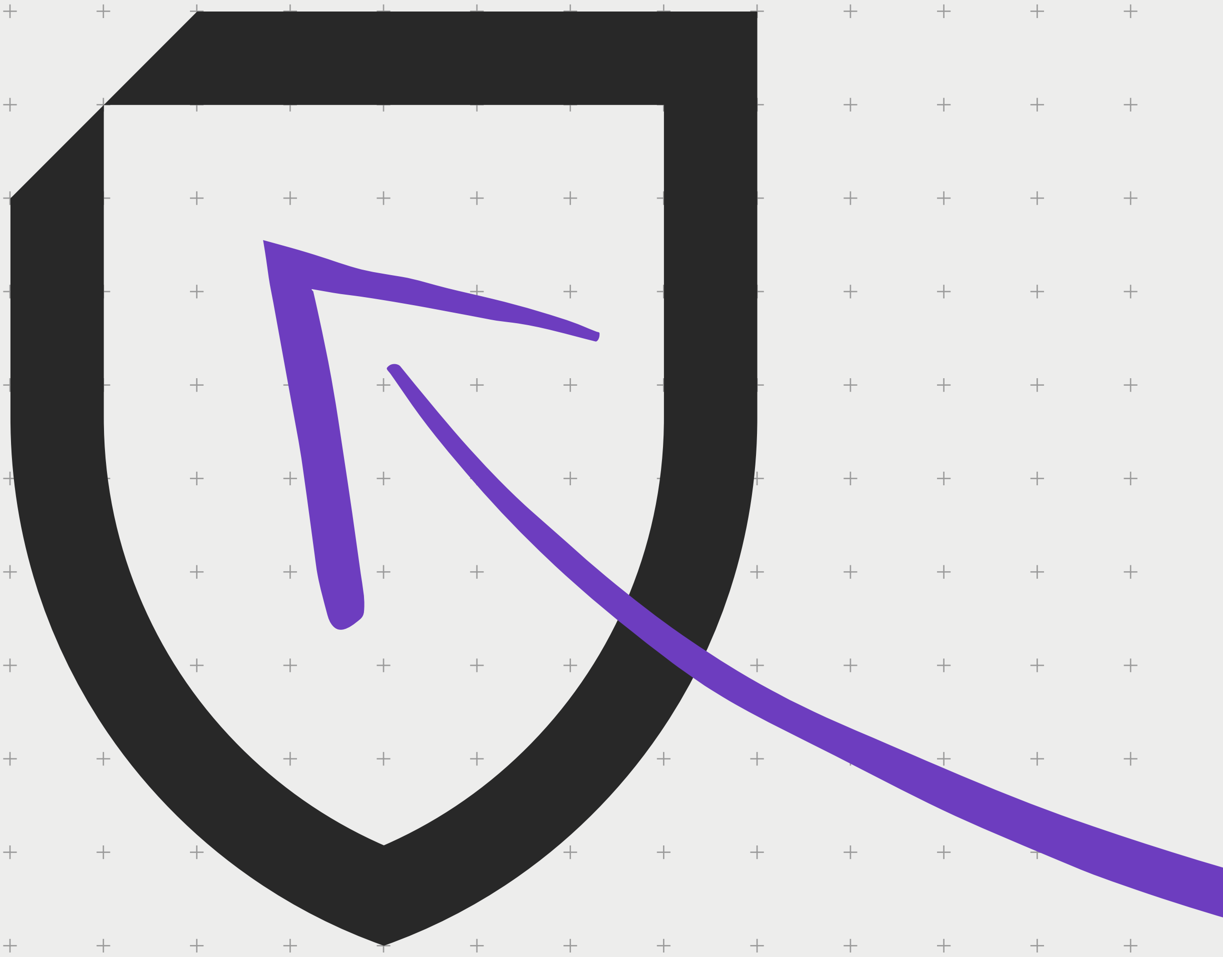
