armadillo

The Evolution of Anti-Virus – 2019

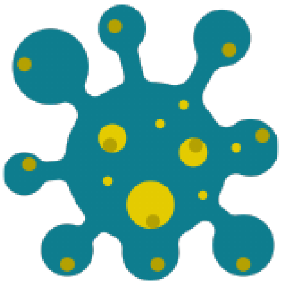
Traditional Anti-virus and 'Endpoint Protection Platforms'

For many years, anti-virus has been reactive. A new virus is written, causes damage and is submitted to one of the anti-virus vendors as a sample. The sample is de-constructed, and the individual characteristics are turned into a 'signature' which uniquely describes the malware and can be used to detect future instances. Scans are generally done either at run time, on a scheduled basis, or both.

In recent years, these products have added other features to augment the scanning capability such as personal firewall, port control and device control to create an 'Endpoint Protection Platform'. Nevertheless, as over 350,000 new malicious programmes are detected every day, the reactive approach leaves organisations open to risk. Anti-virus creation kits can be downloaded from the internet which take an existing virus and obfuscate the code, creating a completely new signature which bypasses anti-virus. Organisations who are regularly targeted will be subjected to targeted malware which is usually not detected by traditional anti-virus.

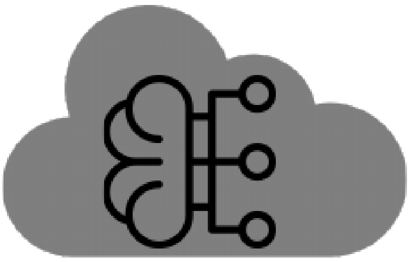
One method which is recommended for organisations who are not ready to progress to 'Next-Gen' anti-virus, is to use multiple scanning engines to increase detection rate. For example, you can use one scanning engine on inbound email, and a different engine on the endpoint. Vendors are emerging which allow the use of parallel scanning across different scanning engines on the endpoint, which increases detection rate, although the same challenges remain with new and targeted threats.

Traditional Anti-Virus



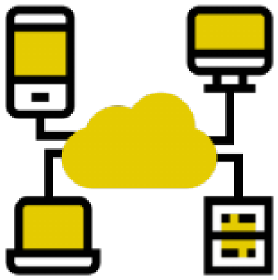
- Reactive
- Open to risk
- Targeted malware usually not detected

Next Gen Anti-Virus



- Machine learning
- No need for signatures
- Managed from cloud
- Only a few updates a year

Next Gen AV & EDR



- Extended visibility
- Central console
- Detect anomalies
- Restores encrypted files

'Next Generation' Anti-virus

In an attempt to resolve the issues with traditional anti-virus, 'Next-Gen' anti-virus leverages machine learning to try to detect malware without the need for signatures. Supervised machine learning is where millions of samples of known bad malware are fed into an algorithm alongside millions of samples of known good files. The machine learning algorithm then looks for commonalities which indicate features commonly used in good and bad programs, and these indicators can then be detected in any new malware sample.

The lack of signatures is also helpful as this means updates only need to be pushed out to clients a few times per year, rather than daily with traditional products. When users are working remotely, outside of the corporate network, this is an important distinction.

Many of these products are managed from a cloud-based portal, which can simplify management in large organisations.

Endpoint Detection & Response

The current state of the art in this area is Endpoint Detection & Response (EDR). As anti-virus requires the installation of client software onto endpoints, it makes sense to use the vast amount of information an agent can collect to extend your visibility into threats across the organisation. These endpoint agents can work together, usually via a central console to detect anomalies and monitor the spread of malware across the organisation. EDR will also try to contain the spread of the malware and even remediate the damage, by restoring encrypted files, for example. EDR solutions are best utilised where the organisation has a mature Security Operations Centre (SOC) who can use the tool for threat hunting, or when outsourced to a managed security services provider.