Why anti-virus software is no longer enough

Contents

In an increasingly digitised and interconnected world, cyber security has become a critical concern for all organisations.

Among the plethora of measures available, perhaps the most popular is technology that protects your laptops, smartphones and servers (the endpoints).

This guide explores two solutions; endpoint protection (including anti-virus software) and endpoint detection & response (EDR). We examine their differences, and why an integrated approach could be the most effective solution for comprehensive cyber security.

1. Understanding Endpoint Protection

Endpoint protection, also known as Endpoint Protection Platform (EPP), refers to a security approach primarily focused on preventing threats.

It involves deploying security measures on endpoints to secure them from malware, hacking, and other potential threats.

Endpoint protection platforms typically include antivirus software, firewalls, host intrusion prevention systems (HIPS), and data loss prevention (DLP). The main focus is ensuring threats cannot penetrate the system in the first place.

2. Understanding Endpoint Detection and Response (EDR)

Unlike endpoint protection, which focuses on prevention, EDR concentrates on identifying and addressing threats that have already infiltrated the system.

Endpoint protection isn't 100% secure - viruses or malware will get through. EDR was developed in recognition of this fact and monitors endpoints to find the threats that slip through.

Upon detecting a potential threat, EDR isolates affected systems to prevent further spread and starts the response process. It uses advanced analytics, threat intelligence, and data from various sources to identify threats, often leveraging AI and machine learning to detect abnormal behaviour.

3. Endpoint Protection vs EDR: A comparative analysis

While endpoint protection and EDR offer valuable security strategies, they differ in their core functions and ideal use cases.

- **Prevention vs Detection and Response:** Endpoint protection primarily focuses on prevention, attempting to stop cyber threats before they infiltrate the system. However, it's estimated that anti-virus software will detect only 24%* of viruses.
  On the other hand, EDR acknowledges that no system can be entirely secure and focuses on quick detection and response to minimise damage when a breach occurs.
- **Static Rules vs Behavioural Analysis:** Endpoint protection uses static rules to identify known threats based on signature databases and protects against them. In contrast, EDR uses behavioural analysis and threat intelligence to identify unknown or zero-day** threats.
- **Operational Ease vs Detailed Insight:** Endpoint protection tools are generally more straightforward to operate, needing less specialised expertise to run effectively. Conversely, EDR solutions provide more detailed forensic insights but require more advanced security knowledge.

While these differences may suggest a need to choose endpoint protection or EDR, a comprehensive security strategy often requires a blend of both.

> “ It's estimated that anti-virus software will detect only 24% of viruses ”

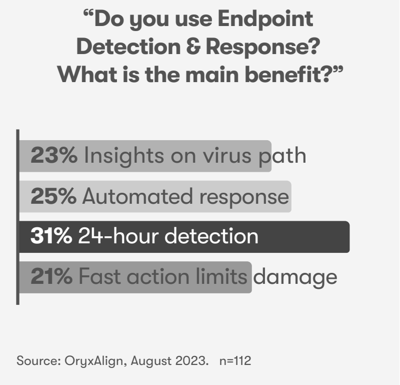
4. What are the benefits of protecting endpoints?

Below are some key benefits of protecting endpoints beyond keeping sensitive data safe, preventing loss and stopping unauthorised access.

- **Compliance:** Many industries have regulatory requirements to secure data. Endpoint protection helps meet these standards, thereby avoiding penalties.
- **Performance:** It can reduce malicious attacks that may slow down or otherwise hinder system performance, ensuring that systems run smoothly.
- **Reduced Attack Surface:** By managing all devices on the network, endpoint protection minimises the potential entry points for attackers.
- **Cost Prevention:** There are potentially significant costs associated with recovery, loss of reputation and fines for data breaches (current GDPR maximum fine is 4% of global turnover).
- **Remote Work Security:** Endpoint protection can ensure devices outside the traditional network are secured.

To further understand the specific benefits of EDR, we surveyed over 100 IT managers. You can see the results in Chart I. It seems 24-hour detection of malware that has breached initial defences is a significant advantage.

Chart I - EDR benefits



Source: OryxAlign, August 2023. n=112

* Source: Email-Based Malware Attacks Report by Brian Krebs (Cyber Security Expert).
** A zero-day threat is an unknown vulnerability in a computer or mobile device's software or hardware.