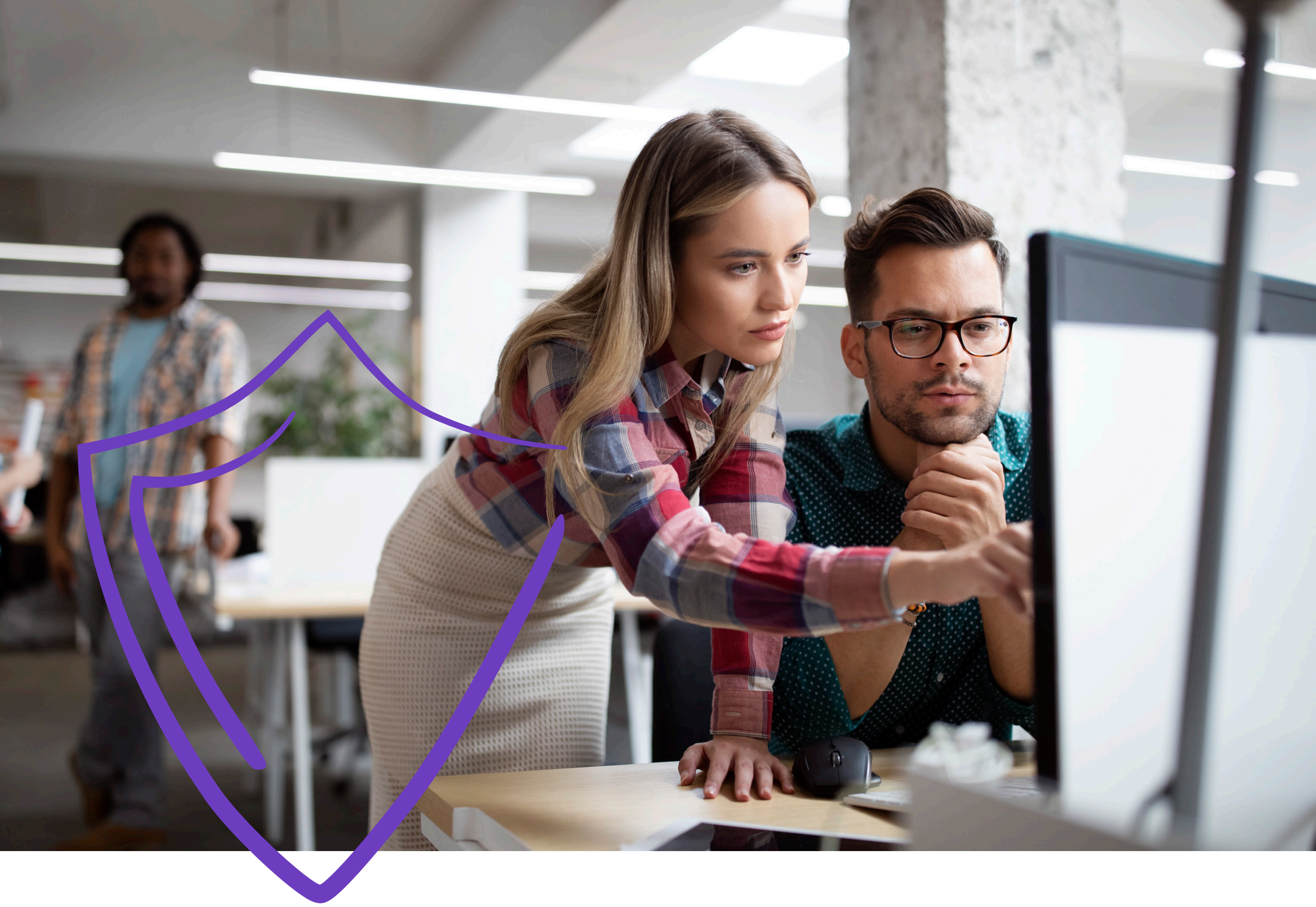
kyoceradocumentsolutions.co.uk

