CHOOSING THE RIGHT PROTECTION FOR YOUR ORGANISATION

Choosing the right antivirus protection for your business or organisation is important, however, it is only one part of your system's security protection and should not be relied on solely.

ANTIVIRUS PROTECTION

Cyber attackers and threats are becoming increasingly sophisticated and resilient to traditional means of protection. Traditional antivirus protection is no longer sufficient by itself. Antivirus relies on identifying traits of harmful files and blocking known threats, however the sophistication of the latest malware make this increasingly difficult for antivirus applications to block on their own.

In order to have sufficient levels of protection for your systems, the focus needs to shift to behavioural-analysis tools, such as endpoint protection, which allows for visibility and control over what's running on your system and endpoints.

HOW DOES ENDPOINT PROTECTION WORK?

Modern endpoint protection tools, often referred to as Endpoint Detection and Response (EDR), observe and analyse the behaviour of everything going on in the system. This includes network traffic entering or leaving a device, every process that runs on a device and what files they access. Depending on the configuration, it can either block or simply alert on unusual activity on a device.

WHY NOT BOTH?

Mixing traditional anti-virus with modern EDR is often painful, as the anti-virus can look like malicious software and trigger false positive alerts. Managing these conflicts can be time consuming, and end up being a net negative.

CHOOSING THE RIGHT PROTECTION

There are a number of endpoint protection products on the market, it is important when choosing the right product for your organisation that you understand your system's needs and requirements.

Some things to keep in mind.

- Do you have a managed security service provider (MSSP) already? An MSSP will often have a chosen EDR tool that they maintain, which will make your deployment and ongoing maintenance easier.
- What products are you using already that it needs to integrate with?
- How does the product work? For example, is it cloud based requiring internet access or is it on premise?
- What support is provided for the product? For example, can you get support locally or does it rely on out-of-band time zones?
- Can you maintain the product internally or will you need to pay to outsource?
    - External support might have a preferred endpoint protection system of choice.
    - If you go with open source tools, you may require additional resource to deploy.
- Consider how long you are locked in to the product you purchase and what would it take to migrate to something else if you need to.

CERT Tonga

certnz

Modern EDR tools will work without significant tweaks, however, getting full value from them generally requires experience with the tool and strong incident response knowledge/ experience. In many cases, this is easiest to achieve with a centralised team of specialists (such as a managed security service provider or a central government team to provide this to all agencies).

Integration with your current system is key and will help with implementation and financial costs. You should ensure you have considered:

- How you will have visibility (do you have a SIEM/ecosystem integration)? Does this have a management interface that you can use or do you need something else?
- How will it integrate and understand your authentication system(s)?
- How it can integrate with your firewalls/other controls?
- How will all parts of your system respond when one part detects something bad?
- What happens with edge cases? For example, loss of connectivity when depending on cloud-based systems.
- What mobile devices do you have, what are they used for and what protections do you need on them? Some endpoint protection has a mobile version, some don't.

SETTING UP YOUR ENDPOINT PROTECTION FOR SUCCESS

When rolling out new protection software, it can be a good idea to deploy it in a non-blocking/alert-only configuration to start with. This will let you see what's going on and what things would be blocked.

Modern EDR tools have a default configuration that will work for most organisations, however, taking some time to ensure it is working correctly on your devices will minimise any business impact. Allow a period of time (maybe 30 days or so), to watch what's happening and refine the configuration of the tool. Once you are confident that you will not block legitimate business processes, switch the tool to block mode.

TIP: ***If possible when deploying a new EDR, work with a person or organisation who knows and understands how the tool works for support and advice.***

When something is blocked or triggers an alert, you need to have a plan in place for how to respond. It is crucial to develop and maintain an incident response plan and process before an event happens.

CERT NZ has a guide on how to develop an incident response plan on its website.

www.cert.govt.nz/business/guides/incident-response-plan

It's important to figure out these processes before choosing which tool is right for your organisation, to ensure they work for your system and the software you'll be running

Find out more information here:

- www.cert.gov.to
- www.cert.govt.nz

CERT Tonga

certnz