Mtech are switching the Endpoint Protection from ESET to Sentinel One – please read the information below.

The Top 5 Benefits of Switching to EDR Security from Traditional Antivirus Products

MTech has seen the rapid evolution of antivirus products over the years, and I can say that traditional antivirus solutions are no longer sufficient to protect organisations from modern-day cyber threats. The emergence of new and sophisticated threats has led to the development of Endpoint Detection and Response (EDR) solutions. In this article, I will take you through what EDR is, its benefits, and how it compares to traditional antivirus products.

Introduction to EDR Security

EDR is an advanced security solution that is designed to detect, investigate, and respond to threats that traditional antivirus products may not detect. EDR solutions use a combination of advanced technologies such as machine learning, behavioural analysis, and threat intelligence to provide comprehensive protection against modern-day threats such as ransomware, zero-day attacks, and advanced persistent threats (APTs).

Unlike traditional antivirus products that rely on signature-based detection, EDR solutions focus on detecting and responding to suspicious behaviour and activities within an organisation’s endpoints. This makes EDR solutions more effective in detecting and responding to unknown threats that may bypass traditional antivirus products.

What is an EDR Solution?

An EDR solution is a type of endpoint security software that provides real-time visibility and control over endpoints within an organisation’s network. An EDR solution can detect and respond to threats in real-time by analysing endpoint activities and behaviours. The solution collects data from endpoints such as laptops, desktops, servers, and mobile devices, and uses this data to identify and prevent potential threats.

EDR solutions also provide additional features such as threat hunting, incident response, and forensic analysis. These features enable security teams to investigate and respond to threats more effectively, reducing the time it takes to identify and resolve security incidents.

The Limitations of Traditional Antivirus Products

Traditional antivirus products have been around for decades, and they have been effective in protecting organisations from known threats. However, as cyber threats continue to evolve, traditional antivirus products have become less effective in detecting and preventing modern-day threats.

One of the limitations of traditional antivirus products is that they rely on signature-based detection. This means that they can only detect known threats that have been previously identified and added to their signature database. This makes traditional antivirus products ineffective against zero-day attacks and other unknown threats.

Top 5 Benefits of Switching to EDR Security

Enhanced Threat Detection and Response Capabilities

One of the key benefits of switching to EDR security is enhanced threat detection and response capabilities. EDR solutions use advanced technologies such as machine learning, behavioural analysis, and threat intelligence to detect and respond to threats in real-time. This means that organisations can detect and respond to threats faster, reducing the time it takes to identify and resolve security incidents.

EDR solutions can also detect and respond to unknown threats that may bypass traditional antivirus products. By analysing endpoint activities and behaviours, EDR solutions can identify suspicious activities and take action before the threat can cause any damage.

Improved Visibility and Control over Endpoints

Another benefit of EDR security is improved visibility and control over endpoints. EDR solutions provide real-time visibility into endpoint activities and behaviours, allowing security teams to identify potential threats and take action before they can cause any damage.

EDR solutions also provide granular control over endpoints, enabling security teams to enforce security policies and configurations to prevent unauthorised access and data exfiltration. This level of control is not possible with traditional antivirus products, which only provide basic endpoint protection.

Advanced Behavioural Analysis and Machine Learning

EDR solutions use advanced behavioural analysis and machine learning to detect and respond to threats. Behavioural analysis involves monitoring endpoint activities and behaviours to identify suspicious activities. Machine learning involves using algorithms to analyse data and identify patterns that may indicate a threat.

By combining these two technologies, EDR solutions can detect and respond to threats more accurately and efficiently. EDR solutions can also learn from past incidents and use this knowledge to improve their threat detection and response capabilities over time.

Greater Scalability and Flexibility

EDR solutions are more scalable and flexible than traditional antivirus products. EDR solutions can be deployed in cloud, on-premise, or hybrid environments, providing organisations with greater flexibility in terms of deployment options.

EDR solutions can also be easily scaled up or down to meet the changing needs of an organisation. This makes EDR solutions ideal for organisations of all sizes, from small businesses to large enterprises.

Cost-Effectiveness of EDR Security

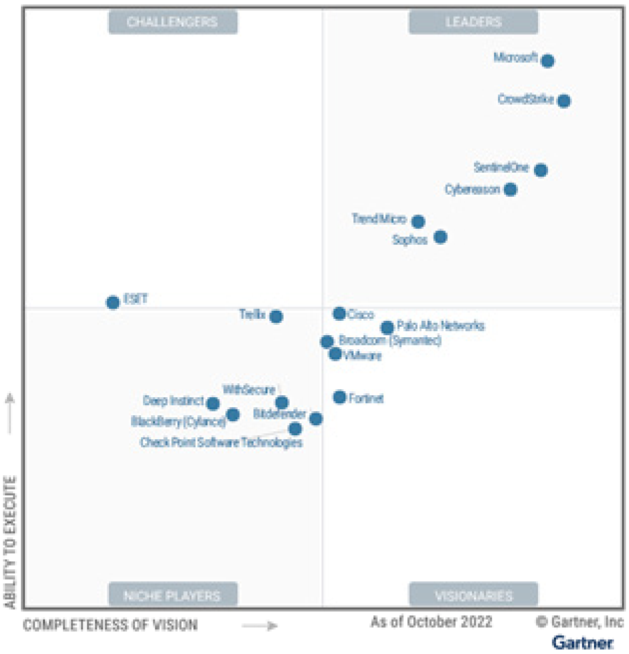
While EDR solutions may seem costly compared to traditional antivirus products, they are more cost-effective in the long run. EDR solutions can detect and respond to threats more efficiently, reducing the time and resources required to investigate and resolve security incidents.

EDR solutions can also help organisations avoid costly data breaches and other security incidents that can result in reputational damage and financial losses.

Conclusion: MTech is switching from ESET to Sentinel One for Endpoint Protection

In conclusion, EDR security offers several benefits over traditional antivirus products. EDR solutions provide enhanced threat detection and response capabilities, improved visibility and control over endpoints, advanced behavioural analysis and machine learning, greater scalability and flexibility, and cost-effectiveness.

Mtech have researched the marketplace thoroughly and have selected Sentinel One as one of the market leaders – highlighted by their position in Gartner's Magic Quadrant of Endpoint Protection Platforms.



MTech will be replacing the existing ESET antivirus product currently deployed to all your corporate devices with Sentinel One Control – the mid-range solution for devices. This will happen over the coming weeks, and we will provide information for your staff to explain the process.

There is an option to upgrade to a fully managed 24x7 service, and if this is something that you are interested in, please speak to your account manager.