datacentrix

The strategy behind effective and agile endpoint security

By Gideon Viljoen, Pre-sales Specialist: ICT Security at Datacentrix, a leading hybrid ICT systems integrator and managed services provider

The mitigation of increasing endpoint security risks is critical for protecting an organisation's valuable data and resources in hybrid ICT and mobile environments with distributed workforces. Effective endpoint security measures that are agile and quick to adapt to the changing attack landscape is paramount for ensuring an effective first line of defence.

It's important to start with the basics and ensure that all endpoints and servers, as well as critical assets and devices, are covered by an anti-virus (AV) or anti-malware security product. Sticking with the basics, patching of these devices and endpoints is a great way to ensure known vulnerabilities are not open to exploitation.

With an ever-changing landscape and attackers using increasingly smarter techniques, machine learning (ML) and user behaviour analytics (UBA) have become absolute musts in the current landscape of cybersecurity. In fact, for more mature cybersecurity portfolios, it is always better to have some form of ML and artificial intelligence (AI) in place, as they are able to take the necessary action much faster than a human. Engineers and analysts are then able to focus on critical risks.

Having an endpoint detection and response (EDR), or better yet, a cross detection and response (XDR) solution in place, compared to the traditional AV option, helps to identify, isolate and respond to suspicious behaviour on an endpoint or critical asset. These solutions also assist in reducing investigation and alert times, with far fewer false positives, which can tend to overwhelm engineers and analysts and cause alert fatigue.

“

Having an endpoint detection and response (EDR), or better yet, a cross detection and response (XDR) solution in place, compared to the traditional antivirus (AV) option, helps to identify, isolate and respond to suspicious behaviour on an endpoint or critical asset.

> The adoption of EDR and XDR solutions is becoming far more important than ever before, as opposed to the traditional stand-alone AV solutions of the past.

Gideon Viljoen, Pre-sales Specialist: ICT Security at Datacentrix

Managing and maintaining a secure endpoint posture in hybrid IT and mobile environments

With a rapidly evolving landscape, changing attack strategies and new technologies being introduced on a daily basis, organisations are under immense pressure to choose the 'right' endpoint security solution, and ensure they are making the correct investment and decision in a specific technology.

Coupled with this is the ability to adapt, be flexible and expand on the solution to move with the aforementioned changing landscape. With this in mind, it is essential that organisations choose a cybersecurity provider and a technology solution that are agile and quick to adapt and adopt; factors that far outweigh the cost element.

Visibility of these mobile and hybrid IT workforces is critical: no business can protect or remediate what cannot be seen. Ensuring that there is a solution that can provide visibility of all devices and assets, regardless of where they are, as well as users and user behaviours, has become essential. This will allow for reduced response times and decreased risk.

Trends in endpoint management

The adoption of EDR and XDR solutions is becoming far more important than ever before, as opposed to the traditional stand-alone AV solutions of the past.

Having a solution that is able to provide intelligence, visibility and response to the holistic network, while also being able to provide a single source of truth, is of utmost importance.

EDR and XDR solutions have helped to reduce response times considerably, providing effective protection against threat actors. However, their evolution is far from over, and with hybrid work forces not going anywhere soon, having agile solutions and technologies in place will continue to be beneficial to businesses.

Common pitfalls with endpoint security

Companies and their executives can be overwhelmingly bombarded with new technologies, and choosing the right solution for the organisation can be tough. Looking to independent, objective authorities like Gartner and Forrester for recommendations can be helpful here, providing guidance and greater confidence around who is leading in which specific areas. Reference cases and business cases/studies also can provide some confidence in selecting the best option for a business.

A lack of agility and slower adoption rates are common pitfalls for many businesses, and so faster adoption and adaptation to the threat landscape by an organisation and its cybersecurity partner is vital.

For more information on Datacentrix's Security Services offering, please visit www.datacentrix.co.za/security-services.html