bettercloud
LET'S MAKE THINGS BETTER

Bigger. Better. Faster. Stronger. UK Business.

Do I ***really*** need to replace my antivirus for EndPoint Protection in 2017?

By Ian Taylor, BetterCloud Services.

In order to make sense of this question we firstly need to understand the differences between a 'virus' and 'malware'. Viruses are a type of malware (specifically designed to replicate and spread), while malware, or 'malicious software' itself, is a broader term used to describe all sorts of unwanted or malicious code.

Malware can therefore of course include viruses, adware, spyware, trojans, nagware, worms, and other types of threat. However, as viruses have been making headlines for a number of years now, the security industry has focused much of its marketing in this area, hence why they are called 'antivirus'.

And the most vulnerable and exploited entry point for the most damaging attacks to businesses: malware, ransomware, and Social Engineering, is the EndPoint Device.

Today **the National Counterintelligence and Security Centre (NCSC)** states 91% of successful data breaches start with attackers infecting an EndPoint via a phishing attack (see below explanation). Many of these are now targeted as specific and seemingly personal by design, (known as 'spear-phishing') at the C-Suite - yet many organisations still believe that antivirus software alone is still an effective means of defending EndPoint Devices.

Antivirus software alone is simply not enough to protect an organisation today.

If your company relies solely on Antivirus then you are relying on a 1990's technology created back then to combat a threat that has been innovating itself for two decades. The threat has been consistently accelerating its ability to avoid detection over many years and, as antivirus software relies on a file-match capability, (known as 'signature match') - to detect potential files that could contain malware, this approach to protecting EndPoint Devices is no longer viable.

Out of date AV. Why is this?

The latest malware statistics suggest on average there are a minimum of ***390,000 new unique samples of malware created daily,*** that's over 2.7m additional variations every week, according to independent IT Security Testing Institute, **AV-Test.**

Looking at this logically, a traditional antivirus approach that needs to build 'signatures' for each sample could never keep pace with this volume of new malware each week. But that is not the end of the bad news in this area. New malware variants are also increasingly using 'file-less' means as their transport mechanism, completely neutering existing antivirus only software methods.

There's no escaping the facts here. Using antivirus protection alone means that you are vulnerable, right now.

To frame how much of a desperate situation the business world could be facing, contingencies for when a breach happens are becoming a regular conversation across board-level risk management discussions and documented procedures. For some time now the question being asked of every **Chief Information Security Officer (CISO)** or equivalent is 'what are we actually doing about this?' The answer should involve a heavy emphasis on protecting EndPoint Devices.

bettercloud
LET'S MAKE THINGS BETTER

So what type of attacks can we expect?

One fact which is certain and without doubt is that your IT environments most unregulated parts are indeed your EndPoint Devices, as when these are largely unprotected they provide a direct open doorway to your data. We are all vulnerable when critical Endpoints are exposed and, of course, there's more than money and data at stake.

Across Healthcare systems and infrastructure to the very heart of our own public personal information (linking heavily into the exposure the new GDPR regulations create), todays modern hackers know no limits. And, an even worse scenario is created by our seemingly 21st Century borderless world, making us even more vulnerable to attack.

As we reviewed earlier in this paper, modern attack methods have made antivirus protection far less effective than it was previously, and evermore sophisticated criminals have learned to slip past antivirus measures, or avoid them altogether.

Two very real examples of common modern attacks now taking the place at scale, and on a daily basis, are summarised below:

- ***Spear Phishing and Social Engineering*** – regularly typified by criminals who send emails that appear to be from a legitimate source, such as banks, credit card issuers or work colleagues. Through this method attackers attempt to gain the trust of the victim, elevating the likeliness that the malware will be clicked and injected onto the EndPoint Device. Once this happens the malware runs in the background, and concerningly, morphs itself to avoid antivirus detection
- ***Malware Innovation*** – in this area using the concept of signatures to prevent malware is simply not feasible knowing that there are now hundreds of thousands of new samples generated each day. Evolution towards file-less malware paired with use of new obfuscation techniques like 'packers' or 'wrappers' means today's antivirus is so far from fit for purpose it actually becomes completely useless altogether as a new method becomes required to counter these seemingly ever strengthening attacks

Building on the above concerns, there are many other scenarios which threaten our organisational security antivirus measures won't stop during our normal day to day activities, as highlighted below:

- ***High Street free Wifi*** – regular everyday team connections for their laptops, tablets and smartphones to the Internet from coffee shops, airports, hotels, home offices etc. These connections are made outside of corporate firewalls (through networks controlled by unknown third parties), and as such now the open up employee assets to all manner of undiagnosed threats
- ***Public FileShare*** —Shared personal video through facilities such as a DropBox account in the Cloud allow malware to be embedded in the download to start infiltrating your contacts, key files and of course, other sensitive information
- ***Downloading Apps*** – When we allow users to download applications from the web although this can create a path to achieving faster innovation we do not know for sure what else being paired alongside the download. Control over the software running on devices connected to your network is essential. If you do not have full visibility then malware can easily creep in through this open door
- ***Thumb Drives*** - Infected USB memory sticks avoid common security gates like firewalls. Many company's security teams simply never get alerted to rogue USB sticks inserted into network-connected devices
- ***Search engines on the Internet*** — Providing users access to the web is mandatory for businesses to operate in today's world however providing unrestricted access is a recipe for disaster

bettercloud
LET'S MAKE THINGS BETTER

More evidence that this criminal activity is developing into a growing and sustainable industry is the formation of online hacker communities, many of which are openly providing free open-source malware and development toolkits for ongoing development and distribution.