# Complete guide to Managed Endpoint Detection and Response (M-EDR).



# Contents.



# Cybersecurity Systems Evolved with EDR.

**Protecting your networks from current and future threats is essential, and having a layered security system is the best defence.**

This means you have two choices; either Antivirus (AV) or Endpoint Detection and Response (EDR).

While both have their merits and use the same resources, some key features make EDR the clear frontrunner. Malware has evolved, meaning cybersecurity systems and solutions must do as well, which is why EDR goes that one step further to secure endpoints and personal information within your  IT estate.

While Antivirus covers a single endpoint to detect and block malicious files, EDR protects your entire network against security attacks by detecting and responding to threats before they cause significant damage to your endpoint.

And when it's a case of choosing either one or the other for your organisation, EDR provides the functionality of Antivirus and goes above and beyond to offer users a host of additional features, making the choice seem pretty obvious.

# Gaps to be aware of: Endpoint vs Antivirus

**Protecting your networks from current and future threats is essential, and having a layered security system is the best defence.**

Although Antivirus provides good protection at a reasonable price point in discovering and quarantining malware, it relies on regular definition (virus signature) updates. Therefore, it is only as effective as the vendor controlling the updates. And with new cyberthreats arriving daily, the next update might take longer to prevent damage. Studies have shown that there has been an 82% increase in ransomware related data leaks during 2021.[1]

For years, cybercriminals have tried to get around antivirus software by using evasion techniques such as malware encryption or changing a signature on a set cadence to slip through the net.

Unlike Antivirus software, Endpoint Detection and Response solutions do not need input from the end user. Instead, they use artificial intelligence to identify and address all suspicious activity before it can cause harm, rather than just focusing on files.

Endpoint Detection and Security includes real-time monitoring and detection of threats that may not be easily recognised or defined by standard antivirus. It is behaviour based so that it can detect unknown threats based on abnormal behaviour.

Data collection and analysis will determine threat patterns and alert the organisation to these threats. When there is a security event, forensic capabilities help to determine what has happened, how it happened and how to prevent it in the future. Any infected or suspicious items are isolated and quarantined to prevent them from infecting other things, and automated remediation or removal of specific threats is included.

> **“Every business is at risk of cyber attacks, which makes it even more critical to protect your systems using an up-to-date and modern cybersecurity solution that excels in areas where antivirus software falls short. Endpoint detection and response solutions have been developed and brought to market specifically to address evolving cybersecurity threats.”**

**Andrew Smith, Group Chief Information & Strategy Officer (CISO) at KYOCERA Document Solutions UK.**

[1] CrowdStrike - Global Threat Report 2022

# How can EDR benefit your business?

**Cybersecurity threats to organisations are steadily increasing, and there is no room for complacency. Businesses across the globe must continue to innovate to give customers' data the best possible protection.**

Kyocera's Endpoint Detection solutions provide cutting-edge protection in an ever-changing and evolving digital and cyberthreat landscape.

With each new cyberthreat that emerges, Antivirus software slowly becomes less and less effective, leaving you more exposed and at risk. Endpoint Detection and Response is a multifaceted and adaptable solution that expands on traditional Antivirus software, taking it to the next level regarding security and peace of mind. Here's what's included:

+ AI and machine learning provides proactive detection, allowing the cybersecurity team to address the root cause of the issue, kill or quarantine the threat, and remediate or roll back the system as needed.
+ A root cause analysis, so you understand why you were attacked by cybercriminals and how to prevent a recurrence.
+ The opportunity to quickly remediate threats, rolling back to a known safe state.
+ New software security threats emerge daily, putting your data at risk.
+ Traditional Antivirus software has significant shortcomings against modern and sophisticated threats.
+ EDR offers behaviour-based protection and proactive response tools to safeguard your system, unlike traditional antivirus software that relies on prior knowledge of the specifics of the malware or cybersecurity attack.

There has been a rapid increase in the number of endpoints and their connectivity in recent years. Coupled with the rise in malicious activity, this means that more and more businesses are being targeted in cyber attacks.

Traditionally, only the largest and best-funded corporations have had access to expert Endpoint Protection skills. Now, most attacks are more complex and happen at machine speed, which has left human teams relying on Antivirus systems unable to keep up.

The answer is simple: A modern Endpoint Detection and Response system that equips security teams with the right tools to confidently deal with these challenges by automatically and proactively detecting and blocking malware or threats.

# Alert management, threat hunting.

**The ability to learn from the baseline behaviour of an endpoint is one of the key characteristics of an Endpoint Detection and Response solution.**

Should any endpoint behaviour drastically differ from the norm, questions are asked like:

+ Has this endpoint performed this activity before?
+ Are unusual patterns being exhibited by this behaviour or file?
+ For example, why are cyber criminals' secure files being hit or looked at?

One of, if not the most critical aspects of a modern Endpoint Detection and Response solution is threat hunting. These solutions are proactive rather than reactive, like Antivirus systems.

The automated nature of threat allows analysts to use data mining to automatically target threats that hold similarities - both on behavioural and functional levels - to previous attacks, with almost instantaneous results. For analysts to save time and expedite the process, results should be displayed in an easy-to-understand format, such as a graphical user interface (GUI).

