SentinelOne
The future of endpoint security

# The CISO's Guide to Getting Your Endpoint Protection Out of the 90's

## Executive Summary

Endpoint devices are the most vulnerable and exploited entry-point for the most damaging attacks to businesses: malware, ransomware, and Social Engineering... According to the National Counterintelligence and Security Center (NCSC), 91% of successful data breaches start with attackers infecting an endpoint via a phishing attack – many of which are now targeted (spear-phishing) at the C-Suite.

As recent data breaches have shown, significant financial, reputational, and personal damage can result, making it imperative that the Information Security team is equipped to respond. The response must be up to the task of dealing with the rapidly increasing level of sophistication that characterizes modern attacks.

Too many organizations fall victim to the belief that antivirus software is still an effective means of defending endpoint devices, it is not. If this is all your organization is doing today, you are relying on a technology created in 1990's to combat a threat that has been innovating itself for two decades, and is accelerating its ability to avoid detection. Antivirus software relies on a file-match capability, called "signature match" - to detect potential files that could contain malware. This approach to protecting endpoint devices is no longer viable.

Why? The latest malware statistics tell the story. AV-Test, The Independent IT Security Testing Institute, says on average there are 390,000 unique samples of malware created daily. A traditional antivirus approach that needs to build "signatures" for each sample could never keep pace with this volume of new malware.

To make matters worse, new malware variants are increasingly using fileless means as their transport mechanism, completely neutering antivirus software methods.

The bottom line: If you don't know what your organization is doing to protect endpoint devices, you are vulnerable. Thinking that your antivirus protection is enough means that you are vulnerable. Thinking that you will avoid being attacked – the proverbial "it won't happen to me" folly – means that you are vulnerable.

Contingencies for WHEN (not IF) a breach happens are becoming a mainstay of board-level risk management discussions and documented procedures. The question, therefore, is “What are we doing about it?” This question should be asked of every Chief Information Security Officer (CISO) or equivalent… and the answer should involve a heavy emphasis on protecting endpoint devices.

## Endpoint Security Primer – What You Need to Know

Anywhere that sensitive business information or systems exists, so too exists the threat of unauthorized access by attackers intent on using it for financial, political, ideological, or personal gain. As the use of computing devices has expanded in the workplace – with the proliferation of PCs, laptops, tablets, USB memory sticks, smartphones, and “wearable” devices – so too has the threat of unauthorized access to information.

The impact that malware can have is potentially catastrophic (when an entire network is compromised), but typically results in nagging, difficult to measure damage in the form of loss of business productivity. As systems are brought down, first by the malware, and then by the time and effort required to fix them, staff productivity takes a double-hit - both to the affected employee as well as to the IT staff tasked with an unplanned machine repair. To compound this, there is the data loss that occurs if uninfected information on the machine was not properly backed-up prior to the attack.

In short, there are now more entry points for attackers, made possible by the growing number of endpoint devices connected to the corporate network. This has fueled the rapid growth and increasing sophistication of attacks and defensive measures, which has accelerated dramatically in just the last few years.

Figure 1

EFFECT

- Dumb terminals
- First PCs arrive on desktops
- Networks are private

- PCs on most desktops
- PC networks connect to internet
- Email is the new normal

- Laptops and USB sticks
- Mobile devices connect to networks
- Mobile phones enter workplace

- Smartphones and "wearable" devices connect to the network
- Wireless networks are the norm
- IT does not control software in use
- Remote workers connect via home networks

| Anti-virus | Encryption | Anti-malware | Advanced Endpoint Protection |
|---|---|---|---|

CAUSE

- The term "Computer Virus" is coined
- First PC viruses detected
- First ransomware detected

- "Morphing" viruses found
- VIruses attached to emails
- Viruses found in MS Word & Excel

- First "Social Engineering"
- Viruses send themselves via email
- Malware logs keystrokes
- Mass virus attacks

- Attacks become targeted
- Endpoint and "phishing" email are top threats
- Malware delivered via downloadable apps
- Attacks target C-Suite
- Ransomware hits business
- Nation state attacks target corporate IP

As shown in Figure 1, viruses and malware have continuously evolved to exploit the vulnerabilities of endpoint devices. In response to growing attacks, antivirus software for business was developed and released in the early 90's. As virus and malware sophistication increased, new antivirus methods such as "signature detection", "black/white listing", and "pattern matching" based on known malicious file formats and characteristics rapidly became the norm. Over time, encryption, anti-malware, intrusion detection, web filtering, and email security solutions have entered the market.

