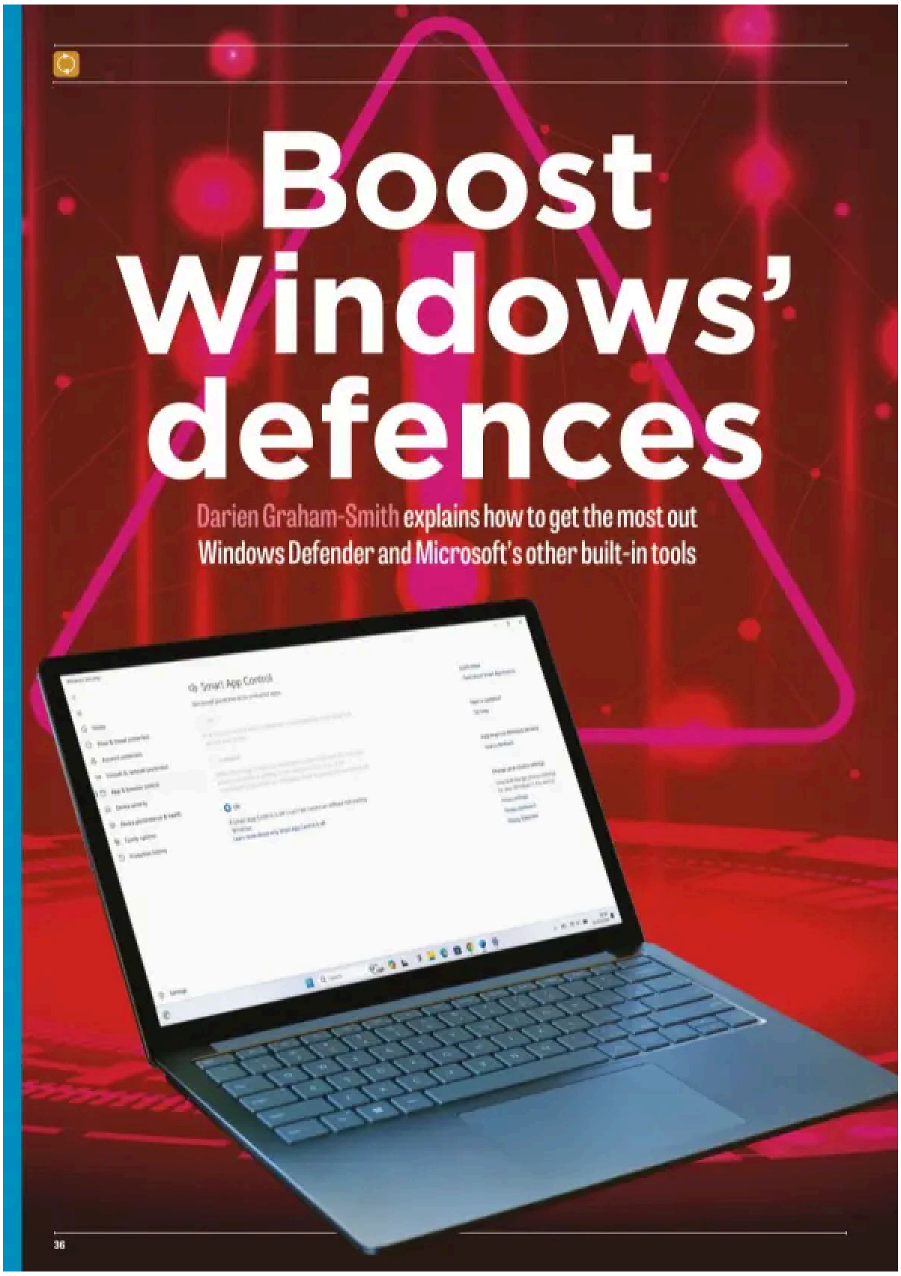
- Windows Defender Firewall / Utilities (Computer software)

Boost Window's defences

Darien Graham-Smith explains how to get the most out Windows Defender and Microsoft's other built-in tools

PC Pro · 1 Mar 2024 · 36

Windows Defender is built into Windows 10 and 11, but are you taking full advantage of its power? Darien Graham-Smith explains the background and reveals how to get more from it.



Boost Windows' defences

Darien Graham-Smith explains how to get the most out Windows Defender and Microsoft's other built-in tools

36

I1 What is Windows Defender?

It's a funny thing: everyone's heard of Windows Defender, but if you search your system, you won't find any program of that name. At least, not if you're running a recent version of Windows 10 or 11.

For more than a decade, though, the OS did include a built-in tool called Defender. In Windows Vista and 7, Defender was a system component that detected and removed spyware from your system; in Windows 8 it was upgraded into a one-stop integrated defence against all types of malware, replacing the optional Microsoft Security Essentials antivirus tool.

Today, Defender has lost its individual identity. Windows 10 introduced a whole spread of new security features, including protection against OS vulnerabilities, intrusion prevention and antiransomware measures. And to house

all of these new features, the new Windows Defender Security Center was created. The Defender app was replaced by a few pages of buttons and drop-down menus, headed
"Virus & threat protection", inside this central Security console. And in the October 2018 update the Defender branding was dropped completely; the app is now known simply as Windows Security.