# Understanding vulnerabilities in an IT system.

**Cyber attacks are constantly evolving in sophistication and scale, reaching such an extent that the World Economic Forum reported a 435% increase in ransomware in 2020.[1]**

The main issue is that computer software is rarely, if ever, perfect and completely free from bugs, glitches or vulnerabilities, which can be very dangerous if discovered by the wrong people. For example, using a company's IT infrastructure vulnerability, a cyber attacker can gain unauthorised access to a computer system to run malicious code, install malware, or steal sensitive information.

In a recent survey, the IDC found that around 70% of respondents had suffered downtime as a result of DNS (Domain Name System) attacks, with an average cost of $942,000 per attack.[2]

In this case, lost productivity will significantly impact the business. It will take several hours to reimage a computer, and the employee's computer would be out of commission each time. For example, it takes 2 hours to reimage a computer, and the employee is without a computer for 2 hours. Across the 1,000 infections per year, a business could lose 4,000 hours of productivity when you factor in the IT departments time.

Moreover, ransomware attackers commonly try to disable backups and disaster recovery. Statistics show that 75% of ransomware incidents involve data theft, with 21.4% of those incidents involving valuable, sensitive, or confidential data being compromised.

Less than one-third of organisations are about to recover financially on their own from a ransomware attack with data breaches costing companies around $4.27m on average. Although Endpoint Detection and Response solutions have a (slightly) higher initial cost to anti-virus software, reduced infections and increased security more than pay for themselves over a year (in some cases, even as little as a month!).

If your business could do with a data backup strategy, our fully managed  Kyocera Protect service makes backing up and restoring valuable software data quick, easy, and cost-effective without compromising data integrity and compliance.

> **"By using a next-generation Endpoint Detection and Response, businesses can cut malicious infections down to just one or two a month. The savings in lost productivity quickly justify the additional initial investment."**

**Andrew Smith, Group Chief Information & Strategy Officer (CISO) at KYOCERA Document Solutions UK.**

[1] WEF The Global Risks Report 2022

[2] IDC 2022 Global DNS Threat Report

# The evolving threats to cybersecurity.

**Each of these cyberattacks represent a clear and current danger to your business; many of these can slip past traditional Antivirus solutions.**

## Ransomware

**Malware that denies the user or organisation access to their files by encrypting them.**

Unfortunately, the best and easiest way to deal with ransomware is to pay the ransom to release the decryption key. Either the computer itself will become locked, or the data stored on it could be stolen, encrypted or deleted. Some types of ransomware also attempt to spread to other endpoints in the network.

## Zero-day malware

**The vulnerability within a systems code has been there since the day of the code release.**

It is called zero-day, as often the vendor will rush to update the code and release an update to rectify the issue. However, there are "zero days" to fix it if it has already fallen into the wrong hands.

## Fileless attacks

A form of malicious code, this type of malware does not need an executable file on the endpoints system besides those that are pre-existing. Typically they will only execute in RAM, meaning they have a low footprint and are very hard to detect.

## Phishing

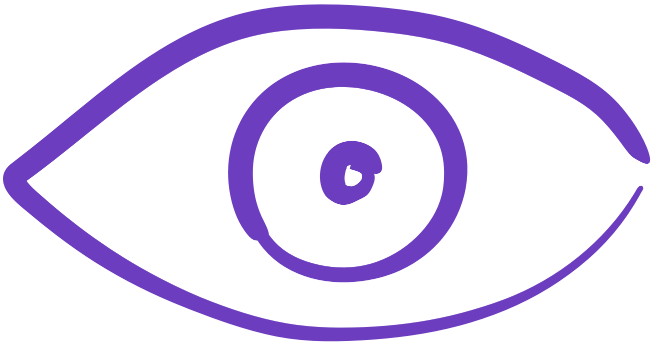
Typically a 'human error', phishing relies on the user doing the wrong thing, with the intention being to trick them into clicking a malicious link, either to download software or to take them to a particular website.

## Privilege escalation

Attackers aim to exploit human behaviours or operating system oversights/design flaws to gain unauthorised access to privileged information within a system.

