Acronis CSPi Technology Solutions

An MSP's guide to endpoint detection and response (EDR):

The key to providing better-managed security services

Overview

It's one of the most challenging problems of running your MSP business.

You must invest in robust cybersecurity tools to keep your clients protected. Yet, at the same time, you need to maintain healthy profit margins.

You cannot afford to lose the trust of your customers by putting their IT assets at risk. So it's imperative you have measures in place to defend them from today's highly sophisticated methods of attack. But these measures come at a cost, which either you or your clients must bear.

That's why it's so important to make the right choice of security solution. It must not only be fit for purpose, but also provide value for money and represent a positive addition to your portfolio of managed services.

In this guide, we discuss how endpoint detection and response (EDR) systems can help meet these objectives.

It explains how EDR works and how it differs from traditional endpoint protection technology. It explores the benefits that EDR can bring to your MSP business. And it also looks at what to consider in your choice of an EDR solution.

But we start with the basics by clarifying what exactly a security incident means.

Growth opportunity for MSPs

According to research published by market intelligence and advisory company Mordor Intelligence, the value of the global endpoint detection and response (EDR) market was an estimated USD 1.76 billion in 2020.

The report forecasts this to reach USD 6.72 billion by 2026, representing a compound annual growth rate (CAGR) of 25.15% during the period 2021–2026.

It said the driving forces behind this rapid growth were the increasing number of data breaches worldwide and the demand for more decentralized and edge-based security approaches.

For MSPs that offer EDR as part of their portfolio of services, this presents an opportunity to stand out in the marketplace, generate more revenue for their business and provide the protection customers need against emerging threats in today's technology landscape.

What is a security incident?

A security incident is a broad term to describe a collection of events and detections that could indicate an attack on an information system.

It may be an attempt to gain unauthorized access to resources or it may be a denial-of-service (DoS) attack, whereby hackers flood systems with huge numbers of server requests in a bid to bring them down.

Unlike a full-blown security breach, a security incident doesn't necessarily mean your data has been compromised. But, even if it hasn't yet developed into a breach, a security incident still poses a serious threat to your data and requires prompt corrective action.

In the context of an EDR system, a security incident is characterized by a series of aggregated alerts to events that correlate to the same developing attack.

> "It takes 20 years to build a reputation and a few minutes of cyber-incident to ruin it."

Stéphane Nappo,
Global Chief Information Security Officer, Groupe SEB.

Source: Blue-Pencil.ca

What exactly is an endpoint?

An endpoint is any device or node that serves as a source or destination for communication over a network. Examples of endpoints include:

- Desktop computers
- Laptops
- Tablets
- Smartphones
- Printers
- Servers
- ATM machines
- Internet-of-things (IoT) devices

But they do not typically include devices designed to manage and forward data communication, such as:

- Routers
- Gateways
- Firewalls
- Load balancers

The concept of an endpoint has played an increasingly important role in cybersecurity in recent years. This has largely been the result of the growing trend toward **remote work** and **bring-your-own-device (BYOD)** policies.

What is EDR?

Endpoint detection and response (EDR) is a technology that provides your security teams with the tools they need to detect and respond to threats to your systems as and when they happen.

It works by collecting data from workstations and other endpoints for threat analysis, enriching it with contextual information to help you prioritize remedial action.

EDR identifies attacks that bypass traditional frontline defenses, such as firewalls, antivirus software, and endpoint protection platforms (EPPs).

As with EPP, EDR is an endpoint security technology. But it differs from EPP in many different ways.

For example, EPPs have traditionally been geared toward signature-based detection of threats. This means they could only generally detect known attacks. However, they have evolved to include a wider range of functionality, such as the ability to block previously unknown malware and untrusted processes and applications, as EPPs have been using heuristics for 20-plus years to detect unknown malware.

They also work in the background, blocking attacks at the point of entry.

By contrast, EDR is mainly a detection and remediation technology that monitors endpoint activity for potential signs of an attack and requires active supervision to deal with the results of its findings.