The Defender name does persist in a few places, however. In the legacy Control Panel interface, the firewall is still referred to as the "Windows Defender Firewall", and as we'll discuss below, the name has been co-opted for various add-on apps and features.

While Defender may have dropped out of sight as a standalone system component, its antivirus engine is still present in the latest versions of Windows, keeping you safer than ever. It just leaves us in a situation where no-one is really sure how to refer to the antivirus component any more: security specialist AV-Test.org continues to refer to Windows Defender, while others such as AV-Comparatives.org and SE Labs UK call it Microsoft Defender Antivirus.

2Windows Security is (probably) all you need

Those security labs specialise in comparative security testing – and they'll all confirm that, in its early days, Windows' native antivirus protection wasn't worthy of the name. As recently as 2018, testers were criticising Defender's mediocre protection, alarming false-positive rate and considerable impact on overall system performance. In issue 291 of PC Pro, published in late 2018, we even ran an 18-page Labs roundup of security suites under the headline "Dump Windows Security now".

That sort of reputation is hard to shake. If you frequent online advice forums today, you'll still see plenty of people rubbishing Defender. But in fact Microsoft has turned things around in recent years. In AV-Test's latest product roundup, Defender was named a "Top Product" (tinyurl.com/ 354avtest), while AV-Comparatives gave Microsoft a two-star protection award – on par with big names such as F-Secure and Norton (tinyurl.com/ 354avcomp). SE Labs gave Defender a triple-A rating, reflecting perfect protection against malware with zero false positives (tinyurl.com/354selabs). In our last Labs test (see issue 343, p85), Defender earned a five-star rating, not only for protection but usability as well.

There are still reasons to choose a third-party security alternative. Independent suites normally include bonus features such as password managers or VPNs, and they're often more user-friendly than Windows Security. However, as our Labs contributor KG Orphanides concluded last year, "for most users concerned about how to best keep Windows safe, Defender does the job as well as anything else".

3 Always up to date

One of the big challenges for antivirus software is "zero day" threats – realworld attacks that exploit previously unknown vulnerabilities. When a zero-day is discovered, the race is on to update everyone's security as quickly as possible and minimise the damage.

That alone might seem like a good reason to steer clear of Defender. Famously, Microsoft only rolls out major security updates once a month, on "Patch Tuesday" – and while you'll sometimes see antivirus signature updates sitting in the regular Update queue, most of us don't make a habit of installing these items manually.

Thankfully, you don't need to. If you don't manually install them, Windows silently installs the latest malware signatures at least once a day. You don't get notified when this happens, simply because you'd be facing a continual procession of interruptions: for example, on Christmas Day 2023 (to pick a date at random) eight new security updates were released.

If that's not reassuring enough for you, Windows also includes a feature called "cloud-delivered protection". You can check it's enabled by opening the Virus & threat protection page in the Windows Security app and clicking the "Manage settings" link.

By default, cloud-delivered protection follows a rule called "block at first sight", which means any unrecognised files are automatically uploaded to Microsoft's servers for immediate analysis before they're allowed to run on your PC. You're protected even against previously unseen dangers – and if Windows suspects a file may contain personal information, you'll be prompted to permit cloud processing before anything is transmitted. If you prefer not to have anything sent to Microsoft, just turn off the switch labelled "Automatic sample submission". t runs on almost every Windows PC, but what exactly does Windows Defender do – and what settings should you be tweaking for the best protection?

Here, we reveal seven tips that not only explain the philosophy (and history) behind Windows Defender, but also how to get the most out of it.

If you frequent online forums today, you'll still see plenty of people rubbishing Defender. But in fact Microsoft has turned things around in recent years

4Turn on ransomware protection

Ransomware is a huge threat to big businesses and personal PCs alike.

It's important to protect your irreplaceable family photos and personal documents, because if you do get hit the ransom demand could run to thousands of pounds.

Hopefully, any ransomware attack should be caught by Windows' antivirus scanner. Windows also encourages you to back up your personal files to OneDrive, where they're safely stored in the cloud, and can be rolled back to previous versions if they're tampered with.

What you may not realise is that Windows Security includes an additional feature that can completely block ransomware before it strikes. Controlled Folder Access prevents any applications from writing to your personal folders – except for programs pre-approved by Microsoft, or manually authorised by you. Even an app running with administrative privileges can't change or delete your data without your approval.

Controlled Folder Access was introduced to the Windows Security Center back in October 2017 – but sadly it's always been turned off by default. You can enable it by opening the Virus & threat protection page of the Windows Security app, clicking the Ransomware protection link and flicking the switch for Controlled folder access.

Once you've done this, you'll see three new links appear, labelled "Block history", "Protected folders" and "Allow an app through Controlled folder access". We recommend you click to review your protected folders, to see which locations are being monitored – and add any extra folders you might want to protect, such as external drives or network storage.

With this done, ransomware should hold no fear for you. However, Controlled Folder Access can interfere with legitimate programs (which is probably why Microsoft doesn't enable it by default). If this happens, you'll see a pop-up alert; click on this to open the Controlled Folder

Access settings and review what's been blocked. If it's something you recognise and trust, click Actions and select "Allow on device" to unblock the affected app.