**"Endpoint Detection and Response solutions have been developed and brought to market specifically to stop current and emerging cyber-attacks. An organisation is only secure from the likes of ransomware and malware if every asset is protected. You must secure all critical areas of enterprise risk: endpoints and cloud workloads, identity and data."**

**Andrew Smith, Group Chief Information & Strategy Officer (CISO) at KYOCERA Document Solutions UK.**



# Do you face any of these business challenges?

**Businesses today face several cybersecurity challenges, and ensuring that each is met could be the difference between a cyber breach and proper cybersecurity.**

Ask yourself the following questions:

- Do you have limited visibility of threats?
- Does your current solution provide deep and comprehensive visibility into ALL applications and processes?
- How does your solution provide near real-time information to help you better understand the threat during an attack?
- Aside from detecting the breach and raising the alarm, does your current solution offer end-to-end response and remediation?

Real-time reporting, such as that afforded by Endpoint Detection and Response solutions, allows cybersecurity teams to find and address the route of the issue rather than putting out fires and running from problem to problem.

**According to a World Economic Forum survey, 59% of respondents said that they feel it would be difficult to adequately deal with a challenging cybersecurity breach due to a shortage of relevant skills within their team.**[1]

- Do you lack a workforce skilled at dealing with cyberthreats?
- Does your current solution require advanced IT skills to operate?
- Will your Endpoint Detection and Response solution run autonomously?
- Are threats analysed in the cloud or at the agent?
- If they are analysed in the cloud, what if there is no internet connection?

Cybersecurity experts are in high demand, yet the number of available positions far exceeds the number of skilled workers. Therefore, businesses must address this issue holistically, considering their employees, processes, and available technology, such as Endpoint Detection and Response.

## 95% of data breaches involved human error.[2]

A data breach occurs when an employee exposes information directly (e.g., by misconfiguring databases) or through a mistake that allows a cybercriminal to access the organisation's systems.

- Are you experiencing alert fatigue?
- Can your solution handle and close alerts automatically to free up time for your analyst?
- Can your solution reduce the number of false positive alerts?

Alert fatigue occurs when an individual or team is exposed to an overwhelming number of alerts, to the point that it becomes desensitising, which impacts performance.

Alarms and alerts will indicate that there's a problem. Said problem will need to be investigated to determine whether it's genuine. Cybercriminals will use advanced techniques, including false-positive attacks, to overwhelm your team.

## Around 45% of cybersecurity alerts are actually false positives.[3]

Not only will this lead to a huge waste of resources, but it will also increase the likelihood of your staff ignoring a genuine cybersecurity threat due to the sheer volume of false positives.

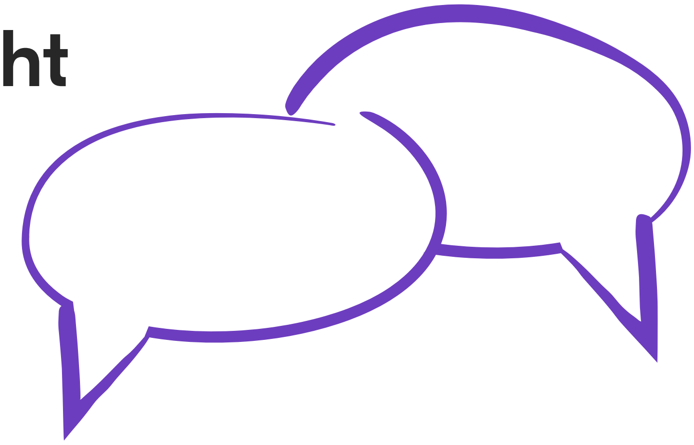
- Do you know about dormant threats?
- Is the ability to build your playbooks and custom detection strategies included?
- Are you able to automate threat-hunting scenarios?
- Is knowledge of scripting required to create playbooks?

Some malware lies dormant until the infected file is accessed. The malware then executes and does its damage. Once activated, malware may spread across your device to other files and programs.

**Did you know that the unemployment rate for experienced cybersecurity professionals was at 0% in 2021, where it's been since 2011?**

[1] WEF The Global Cyber Security Outlook 2022
[2] The Global Risks Report 2022
[3] Enterprise Strategy Group, Research and Insights Paper

# Have you got the right Endpoint solution?



**Cybersecurity threats have evolved at an alarming rate over the last decade. Endpoint Protection solutions have had to undergo a similar evolution to keep pace. Antivirus software is no longer effective as a standalone product in many situations.**

As a result, many businesses need assistance determining the best solution for their circumstances.

However, there is some good news. Endpoint Detection and Response solutions, such as those available from Kyocera, have been specifically developed to meet the needs of all types of businesses. The best part is that they are increasingly effective against unknown signatures, zero-day vulnerabilities, and fileless malware.

