



SME CYBERSECURITY

An impartial guide to the best malware protection solutions for businesses

Contents

Introduction	1
What is antimalware?	2
How does antimalware work?	4
Top antimalware solutions	7
Layering your protection	13
Secure your business with CyberSmart	15





INTRODUCTION

Malware never sleeps, so your protection can't either

Malware is the catch-all term for malicious software that damages, disrupts, or gives cybercriminals access to a computer system. It comes in many forms – from ransomware and spyware to bots and worms.

Finding effective ways to mitigate malware has never been more important. The AV-TEST Institute registers over 450,000 new malicious programs and potentially unwanted applications (PUA) every day, contributing to the billions of attacks that occur annually.

Large organisations can absorb the financial and reputational blow of a successful attack. However, malware is an existential threat to small and medium-sized businesses (SMEs) with limited resources.

It's no exaggeration to say that effective malware protection solutions, or antimalware, is essential. So, we've put together a list of some of the best solutions so you can surf, click, and work with confidence.



WHAT IS ANTIMALWARE?

Your shield against complex cyber threats

Every business has some form of cybersecurity, even if it's only free antivirus software. Windows Defender comes pre-installed on any device that uses Windows OS, and many businesses are content with this basic level of protection.

However, new threats emerge every day that free, entry-level antivirus software can't deal with. High-quality, dedicated antimalware is a great option for businesses that want a higher level of protection. It works alongside other cybersecurity measures, including antivirus software, to protect your systems against new and advanced threats.



How does antivirus differ from antimalware?

Contrary to popular belief, the two terms aren't interchangeable. But to understand the differences between antivirus and antimalware, you must understand the threats they deal with.

A computer virus is self-replicating malicious code designed to damage the victim's device, for example, corrupting the victim's system or deleting the stored data. Viruses tend to be older, known threats which are easier to identify. Malware covers new, advanced, and constantly evolving threats, which includes some self-replicating threats, like worms. Malware's fluid nature makes it harder to detect and a popular choice for cybercriminals.

Antivirus programs are highly effective at neutralising established computer viruses but offer limited protection against advanced threats. By contrast, antimalware secures your systems against the latest threats, including ransomware, phishing scams, and zero-day attacks.

Naturally, there's some overlap between the two. Premium antivirus software often includes antimalware capabilities and vice versa. However, you'll achieve the best results by combining the two.

Antivirus vs anti-malware

Antivirus

Protects against older, more established threats that are easier to detect and repel.

Antimalware

Defends against a range of sophisticated, emerging, and evolving threats such as ransomware and spyware.



HOW DOES ANTIMALWARE WORK?

Three steps to a secure system

Antimalware follows a three-step process:

Step 1. Detection

The antimalware scans your system, flagging potentially harmful software that's made it past your digital defences. Premium malware protection solutions monitor the internet to identify suspicious websites that may harbour malware. It then blocks you from accessing these sites to reduce the chances of malicious software infiltrating your systems in the first place.

Antimalware typically uses one of three detection methods:



Signature-based detection

In signature-based detection, the antimalware program uses a database of known malware definitions (or signatures) to identify malicious software.

Signatures are essentially a record of the malware's *modus operandi*. The program flags any software that matches a registered signature.

Signature-based detection protects against common threats with similar characteristics, such as keyloggers.



Heuristic analysis

Heuristic analysis identifies malicious software by observing its behaviour and characteristics – [the tell-tale signs that accompany a successful malware attack](#).

Suspicious activity could be anything from encrypting data or removing critical system files without consent.

Heuristic analysis excels at recognising previously undiscovered types of malware, as it doesn't rely on existing threat definitions.



Sandboxing

Sandboxing isolates suspicious software and runs it in an enclosed virtual environment which has limited access to resources, programs, and files.

Once secured, the antimalware monitors the software and either blocks it, if it demonstrates malicious tendencies, or allows it to run normally.

Think of it as a filter that separates legitimate software from harmful counterparts.

Step 2. Removal

The antimalware program removes the suspicious software from the infected system.

Occasionally, cybercriminals program malware to cause additional damage in response to attempted intervention from security programs. In such cases, the antimalware quarantines the file to prevent further damage. You're then free to delete it safely at a later date.

As a rule of thumb, [wait two weeks before deleting a quarantined file](#) to avoid removing legitimate software your antimalware has incorrectly labelled as harmful (a false positive).

Step 3. Repair

The antimalware program repairs any damage caused. Depending on your antimalware program and the severity of the attack, this may include:

- Restoring system files to their original state
- Cleaning up system registries
- Fixing system settings (e.g. network configuration or browser settings)
- Flagging or patching system vulnerabilities
- Monitoring for residual threats



TOP ANTIMALWARE SOLUTIONS

Finding the right malware protection solution for your business

Malware is diverse, and so are the solutions that protect against it.

As with traditional antivirus software, numerous free options exist. But for businesses that need to support multiple users and adhere to rigorous security standards, paid solutions are the only real choice.

Thankfully, there are numerous cost-effective and scalable antimalware solutions that cater to businesses of all sizes. The following is a selection of our top picks based on a combination of professional and user reviews.