	EPP	EDR
Security strategy	Prevention	Detection
Protection mode	Passive	RTO and RPO dependent on integration with backup and recovery vendors
(Runs automatically in the background without supervision)	Active	SentinelOne cannot provide business continuity nor restoration. It is not integrated with backup and recovery vendors
(Provides security teams with real-time incident response and investigation capabilities)	Better value - a single license for a single platform for backup + recovery + advanced security + EDR, pay-as-you-go	Hidden costs adding other vendor backup/recovery solutions; additional licenses for XDR service
Primary method of detection	Signature-based	Analysis of endpoint behavior
Effective against	Known malware	Zero-day exploits, hacking tools, fileless attacks, advanced persistent threats (APTs)
Layer of protection	Basic first line of defense	Advanced detection of attacks that bypass other defense layers
False positives	Low	Higher probability
False negatives (Missed detection)	High	Low

Why do MSPs need EDR?

Traditional security approaches, such as antivirus, firewalls, and EPPs are no longer sufficient to safeguard modern IT deployments — as the majority of successful cyberattacks today use previously unknown malware.

However, EDR offers the protection your customers need against today's new and more sophisticated threats. It provides visibility into endpoints and real-time investigation and incident response capabilities. This allows you to play a more active role in their security.

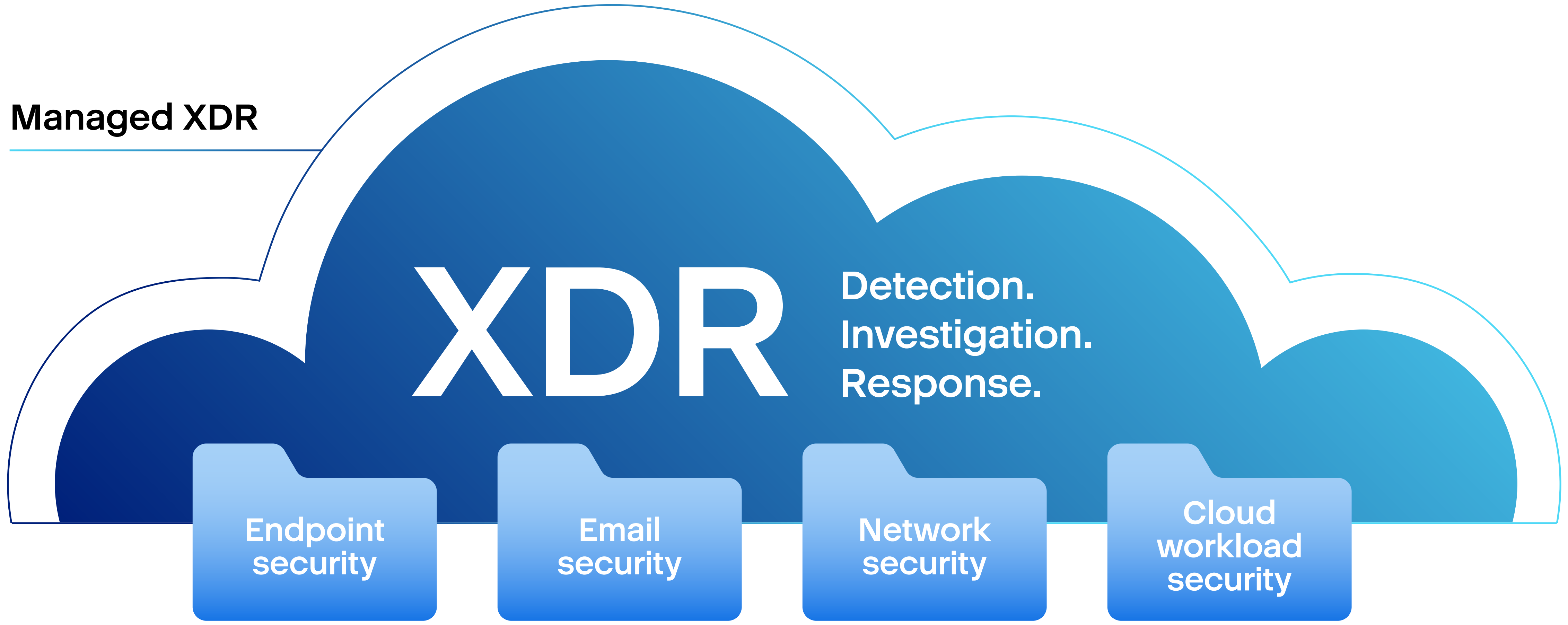
It will give you peace of mind that you're in control and will serve as an indispensable tool without which breaches can go undetected and potentially take months to identify and contain.

