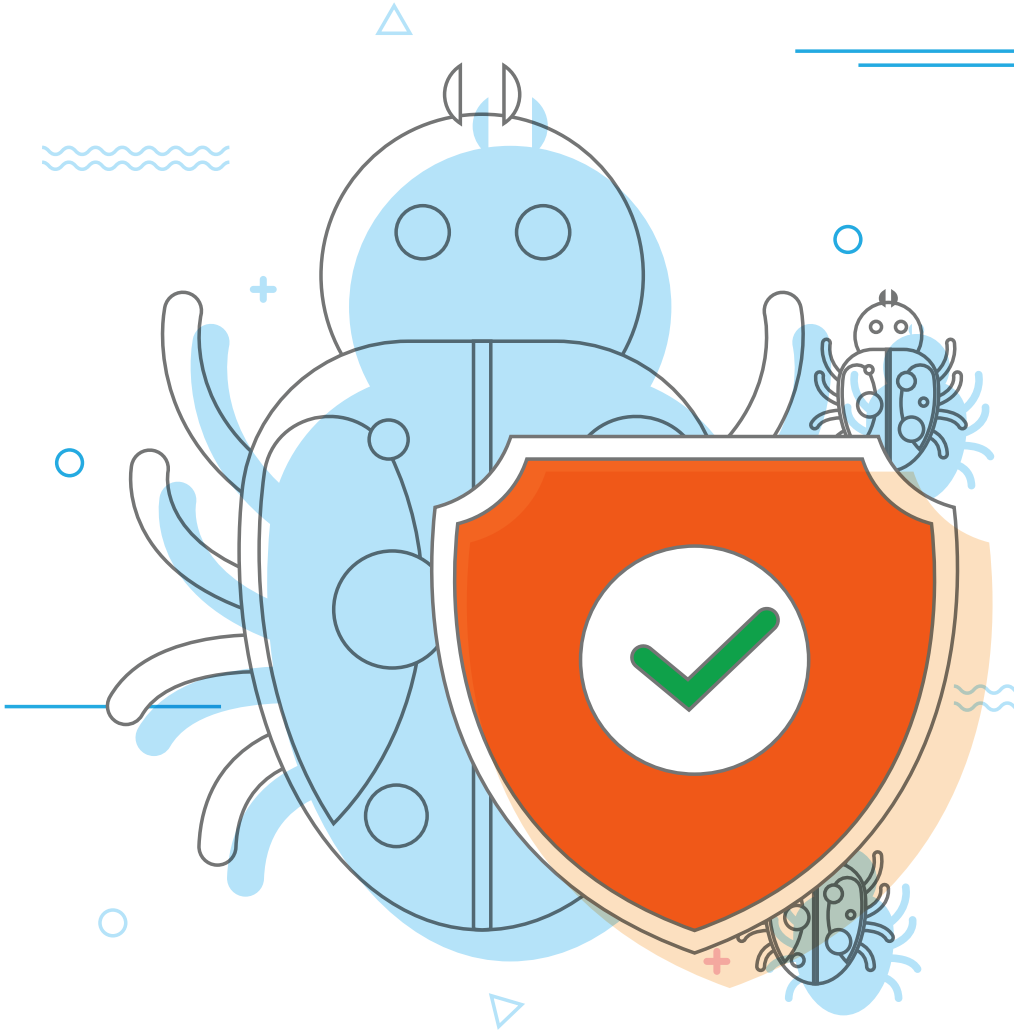
SOPHOS



Why Traditional Antivirus Needs Help

Today's cybersecurity threats are smarter, more targeted, and more dangerous than ever before. Unfortunately, traditional antivirus cannot keep up.

The solution? Defense in depth. One of the best places to start is an endpoint security solution that uses the latest techniques and features such as machine learning and active adversary mitigations to stop modern threats.

This paper will look at the security holes left wide open when relying solely on traditional antivirus, and reviews the modern protection features all organizations need to stop the latest threats.

Antivirus solutions have existed for a long time, and have proven to be very effective at dealing with known threats. Unfortunately, the threat landscape is continually evolving, so relying on traditional antivirus techniques is no longer good enough to stop modern threats such as never-before-seen malware or targeted and blended attacks.

Further illustrating this, a recent Sophos survey of IT managers revealed that 68% of organizations were victims of a cyberattack over the past year, and on average they were hit twice . Simply put, you need endpoint protection that mixes traditional features with next-gen features that are designed to stop the latest attacks.

Traditional antivirus strengths

Signature-based malware detection is highly effective at identifying and blocking malware that has been seen before and thus has a signature. It is effective against executables, but also can be used to detect things like malicious JavaScript on websites.

Application lockdown stops the malicious behaviors of applications, like a weaponized PowerShell command that installs another application and runs it.

Web protection and control identifies and blocks known malicious websites and lets admins control which file types users can download. It also blocks communication with known C2s (command and control servers).