5. The importance of a comprehensive approach to cyber security

In today's dynamic threat landscape, an integrated approach that combines the proactive measures of endpoint protection with the reactive, intelligent capabilities of EDR is becoming increasingly popular.

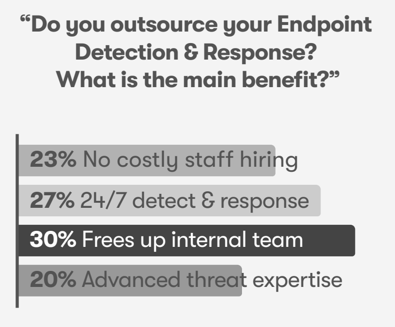
This approach often starts an organisation's journey to 'Extended Detection and Response' (XDR). More details can be found in this article 'EDR security versus MDR or XDR'.

However, this approach does require expert handling, and many firms struggle to hire (and retain) the necessary cyber expertise. SMEs that go down this route often choose to outsource their cyber security*.

We conducted another survey to understand why IT Managers would choose to use a managed EDR service (or MDR, Managed Detection & Response). Two reasons became apparent (see Chart II).

Again, 24-hour detection was a factor, but out in front was the ability to free staff from cyber security chores so they could focus on more productive technology projects.

Chart II - EDR benefits



Source: OryxAlign, August 2023. n=137

6. Conclusion

UK government research suggests that large organisations are more prone to attack (see Table I). But the figures could be misleading, as large firms probably have EDR, which is better at detecting malware. Micro-medium companies tend not to have that capability, so that they may miss an attack or infection.

Table I - Cyber attacks by size

Organisation size	% hit by attack
Micro	31%
Small	32%
Medium	59%
Large	69%

Source: UK Govt "Cyber security breaches survey 2023" n= 2,263

Micro business; 1 to 9 employees
Small business; 10 to 49 employees
Medium business; 50 to 249 employees
Large business; 250 or more employees

Also, cybercriminals will always go for the easy target - companies with poor security. Often that is smaller firms. Small companies are a gateway for cybercriminals to reach their larger clients. Infecting a client because of inadequate cyber protection can seriously damage relationships.

Endpoint protection was the bare minimum; now, it is no longer enough. Anti-virus is only 24% effective, and firewalls can be breached. While it is low cost and low maintenance it is also low protection.

EDR may be the next logical step. But it requires a skilled team to be truly effective, and some smaller organisations cannot afford to hire expensive cyber experts.

Outsourcing EDR is an option, and small (10-49 staff) or medium (50-249 staff) companies are most likely to outsource their cyber security*.

But outsourcing is a big decision and can lock companies into a 2-5 year agreement. However, our research shows that those using a managed EDR service benefit from 24/7 peace-of-mind and their staff are freed from unproductive cyber protection projects.

* "Do you outsource cyber security?"

Micro business; 32% outsource cyber security
Small business; 50% outsource cyber security
Medium business; 58% outsource cyber security
Large business; 37% outsource cyber security

Source: UK Govt "Cyber security breaches survey 2023" n= 2,263

OryxAlign
Bury House
31 Bury Street
London EC3A 5AR

T: +44 (0)207 605 7890
E: hello@oryxalign.com
W: www.oryxalign.com

For some good advice on Endpoint Detection and Antivirus you can book a 45-minute consultation or email hello@oryxalign.com.

OryxAlign brings people and technology in parallel to drive better, faster outcomes.
By listening closely, adjusting along the way and delivering to the highest standards, we create true alignment between your ambitions and the technology you need to reach them.

No Warranties and Limitation of Liability
Information provided via this tool is provided 'as is' without warranty of any kind, either expressed or implied, including fitness for a particular purpose and non-infringement. Oryx Align Ltd does not make any warranties or representations as to the accuracy or completeness of this tool, and assumes no liability or responsibility for any errors or omissions in its content. Your use of this tool is at your own risk, and Oryx Align Ltd is not liable to you or any other person for any indirect, direct, special, incidental or consequential damages arising from your access or use of this tool. E&OE.

First published 13 July 2023

If printed, please recycle the paper.