Kyocera has five kinds of Managed Endpoint Detection and Response solutions, each of which has varying degrees of functionality. However, they centre around five pillars, Identification, Protection, Detection, Response and Recovery.

With a breadth of solutions, each with varying degrees of functionality available, there will be a solution that is right for you. If you are still determining which Endpoint Detection and Response product is right for you, speak to one of our experts, who will assist you with making your decision.

You can talk to us; we are human, after all!

# What Kyocera's Endpoint Detection solutions can do for you.

**Kyocera provides a fully managed cybersecurity service, so your IT teams are free to focus on more strategic business goals.**

A truly effective EDR solution needs human oversight to ensure the best possible implementation and establish cyber-safe practices throughout your organisation. In turn, this gives you meaningful insights into the state of your security, and provides immediate expertise should your business experience a major attack.

**That's where Managed Endpoint Detection and Response comes in.**

"The fundamental philosophy behind our services is to prevent before responding and remediating. With our insight reports and customer success journeys, we work with customers to improve their overall cybersecurity position, making cybersecurity incidents less likely to occur."

Andrew Smith, Group Chief Information & Strategy Officer (CISO) at KYOCERA Document Solutions UK.

# Key features of M-EDR.

### Complete protection.

Advanced defence against cyberthreats, 24/7, 365 days a year.

### Best in class.

Protect your business with the best in class Endpoint Detection and Response solutions powered by CrowdStrike.

### Cloud-based.

A cloud-based solution with no added infrastructure costs.

### Real-time monitoring.

Total real-time visibility of endpoint activity throughout your organisation.

### Take charge.

Proactively uncover and lock-down vulnerabilities.

### Latest technology.

Up-to-date protection against the latest viruses and other security threats.

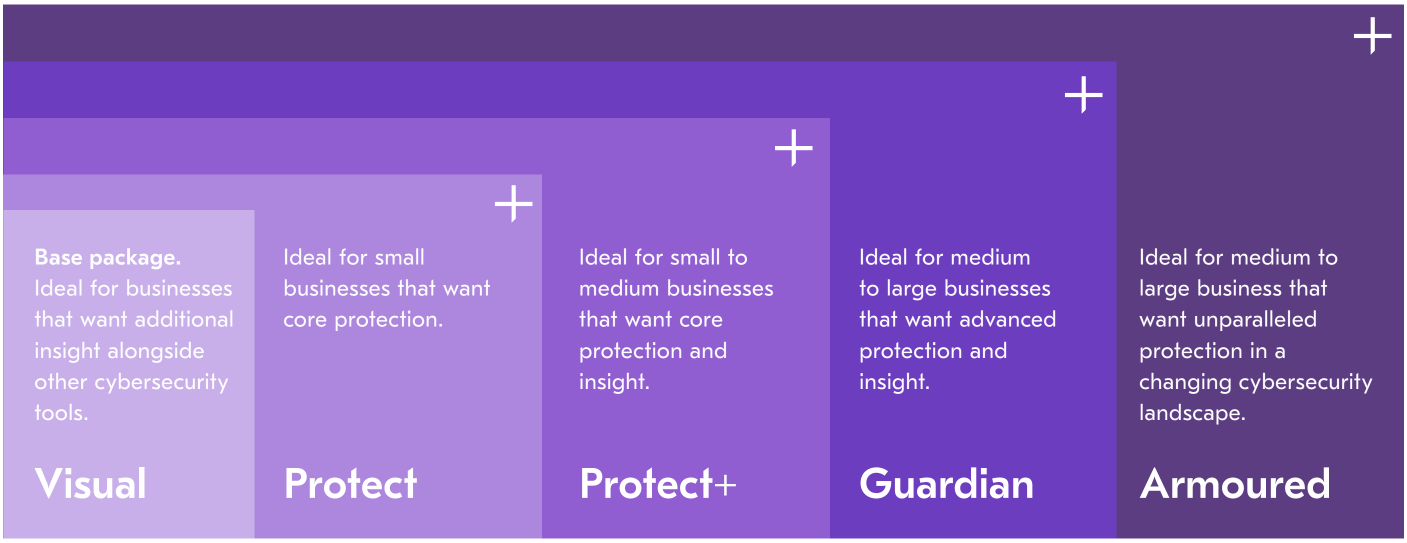
### Constant analysis.

Continual risk analysis and response.