But beware: EDR is intended to complement rather than replace conventional security tools. Attackers are always on the lookout for easy targets. So it's important you still maintain your frontline defenses against more basic malware threats.

What is XDR?

Extended detection and response (XDR) works in much the same way as EDR. However, it takes a more holistic approach by monitoring and correlating information from a much broader range of collection points, such as networks, email, and cloud-based workloads.

The primary goal of XDR is to integrate multiple products into a unified, cohesive security operations platform, providing visibility into all your security telemetry through a single pane of glass.



Source: Trendmicro.com

> "I believe in having each device secured and monitoring each device, rather than just monitoring holistically on the network, and then responding in short enough time for damage control."

Kevin Mitnick,
American computer security consultant
and the world's most notorious hacker.

Source: Brainyquote.com

The MITRE ATT&CK framework

The MITRE ATT&CK framework is a freely accessible knowledge base that catalogs different types of adversary behavior based on findings from real-world cybersecurity attacks.

It provides a breakdown of individual steps and methods hackers follow to achieve specific tactical goals during an attack. This helps you understand how different types of attacks work and the measures you need to take to mitigate them.

The framework documents the various phases of an attack lifecycle in the form of a matrix — with different alternatives for different types of environment, such as Windows, Linux, macOS and cloud-based platforms.

The model can also help you evaluate existing defenses and prioritize detection.

How EDR works

The specific operational capabilities of each EDR solution vary from vendor to vendor. However, they should all provide the same core functionality to help you through the following three phases of dealing with a security incident.

Detection phase

EDR systems collect a lot of data and can generate a lot of alerts. To help keep noise to a minimum, they should: Automatically respond to known indicators of compromise (IOCs) and contain or remediate the impact of any corresponding malicious endpoint activity in real time.

- Deliver all endpoint telemetry to a central incident management console to aid incident evaluation and avoid duplicate work.
- Correlate alerts to security incidents, providing you with contextual information that you can quickly piece together to form of a clear picture of the attack.

Prioritization phase

Using these insights, you should be able to determine:

- How the perpetrator initiated the attack
- Any lateral movement of the attacker through your network
- The impact of the attack on your business
- The corrective steps you'll need to take
- The level of priority relative to other ongoing incidents
- Whether you need to carry out any additional investigation

However, the better the quality of information your EDR system provides, the better the decisions you'll make about prioritizing your responses.

A fully featured EDR system will also give you a means of documenting incidents and actions for later analysis.

Response phase

EDR platforms also offer a range of features for managing your response to a security incident. For example, they should provide you with the ability to:

- Stop and contain the attack
- Quickly and efficiently roll back endpoints to their pre-infected state
- Remediate the vulnerability the attacker exploited and apply lessons learned from the attack
- Create automated playbooks for similar attacks
- Monitor endpoints after restore to prevent recurring breaches