It is a little bit tiresome that you have to jump into the Windows Security app to find out what apps have been blocked. Third-party suites such as Bitdefender, Trend Micro Internet Security and the free Avast One Essential make it easier to approve access with a click directly from the alert. But if you're sticking with Windows' built-in protections it's a good idea to turn on Controlled Folder Access as soon as possible.

5Anti- phishing everywhere

Another risk that's on the rise is phishing attacks, where fake websites trick you into entering the login details for your bank, email account or corporate network. In reality you're handing your credentials over to an attacker, who can then use your identity to wreak havoc without touching your computer.

Windows Security includes phishing protection as part of its SmartScreen feature: if you try to visit a web address that's been reported as unsafe, you'll see a big red warning page alerting you to the fact. However, this is only built into Microsoft's own Edge browser. If you're using Chrome, you'll get similar warnings from Google's own Safe Browsing system – but you can gain belt-and-braces protection by installing the Microsoft Defender Browser Protection extension from the Chrome Web

Store, which adds SmartScreen warnings to the Google browser.

If you're using Windows 11 Pro, you can also take advantage of a feature called Enhanced Phishing Protection (introduced in the 22H2 update), which will alert you if your Windows password is entered into any untrusted website or application. You can check it's enabled by opening the Windows Security app, navigating to the App & browser control page, clicking on Reputation-based protection, and scrolling down to the Phishing protection settings. Check that the main switch is turned on, and optionally tick "Warn me about password reuse" and "Warn me about unsafe password storage".

6Built- in parental controls

There are plenty of commercial security suites that boast parental controls as part of their premium feature set, but you may be fine with Microsoft's free Family Safety service. Although this is a cloud service, you'll find a link to the web-management dashboard – plus a handy overview of what you can do – on the Family options page of the Windows Security app.

Family Safety features include time limits, app restrictions, website filtering, device tracking and a digital wallet that you can top up to allow your kids to buy online content. You can also set up and access a shared family calendar and a shared OneNote notebook for lists and memos.

The catch is that it's very Microsoftcentric. Shared resources are hosted at outlook.com, and the money you put in kids' wallets can only be used to buy items in the Microsoft and

Xbox stores. To use the full range of parental controls, your kids need to be using Windows PCs or laptops – or signing onto yours with their own

What you may not realise is that Windows Security includes an additional feature that can completely block ransomware before it strikes

Microsoft accounts. There are some controls available for Android devices, but if your kids are using iPads, Fire tablets or Chromebooks – or gaming on other consoles – they're beyond the reach of Family Safety.

It's worth noting, too, that web filtering only works in the Microsoft Edge browser; in all, this is one area where you might want to consider running Windows Security alongside third-party tools.

7Not just for your home PC

Every copy of Windows includes the core antivirus functions, but if you're subscribed to Microsoft 365, you can also take advantage of a separate tool called Microsoft Defender for Individuals (sigh), which serves as a multipurpose security dashboard for Windows, macOS, Android and iOS.

The capabilities of this tool vary from platform to platform. On Windows and iOS, the Defender app is mostly focused on monitoring the security status of all your devices, and logging incidents and notifications along with security tips. On macOS it can scan for viruses, and on Android it will not only scan all the contents of your phone and spot potentially dangerous items, but also monitor your network traffic for suspicious activity and block connections to websites that are known to host malware, or phishing attempts.

There's also a whole spread of Defender-branded tools for big

BELOW Microsoft 365 subscribers can take advantage of additional tools businesses. Defender for Endpoint is a version of the software designed for centralised deployment and management, while Defender for Office 365 scans and secures Office content. Defender for Cloud Apps watches over information that's shared over the internet, and Defender for Identity tracks suspicious account activity. Defender XDR brings all of these elements together in a cloud-based service that automatically identifies and blocks emerging attacks before they can do damage. We've come a long way from Microsoft Security Essentials.

8Easier ways to manage your security

While the Windows Security app brings together a lot of valuable features, it's not exactly a joy to use. Everything's much more spaced-out than it needs to be, and its functions are split up across dozens of different pages and subpages, with little indication of which are important and which you can safely ignore.

If you'd prefer not to use the Windows Security app, you can also launch security actions using PowerShell. Two useful commands are Update-MpSignature and Start-MpScan, which respectively download the latest malware updates and start a system scan.

You can also use the extremely powerful Get-MpPreference and Set-MpPreference commands to check and change a wide range of security settings. Be warned, there are a lot of parameters here: you'll find a full list of PowerShell commands, and further documentation on how to use them, at tinyurl.com/354powershell.

Another alternative is to use a free front-end called ConfigureDefender, which you can download from tinyurl.com/354configure. This thirdparty creation looks rather clunky, but it provides quick access to the most useful security settings via easy drop-down menus – and you can also click to instantly switch between predefined High, Interactive or Maximum security profiles, with built-in help pages to explain the differences between modes.

Microsoft Defender for Individuals serves as a multipurpose security dashboard for Windows, macOS, Android and iOS