Data loss prevention detects files that attackers are attempting to exfiltrate and blocks them. It does this by monitoring a variety of sensitive data types.

Problem areas for traditional antivirus

Unknown malware, also known as signatureless malware (including polymorphic and metamorphic) is capable of changing its signature to evade protection relying on signatures. Some traditional antivirus solutions have techniques that help detect this type of malware, but they are not foolproof. The speed today at which new, never-seen-before malware is produced further compounds this problem and makes it difficult for traditional antivirus to keep up.

What else do you need? Machine learning capabilities that can identify and block signatureless malware. Machine learning looks at the attributes of the file and compares its "DNA" to millions of samples to understand what is malicious and benign. So even if a malicious file has never been seen before it can be convicted and blocked. This automated approach is highly effective at staying ahead of the copious amounts of new malware.

Fileless/memory-based attacks are also particularly dangerous for solutions relying on signature-based and rules-based detection. Because they don't come as an executable, it is hard for signature-based detection to identify these types of attacks. Host Intrusion Prevention Systems (HIPS) comes into play here but is less effective than modern techniques. These types of attack are becoming increasingly prevalent, with recent examples including Emotet, Trickbot, and Ryuk.

[1]https://secure2.sophos.com/en-us/security-news-trends/whitepapers/gated-wp/uncomfortable-truths-of-endpoint-security.aspx

What else do you need? Exploit prevention and active adversary capabilities that can block fileless and memory-based attacks before attackers gain a foothold on your devices. For example, codecave mitigation, process privilege escalation, and stack pivot protection are all important techniques that are used to stop these types of exploit-based attacks.

Ransomware is a threat everyone has heard of, hitting the headlines repeatedly over the past few years with no sign of slowing down. Many traditional antivirus solutions don't have dedicated anti-ransomware capabilities, so they fall victim to ransomware that is so often used as the payload in attacks. Well known examples include WannaCry, SamSam, and Ryuk.

What else do you need? Anti-ransomware features that can detect and block the malicious encryption of files (without relying on signatures of previously seen ransomware) and roll back affected files to a safe state, minimizing impact on business productivity.

On-premises management can be a weak point even when traditional antivirus has some elements of modern protection. If an active adversary breaches your network, it is much easier for them to compromise your security management system and disable all protection for all endpoints if that management system is run on the same, compromised network.

What else do you need? Cloud-based management lets you manage devices wherever they are and wherever you are. In addition, it is much more difficult for an attacker to compromise a management system that is hosted in the cloud. That's in addition to other features such as multi-factor authentication (MFA) providing additional security to your cloud management console.

Blocking high impact ransomware: traditional and next-gen are better together

As we've seen traditional antivirus solutions mostly lack the features needed to effectively combat modern malware and exploit techniques. In this section let's take a look at a few recent threats, how they work and what's needed to stop them.

Emotet

Emotet first rose to prominence mid-2018, when the U.S. Department for Homeland Security described it as among the most costly and destructive threats to U.S. businesses at the time. The creators are skilled and extremely active, updating the malware tens of times per day. It has three main goals:

1. Spread onto as many machines as possible
2. Send malicious emails to infect other organizations
3. Download a malware payload – commonly banking trojans that will drain your bank account and PayPal accounts, but variants that deploy ransomware or steal passwords also exist

In many cases Emotet also tries to steal data, turning a malware infection into a data breach. Some Emotet variants skim email addresses and names from email client data and archives, likely so they can be sold as part of a wider list and used to spread more malicious spam. Others inspect your web browser, stealing histories and saved usernames and passwords.

Compounding the pain, Emotet can also be a smokescreen for targeted ransomware attacks. While organizations are dealing with Emotet infections, ransomware like Ryuk takes advantage of the distraction to hold the organization's data hostage.

Ryuk

Ryuk ransomware is delivered by a sophisticated, multi-stage attack that paralyzes organizations and demands a significant payment for the return of data – often seven figure sums. It's an example of a 'blended' attack – often Ryuk uses Emotet to compromise an organization before the attackers themselves take over to deliver the payload.