In just the past year, according to the Verizon Data Breach Investigation Report, phishing attacks via email account for the majority of successful data breaches. The consequences happen fast – as stated in the report: "30% of phishing messages were opened by the target across all campaigns."It gets worse, "About 12% went on to click the malicious attachment or link and thus enabled the attack to succeed." This represents a 22% increase in phishing effectiveness versus 2015, which means the level of sophistication is increasing.

## Case-in-Point

Take, for example, the case of the CFO who received an email from her CEO requesting that a bank transfer of $60,000 be sent to a partner in Denmark. Everything seemed normal. The CEO's email was from his email address, the partner was a long-standing reseller, and the bank information and account numbers checked out to be a large commercial bank in Copenhagen. The email was an ordinary request that occurred occasionally when the CEO was meeting with partners in Europe.

The only problem was that the CEO's email account had been hacked that morning. The email to the CFO was fake and was constructed using information from the company's web site where the reseller partner organizations were listed. Minutes after the transfer went through, the CEO replied thanking the CFO, and sheepishly admitting that he had made a mistake and needed another transfer in the amount of $120,000 to be sent!

So, the CFO sent it. A few hours later, when the real CEO called to inquire about how the day was going, and only when the CFO mentioned in passing that the transfers had gone through without a hitch, did the breach become known. Within minutes, inquiries to the bank were made only to learn that the account had been drained of all $180,000, and closed within minutes of the last transfer.

# Why Do I Need to Replace Antivirus?

Modern attack methods have made antivirus protection far less effective than it once was. Sophisticated adversaries have learned to slip past antivirus measures or avoid them altogether.

Modern attacks are now taking the form of "Advanced Targeted Threats", such as:

- **Spear Phishing" and "Social Engineering"** – Exemplified by adversaries who send emails that appear to be from legitimate sources, like a bank or credit card issuer, or worse, from a colleague such as the example above. Through these means, the attacker gains the trust of the targeted victim, and elevates the likeliness that the malware will be "clicked" and injected onto the endpoint device. Once there, the malware can run in the background, morphing itself to avoid antivirus detection. The attacker can also begin to use the credentials of the victim's accounts to wreak additional havoc.
- **Malware Innovation** – The concept of using signatures to prevent malware is simply not feasible knowing that there are now hundreds of thousands of new samples generated daily. Evolution towards fileless malware paired with use of new obfuscation techniques like "packers" or "wrappers" means today's antivirus doesn't stand a chance. A new method is required to counter these new realities.

Adversaries have begun to form online hacker communities where free open-source malware and development toolkits are developed and distributed. These same communities share information among members, often citing common work-around methods for defeating anti-virus software. Attackers who already know how to defeat your antivirus tools will be successful, unless you take further steps. Remaining reliant solely on antivirus software is like burying your head in the sand, hoping that the adversaries using advanced methods will not find you (Figure 2).

In addition to spear phishing and use of new, advanced malware, there are several other threat scenarios that antivirus measures won't stop:

- **I attended the web meeting from Starbucks!** Your team connects their laptops, tablets and smartphones to the Internet from anywhere – coffee shops, airports, hotels, and home offices. The connections are made outside of the corporate firewall, through networks controlled by unknown third parties. The corporate firewall used to be enough to protect the devices connecting to your network. Not any more. Now the Barista at the café might be lurking in your network.
- **That video is hilarious!** Your friend's video, shared through a DropBox account in the cloud, kept you in stitches for ten minutes… While the malware embedded in the download started exfiltrating your contacts, key files and other sensitive information.
- **There's an app for that!** Allowing users to download applications from the web may be a path to achieving faster innovation, but… what else is riding along with the downloads? Do you have control over the software running on devices connected to your network? If not, malware can easily creep in through this open door.
- **Put it on a stick!** USB memory sticks are prevalent. Infected USB memory sticks are too, and they avoid common security gates like firewalls. Does your security team get alerted when rogue USB sticks are inserted into network connected devices?
- **Just Google it!** The web is the number one resource for professionals in almost all industries and job roles. Providing users with access to the web is mandatory for businesses to operate in today's world. Providing unrestricted access is a recipe for disaster.