How to manage a security incident

Preparatory

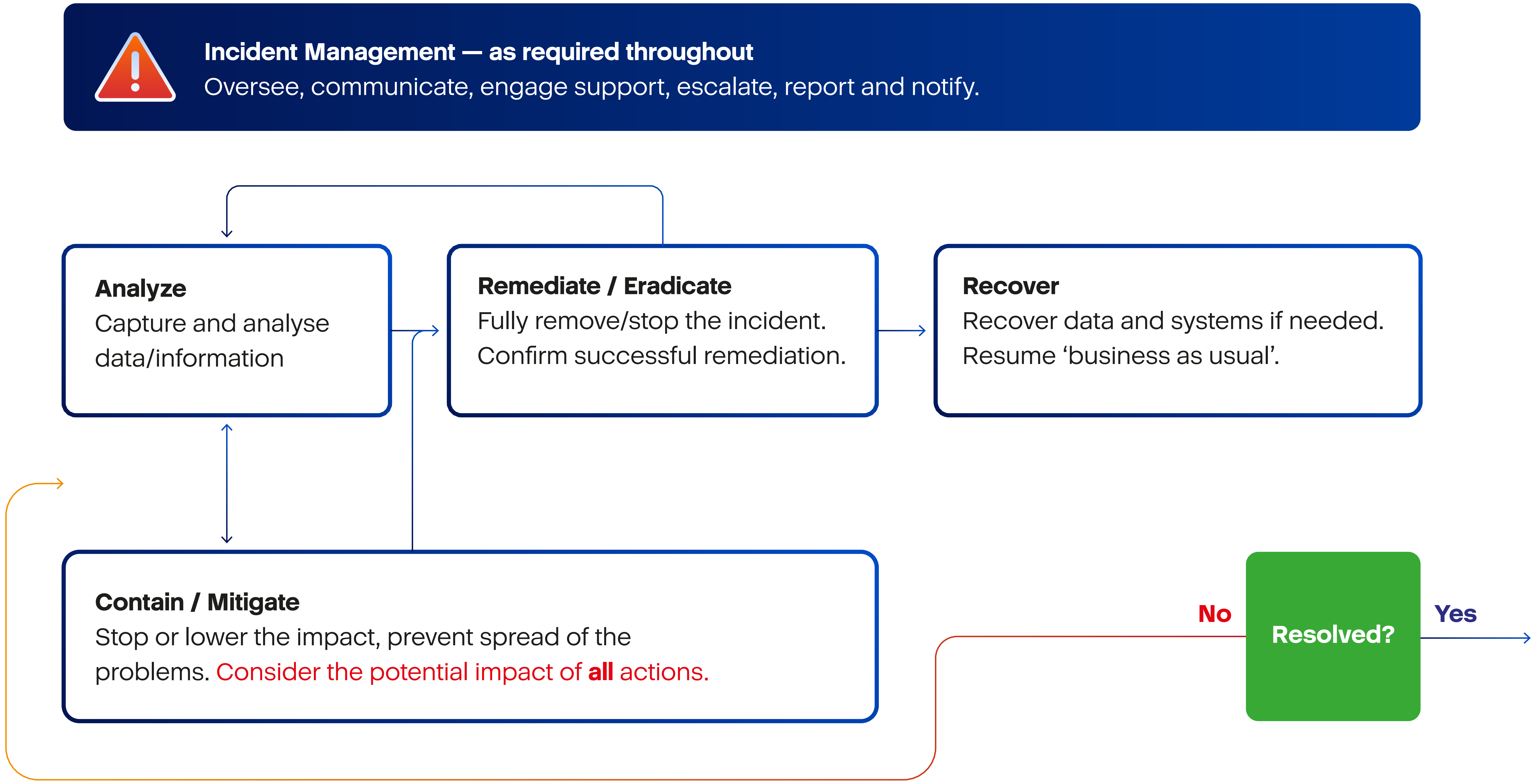
Triade
Assess impact.
Categorise incident.
Assign incident manager.
Check for false positive
Is legal input needed?

Escalate
If required.
Within IR Team or to CIO / CISO
who may escalate further.

Kick off response
Who else needs to be involved?
IT, Legal, HR, PR?
Consider internal and external parties.

Reporting
Consider reporting and evidence capture requirements.
For example, in the case of a data breach.

Core response



Incident Management — as required throughout
Oversee, communicate, engage support, escalate, report and notify.

Analyze
Capture and analyse data/information

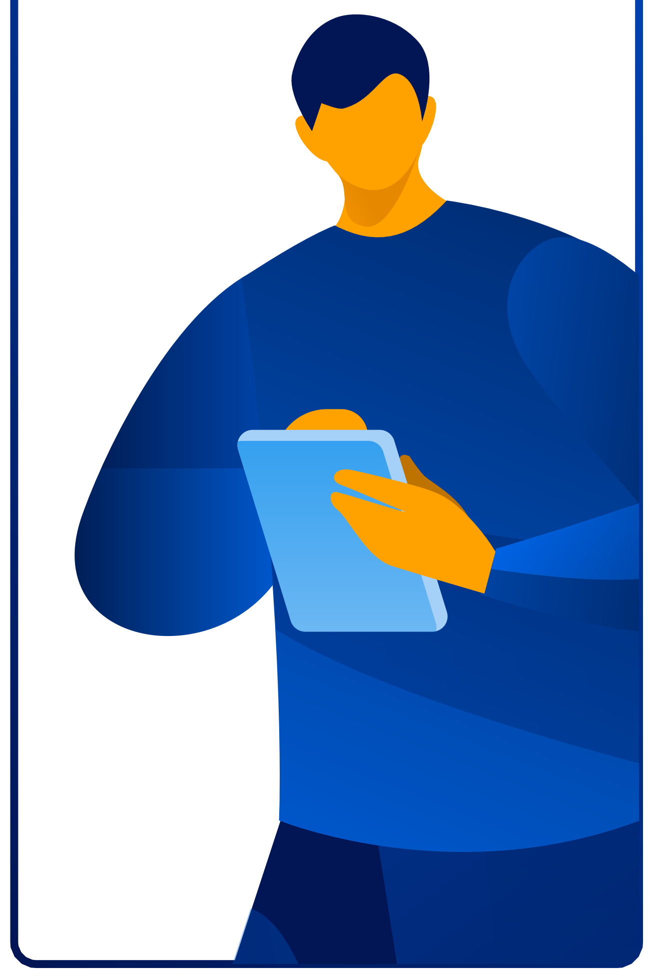
Remediate / Eradicate
Fully remove/stop the incident.
Confirm successful remediation.