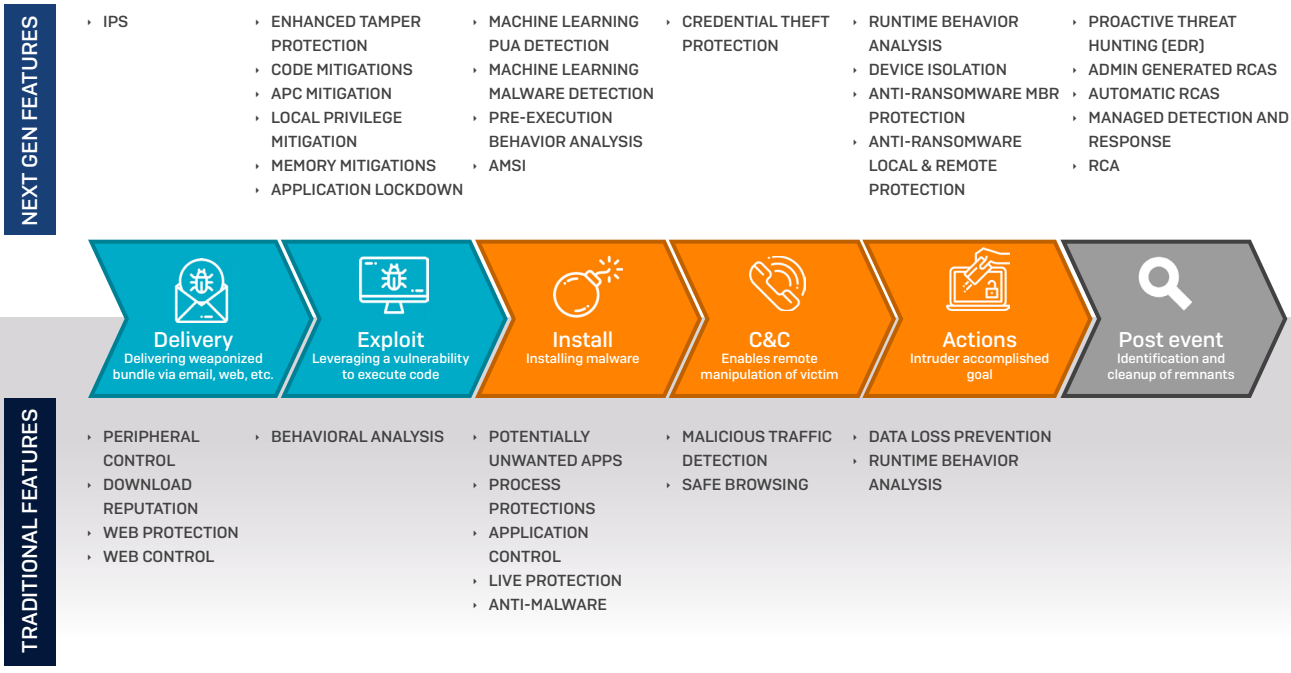
Ryuk attacks are complex. They frequently start with an Emotet or TrickBot attack, delivered via malicious attachments in spam emails, which enables the cybercriminals to get on your network.

Once there, they steal a domain admin user's credentials. With their escalated admin privileges in place, the hackers can move around your network, survey your active directory, and delete your backups.

After removing your safety net, they attempt to disable your cybersecurity products before finally releasing the Ryuk ransomware, encrypting your files and demanding huge ransom payments.

The stages of an attack

Now let's look at the various parts of a typical attack (note that delivery methods and payload may differ depending on the particular strain of malware), what features are needed to stop them, and how traditional and next-gen technology working in conjunction give you the best chance of stopping an attack. It's important to remember that no feature is totally foolproof. Your solution needs to be able to catch and block a threat at each stage of an attack.



As you can see from the diagram, for each stage of an attack, both traditional and next-gen features are present. This is crucial as the combination of technologies provide layered defenses and an even greater opportunity to block a threat at each stage of the attack chain. In short, your solution has to have a combination of traditional and next-gen protection. Relying solely on one or the other is a risky strategy.

Threats are evolving. So should your protection.

Unfortunately, cybersecurity threats are only getting more advanced, so you need protection that can keep up and let you add new functionality and solutions as you need them.

Endpoint Detection and Response (EDR) and Managed Threat Response (MTR)

EDR gives you the tools you need to identify suspicious items and understand whether they pose a threat to your organization and if they need to be cleaned up or can safely be ignored. Used in tandem with strong endpoint protection, it provides an additional layer of security so you can report on your security posture confidently.

The Sophos MTR service gives your organization 24/7/365 threat detection and response, backed by an elite team of threat hunters and response experts who take targeted actions on your behalf to neutralize even the most sophisticated threats.

Management console

It's crucial to have a management console that is easy to use and clearly highlights key information in a logical format, while also making it easy to take action. Plus, you want to be able to manage it from anywhere if something happens while you are out of the office, so cloud-based is the way.

Security that works together

Security ecosystems are the future, so you want solutions that can work together sharing threat intelligence and data to quickly make automated decisions giving you better security. For example, coordination between your firewall and endpoint protection to isolate compromised devices while they are cleaned up or preventing devices from connecting to a compromised server.

Intercept X: Industry-leading protection for your endpoints and servers

Intercept X and Intercept X for Server give your organization unmatched protection for your endpoints and servers, filling the holes left by traditional antivirus and much more.

In addition to protection against the latest malware, ransomware, and exploits, you get detailed visibility with EDR that allows you to investigate and respond to potential threats across your estate.

You can learn more and start a free trial at **Sophos.com/interceptX**

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

19-11-14 WP-EN (MP)

SOPHOS