Given the scenarios described above, the need for a more comprehensive means of protecting the endpoint is obvious. The range of solutions and options is expanding rapidly, making it difficult to know what is the right approach for your organization. A means of assessing the value to the organization is a useful component to start with, as described in the following section.

## How to Assess the Value of Advanced Endpoint Security Solutions

Modern attack methods have made antivirus protection far less effective than it once was. Sophisticated adversaries have learned to slip past antivirus measures, or avoid them altogether.

Solutions from leading endpoint providers should include a means for the following functions:

- **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 behaviors.
- **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 the 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 in Figure 3 below.

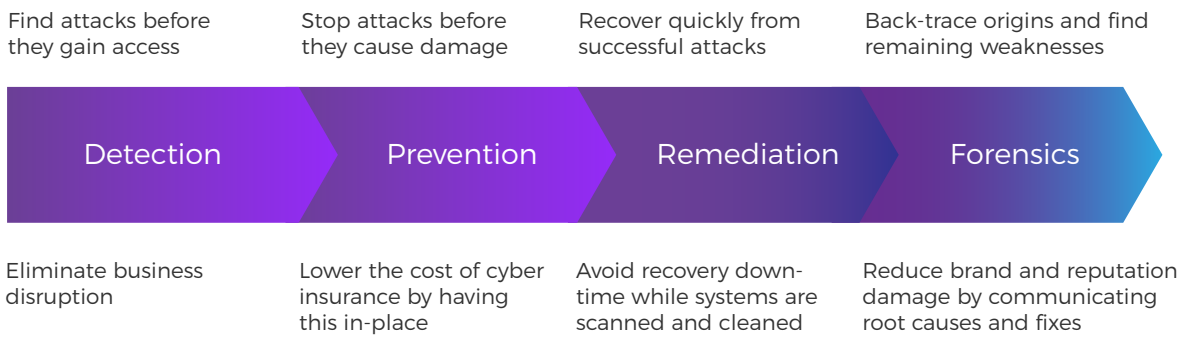


Figure 2: The Endpoint Security Value Chain

Endpoint attacks have become highly targeted, aiming to efficiently capture or destroy valuable corporate assets that can materially impact an organization. The vulnerabilities this represents to the company are numerous, and include:

- **Customer Loyalty-** Breaches become a public relations fiasco and erode customer trust. Recovery can take years and competitors gain a new weapon against you. This alone should justify a next-generation endpoint solution.
- **Brand Reputation –** In addition to the customer challenges described above, your good brand reputation is essential in attracting and growing trading partners and doing business within your industry. Suppliers, vendors and resellers want to know that their data, when shared with your organization, will be safe.
- **Share Price-** Recent breaches have illustrated the impact that they can have on share prices, many of which caused declines that took 2-3 years from which to recover, if at all.
- **Downtime Costs-** When systems must be taken off-line, the time to replace them with new or temporary machines, and the resulting inefficiencies can bring operations to their knees, especially if the infection is spread within groups or across the enterprise.
- **Employee Dissatisfaction** – A "hidden cost" that can destroy a company. Employees confronted with continual disruptions caused by endpoint breaches, or over-burdensome security can result in defections.
- **Cyber Insurance** – Providers of cyber insurance are becoming increasingly demanding, requiring clients to prove that they have implemented robust endpoint security. Without it, your next loss incurred may not be covered.

The recent progression of attacks have revealed a range of adversary intent – the most dominant being to infiltrate organizations at the highest levels possible. While some attacks are aimed at obtaining corporate IP assets, most are launched by criminals seeking financial gain through ransomware-fueled extortion, as well as fraud of the type described in the Case-in-Point above.

The justification for investing in next generation endpoint security is plainly obvious. Perhaps the most compelling challenge remains the lingering "head in the sand" mentality… one which can only be overcome through education and awareness of the business impact and havoc that an endpoint failure can wreak.

For more information on SentinelOne, visit **www.sentinelone.com.** To schedule a demo tailored for your organization, visit **www.sentinelone.com/contact.**

SentinelOne
The future of endpoint security

For more information about SentinelOne Next-Generation Endpoint Protection Platform and the future of endpoint protection, please visit: sentinelone.com