These same communities share information among members, often citing common work-around methods for defeating anti-virus software ensuring attackers already know how to defeat your antivirus tools – and they will be successful, unless further steps around wiser investments are taken by organisations worldwide.

Relying on antivirus software alone today can be equated to the proverbial act of burying your head in the sand, in the hope that the attackers, using advanced methods of infiltration, will simply, not find you.

What does the ideal EndPoint Security Platform look like?

The very real need to invest in next generation EndPoint Security is obvious and whilst some attacks are aimed at acquiring the corporations IP assets, the majority are designed with financial gain in mind through ransomware-fuelled extortion and fraud.

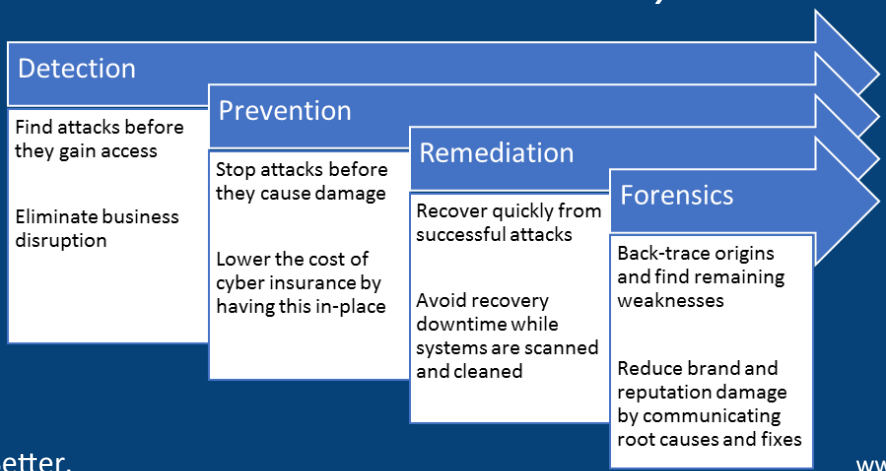
EndPoint attacks are becoming highly targeted, with seemingly consistent ability to capture or destroy valuable corporate assets, significantly impacting an organisation and its ongoing ability to operate. The recent progression of attacks through to mid 2017 has revealed a range of dominant adversary intent to infiltrate organisations at the highest possible levels.

One question naturally in the minds of organisations today is whether there is a single EndPoint Security Platform capable of covering all of the scenarios outlined in the previous section of this paper? We know from experience in this area too that it can be an absolutely daunting task in determining how much EndPoint Security a company may require in order to maintain protection in such threateningly uncertain times.

Providers should in our opinion include in their software the following minimum capabilities and approach to this growing and considered threat to public and private enterprise worldwide:

- ***Detection*** – the ability to predict malicious content and stop it from executing. And if it can't be stopped before execution, sense when an attack is happening by closely monitoring the system, looking for malicious behaviours
- ***Prevention*** – the ability to automatically enact countermeasures - killing malicious processes and quarantining devices, to thwart the attack from achieving its objectives
- ***Remediation*** – the ability to automatically return systems to their pre-attack state, restoring full functionality, thus reducing costs and productivity drain associated with system downtime
- ***Forensics*** – the ability to trace back all actions and instances that led to the attack being successful. This helps determine where weaknesses still persist so they can be addressed

The four categories of EndPoint Protection listed above form a ***Security Value Chain*** that is illustrated below.



bettercloud
LET'S MAKE THINGS BETTER

Any viable platform solution to the significant and growing challenges posed by the increasing volume and sophistication of malware needs to incorporate best-of-breed practices from every aspect of EndPoint Protection.

Additionally, the solution must cover malware of every variety and description, including of course, file-less malware. It also must combine the attributes of defence-in-depth across a single vendor integrated platform to incorporate mechanisms to deal with malware before it executes ***(Pre-Execution),*** while it's executing ***(On-Execution),*** and after it has executed ***(Post-Execution).***

Pre-Execution. This should ideally incorporate cloud intelligence to block all known bad programs and utilise advanced Machine-learning algorithms to extrapolate binaries to identify malicious files.

On-Execution. This part of the solution should identify malicious behaviours from any malware that gets past the automated blacklisting phase. Even file-less malware must undertake certain actions in order to compromise and exfiltrate data. This stage is where it stops

Post-Execution. Here the threats are automatically mitigated and the machine-learning algorithm automatically programs itself to recognise and terminate any previously-unknown malware. Administrators are provided with a comprehensive view of the malware's attack path, and can use the EndPoint Security application to manually or automatically roll back any changes

In closing this paper Better**Cloud** submits the ideal EndPoint Security Platform will have all of the following attributes and will deliver without compromise.

- Scalable, Cloud and On-Premise Management, Offline Support, and a Robust API
- Utilise behavioural, machine-based models that can truly detect almost any type of attack without any prior knowledge
- A single, holistic, lightweight and high-performance agent across delivering security in real-time on the device, and fully autonomous
- A solution that can serve either as a platform or as an integrator itself
- Recognised proven industry compliance through such organisations as Gartner, NSS Labs, AV-Test, AV-Comparatives, MRG Effitas, PCI-DSS, and HIPAA
- A solution built for the threats of tomorrow, utilising behaviour + AI with an equally important focus around product architecture, infrastructure, and usability

and finally but perhaps more poignantly in the eyes of customers ..

- A company which puts its *'money where its mouth is'* through a realistic ransomware warranty program

We here at Better**Cloud** work with a Security Platform Vendor who provides all of these elements, and more, so come and talk with us about your EndPoint Device Security concerns, soon.

Let's Make Things Better.

www.bettercloudservices.com