#1 Avast Business

Flexible, competitively priced cybersecurity tailor-made for small and medium-sized businesses. [Avast's SME cybersecurity solutions](#) provide robust protection for up to 100 users. It's split into three tiers:

- Essential
- Premium
- Ultimate

The Essential tier lacks some useful features included in the Premium and Ultimate tiers, like web control and patch management. But with reliable endpoint, ransomware, and phishing protection, it's a great starting point for businesses on a budget.

Prices start at £30 per device per year.



Pros

Award-winning malware, phishing, and ransomware protection.

Intuitive online management platform; monitor devices and manage subscriptions from one screen.

Premium and Ultimate tiers include web control, restricting access to potentially harmful websites.



Cons

Complicated, time-consuming installation process.

Full scans take time and can affect PC performance.

Web control, personal VPN, and patch management aren't available on macOS.

#2 Bitdefender GravityZone Business Security

Aimed at budget-conscious SMEs, [Bitdefender GravityZone Business Security](#) offers next-gen cybersecurity that perfectly balances ease of use, performance, and cost.

It consistently ranks number one in independent security tests and provides complete protection against a range of malware threats for up to 100 users, including:

- Ransomware
- Spyware
- Phishing
- Zero-day attacks



Pros

Comprehensive security: prevention, detection, and response.

Provides advanced threat protection, supported by machine learning and behavioural analysis.

On-premises and cloud hosting options available.



Cons

Cloud dashboards are difficult to navigate.

Limited reporting capabilities.

Customer support sometimes slow to respond.

#3 Kaspersky Medium Business Security

[Kaspersky Medium Business Security](#) offers complete system security, with advanced malware protection and managed network security to keep your data safe.

Like many cybersecurity providers, Kaspersky splits its medium business offering into tiers that deliver increasingly advanced levels of protection. This lets you choose the solution that best meets your needs and budget.

Basic protection starts at £180 per year for a minimum of five users.



Pros

Simple, intuitive interface from a single cloud console.

Comprehensive security suite, including endpoint detection and response (EDR), patch management, and ransomware protection.

Scalable, cost-effective protection.



Cons

Resource intensive, which can affect system performance.

Users report compatibility issues with some operating systems.

Customer support can be difficult to reach and slow to respond.

#4 Malwarebytes for Teams

Industry-recognised cybersecurity without the complexity, [Malwarebytes for Teams](#) offers more than standard antivirus or malware protection. It uses intelligent behaviour-based technology to detect and block real-time threats, including brute force attacks, spyware, and ransomware.

Malwarebytes for Teams supports up to 20 users and is compatible with Windows, Mac, Android, and Chromebook. This makes it the ideal solution for one-person operations and small teams.



Pros

Proactively scans for threats using idle CPU resources.

Award-winning malware remediation keeps your systems clean and secure.

Fast installation, with no complicated IT infrastructure.

60-day money-back guarantee.



Cons

Focuses on malware detection and removal, making it less comprehensive than some of the solutions on this list.

Resource-intensive, which may affect system performance.

Limited number of users; unsuitable for medium-sized businesses and enterprises.

#5 Sophos Intercept X

[Sophos Intercept X](#) offers comprehensive enterprise-level endpoint security with various licensing options to suit your needs.

The basic package, Intercept X Advanced, delivers reliable antimalware and exploit protection that harnesses AI to neutralise cyber threats. Premium licensing options add 24/7 extended threat detection and response, securing your enterprise against complex threats.

Sophos keeps its cards close to its chest when it comes to pricing. However, free quotes are available on request.



Pros

- Effective and reliable endpoint protection.
- Industry-leading malware detection and exploit protection defend against old and new threats.
- Intuitive user interface.



Cons

- Less affordable than some solutions on this list. Costs can quickly mount up as you add more advanced functionality.
- Resource intensive.



LAYERING YOUR PROTECTION

Defence in depth is the secret to malware security

Antimalware protects your business against an ever-growing range of cybersecurity threats. The best solutions:

- Flag potentially harmful websites
- Identify and remove malicious software that infiltrates your systems
- Get you back to business as usual, fast

Of course, no solution can guarantee 100% protection. The UK government recommends a layered approach, known as defence in depth. This means employing multiple security measures and controls to reduce your cyber risks. If a threat gets past the first layer, others kick-in to pick up the slack.

“

As with physical and personnel security, cyber security can make use of multiple measures which (when implemented simultaneously) mitigate single points of failure. This approach is commonly referred to as 'defence in depth'. Each measure provides a layer of security and deployed collectively, greatly reduce the likelihood of a cyber incident.

NATIONAL CYBER SECURITY CENTRE

Our advice? Give your malware protection solution a helping hand by installing reliable antivirus software and adopting proven cybersecurity controls, like those featured in the government-backed [Cyber Essentials](#) scheme. Together, they give your business the best chance of staying safe from malware.



SECURE YOUR BUSINESS WITH CYBERSMART

24/7 protection, expert support

CyberSmart is an all-in-one cybersecurity monitoring, optimisation, training and insurance solution proven to defend against the unexpected. Our everyday cyber protection stops threats dead in their tracks and gives you peace of mind with continuous compliance and round-the-clock protection.

We're also the UK's largest provider of cybersecurity accreditations, making us the perfect partner to help your business achieve complete cyber confidence.

Prevention is the best defence

Stay safe from online threats with our tried and tested malware prevention tips.

[Read the guide](#)