### Experts on call.

Decisive intervention and expert crisis management from a team of cybersecurity professionals.

## Our 5 individual M-EDR service packages:



**Base package.** Ideal for businesses that want additional insight alongside other cybersecurity tools.

**Visual**

Ideal for small businesses that want core protection.

**Protect**

Ideal for small to medium businesses that want core protection and insight.

**Protect+**

Ideal for medium to large businesses that want advanced protection and insight.

**Guardian**

Ideal for medium to large business that want unparalleled protection in a changing cybersecurity landscape.

**Armoured**

# The key takeaways.

**Since the first Antivirus program was written, new categories of malware have been created, like ransomware or fileless attacks. The traditional fingerprinting approach utilised by the old anti-virus products often goes undetected.**

Moreover, cybercriminals are increasingly developing sophisticated malware for specialised attacks against companies, and critical infrastructure as the automated production of mass malware continues to grow. Every day, the AV-TEST Institute[1] registers over 450,000 new malicious programs (malware) and potentially unwanted applications (PUA).

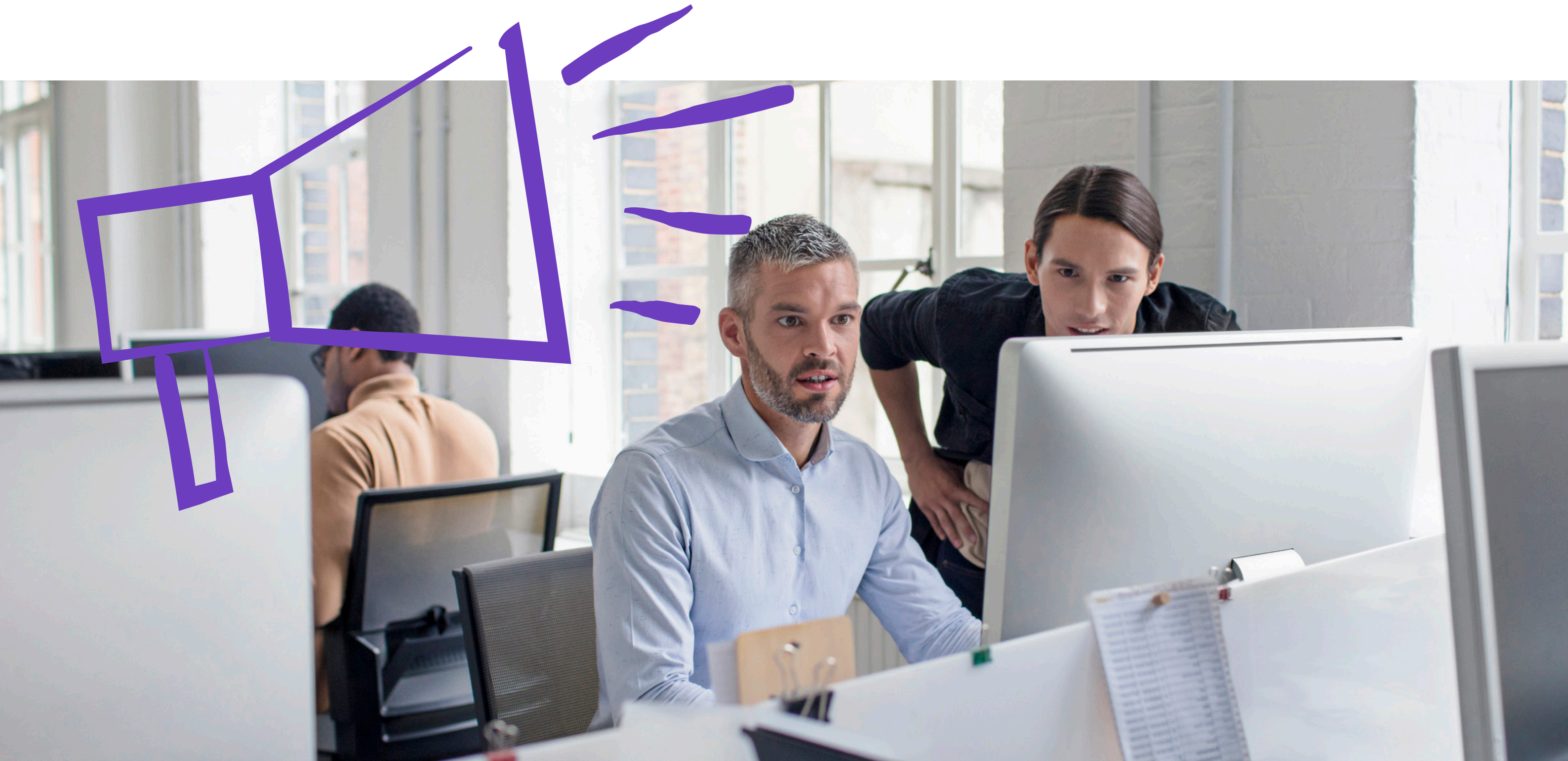
With more than 150 million newly-developed malware applications in 2021, the malware industry was more active than ever. Expert Insights reported that a successful ransomware attack hit 53% of organisations in 2021, and around 23% were hit more than once as a testament to this malicious software's rapid growth and intensity.