Recover
Recover data and systems if needed.
Resume 'business as usual'.

Contain / Mitigate
Stop or lower the impact, prevent spread of the problems. Consider the potential impact of **all** actions.

Close down

Review and close down
Document and assign improvements.



Source: National Cyber Security Centre

EDR challenges for MSPs

There's no shortage of EDR offerings available on the market. However, MSPs have very specific needs. So, they should look for a solution that fits around their role as a third-party company responsible for managing the IT of numerous different customers.

This is no easy challenge given the problems MSPs encounter with many of the EDR products currently at their disposal. For example:

- The insights many EDR systems provide are generally only suitable for users with a high level of technical expertise. However, security professionals are expensive. This puts them outside the domain of most MSPs and makes such solutions ill-suited to their business objectives.
- EDR platforms often generate a large number of alerts to low-level events and incidents. But, without a wider contextual understanding, investigation can be a very complex and time-consuming exercise — all the more so for MSPs with limited manpower to piece together the full facts and get to the root cause of the incident.
- Backup and disaster recovery (DR) mechanisms are rarely integrated into EDR solutions. This makes recovery from an attack all the more cumbersome, as MSPs need to use separate tools to restore systems and fully remediate the threat.

Built for MSPs

MSPs should therefore look for EDR solutions that are built with their needs in mind. Ideally, these should include:

- **Automatic, easy-to-understand interpretation of attacks:** That way, you won't need to analyze hundreds of lines of logs, helping you to reduce threat investigation and response times from hours to just a few minutes.
- **Centralized response management:** So you can investigate, remediate, and recover from breaches quickly and easily via a single console.
- **Integrated backup, rollback, and DR:** Through which you can get customers up and running again as quickly and efficiently as possible, seamlessly returning them to normal operation.

A competitive advantage

An EDR system can significantly enhance your portfolio of managed services, reducing the security risk to your customers through advanced protection against a new generation of more sophisticated attacks.

But, to realize the full potential of EDR, it should be simple and efficient to use. This will prove essential in maintaining your margins and preventing runaway costs.

If you can achieve this objective, you'll be able to stand out in a crowded marketplace. You'll be able to command a premium for your security capabilities. But, above all, you'll open up new revenue opportunities for your MSP business and enjoy a much healthier bottom line.

Acronis CSPi Technology Solutions

About Acronis

Acronis unifies data protection and cybersecurity to deliver integrated, automated cyber protection that solves the safety, accessibility, privacy, authenticity, and security (SAPAS) challenges of the modern digital world. With flexible deployment models that fit the demands of service providers and IT professionals, Acronis provides superior cyber protection for data, applications, and systems with innovative next-generation antivirus, backup, disaster recovery, and endpoint protection management solutions powered by AI. With advanced anti-malware powered by cutting-edge machine intelligence and blockchain based data authentication technologies, Acronis protects any environment – from cloud to hybrid to on premises – at a low and predictable cost.

Founded in Singapore in 2003 and incorporated in Switzerland in 2008, Acronis now has more than 2,000 employees and offices in 34 locations worldwide. Its solutions are trusted by more than 5.5 million home users and 500,000 companies, and top-tier professional sports teams. Acronis products are available through over 50,000 partners and service providers in over 150 countries and 26 languages.

About CSPi Technology Solutions

CSPi Technology Solutions, an Acronis partner, provides the expertise and service scope - including Managed IT Services,
Professional Services, and Cloud Services - to help you architect and manage a high performance, highly available, and highly secure infrastructure