In the modern era, most cyber-attacks are customised to each target, with most of them having never been seen before and unable to defend their operating systems against malware attacks, even with the top anti-virus products.

Quite simply, modern problems require modern solutions. Just because an approach has been effective does not mean it remains the best solution today.

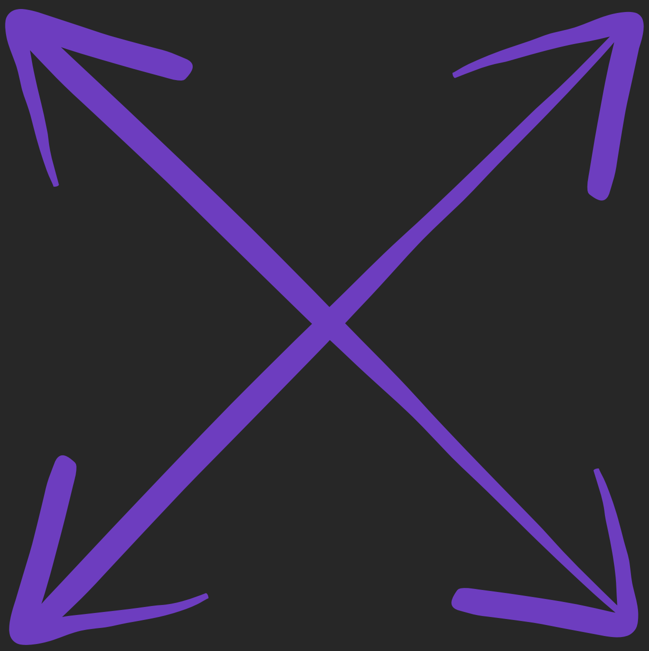
In other words, there should be a seismic shift away from outdated security programs such as antivirus to a more adaptable, reliable solution like Managed Endpoint Detection and Response. Ultimately, Kyocera's Endpoint Detection and Response is the best solution for arming your business for future fights against cyberthreats.

[1] 2022 AV-TEST - The Independent IT-Security Institute



# What you need to remember...

- New threats emerge daily.
- Multifaceted security solutions such as **Endpoint Detection and Response** are the new gold standard in cybersecurity.
- Traditional Antivirus platforms no longer offer reliable protection from all cyber attacks.
- **Endpoint Detection and Response** solutions are behaviour-based and use artificial intelligence to identify previously undetected malware without needing updates.
- You need to understand cybersecurity's challenges to your business or organisation.
- Effective alert management and threat hunting allow your cybersecurity team to address the root cause of an issue rather than fighting individual fires.
- Choosing the proper **Endpoint Detection and Response** is essential in an ever-changing cybersecurity environment.
- You need to be aware of numerous vulnerabilities, ranging from human error to bugs and glitches in the software code.
- **Endpoint Detection and Response** solutions will futureproof your endpoints while helping you understand and address the cause of a cyber attack.
- Cyber attacks are considered the second most threatening for global commerce over the next decade.
- Using Kyocera's **Endpoint Detection and Response** solutions, we can prevent most cyber attacks and effectively respond to and resolve the rest. Additionally, we work with customers to improve their overall cybersecurity position by providing insight reports and customer success journeys.



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

KYOCERA

WE ARE CARBON NEUTRAL • WE ARE CARBON NEUTRAL •

Kyocera Document Solutions does not warrant that any specifications mentioned will be error-free.
Specifications are subject to change without notice. Information is correct at time of going to press.
All other brand and product names may be registered trademarks or trademarks of their respective holders and are hereby acknowledged.