Microsoft | intel vPRO PLATFORM | ebuyer business

NEW SOLUTIONS FOR ENDPOINT MANAGEMENT

How endpoint mediates, enables and enhances the workplace

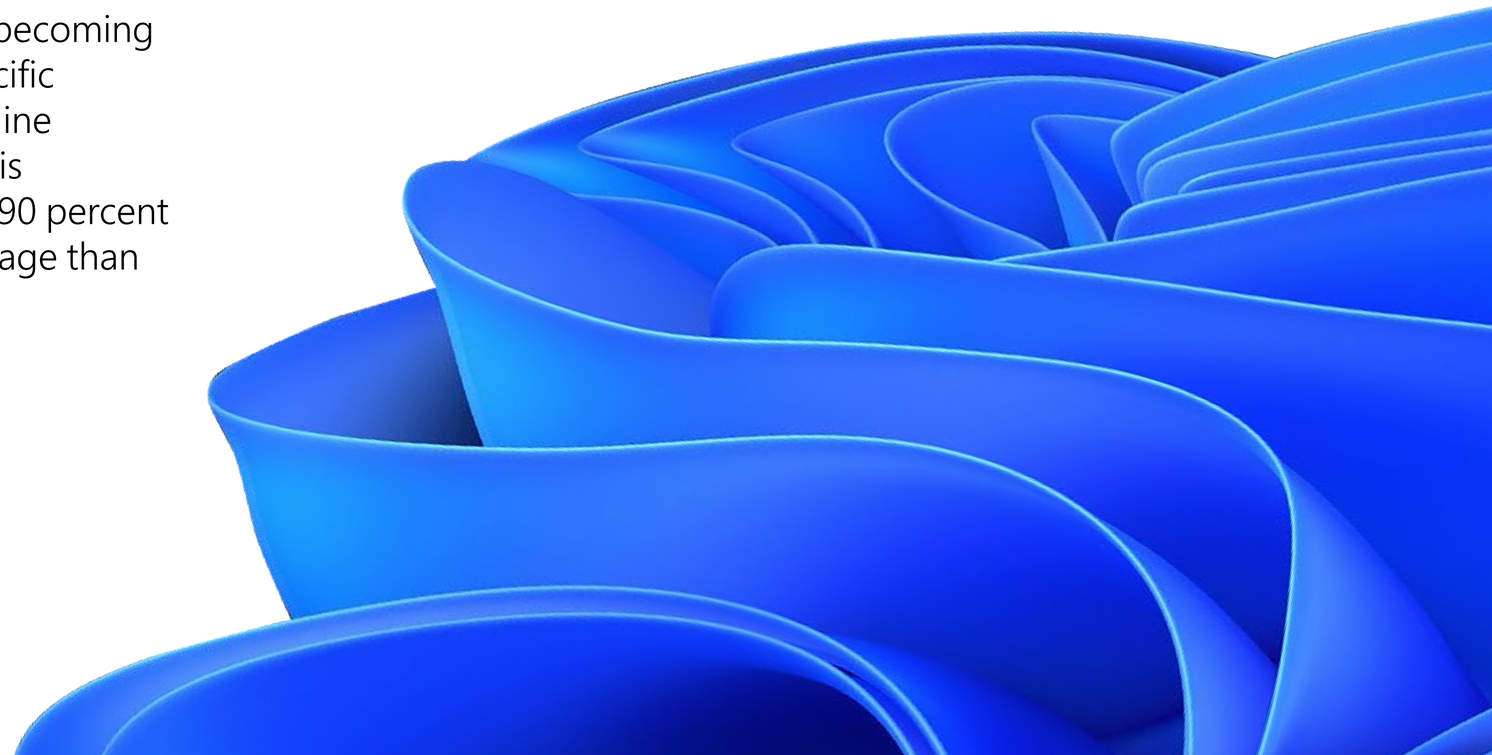
Today's organisations extend far beyond the traditional bricks-and-mortar office, with many employees now routinely using a bewildering array of platforms, applications and devices to get work done. New tools and organisational cultures empower them to work at home or on the go, use their own devices to access company data, and collaborate with colleagues from anywhere.

As we move into this new world of hybrid work, it's becoming clearer that the endpoint is the workplace – in the sense that it mediates, enables and creates the work experience.

This explains why endpoint management and strategy is becoming a key IT focus, with many organisations tailoring role-specific endpoint experiences for their information workers, frontline workers and temporary workers. Undoubtedly, the cloud is powering this transformation; a recent survey found that 90 percent of enterprise respondents now anticipate higher cloud usage than before COVID-19.[1]

For all their strengths, however, the new hybrid working practices present multiple challenges for the IT team. For one thing, they require an integrated cloud service to manage the growing complexity of endpoints. Moreover, a distributed workforce can increase the risk of security incidents such as malware, identity theft, password compromise and other threats. Employees working across multiple devices also raise the risk of security breaches through human error or targeted attacks, or both.

An effective strategy for endpoint management can help by delivering three key organisational goals – a better end-user experience, improved security and better IT efficiency. Let's look at each in more detail.



Improving the end-user experience

In recent years, employers have increasingly attracted and retained staff by offering more flexible conditions, including remote working options. The pandemic has accelerated this trend. Now, with Generation Z entering the workplace, employee expectations can extend to aspects of IT, such as bring your own device (BYOD), open-platform policies and up-to-date tools.

As reported in a recent Forrester Total Economic Impact™ study commissioned by Microsoft[2], a significant contribution to job satisfaction arises from employees' experience of using technology to get work done. Executives and frontline workers alike prefer a smooth and enabling user experience that helps them efficiently complete tasks, almost wherever they're working. Equipping hybrid organisations with modern endpoints is a practical way to improve the end-user experience.

Modern business PCs powered by Intel vPro® platform processors deliver the experience hybrid workers need to do their best work from anywhere. By providing high-performance computing power and functionality across a variety of form factors, the Intel vPro platform provides a secure, premium computing experience that helps end-users work, create and collaborate seamlessly.

Enhanced employee experience can improve the bottom line by generating significant savings.[3] For example, Microsoft Endpoint Manager – which offers improved cloud-powered endpoint security and device management – helps cut the time end-users have to wait for their devices to be provisioned or made compliant. Users can further benefit from devices that run more reliably.

Microsoft Endpoint Manager helps cut the time end-users wait for devices to be provisioned or made compliant.

Microsoft Endpoint Manager comes with built-in analytics tools that also allow organisations to improve the quality of the end-user IT experience. If policies or hardware issues are slowing devices, for example, managers can tackle the problem before users create a help-desk ticket.

In addition to boosting employee satisfaction, reliable and secure modern endpoints can help delight customers and drive trust. Every smooth customer encounter, every rapidly fulfilled order and every responsive client service delivery helps build reputation and customer retention.

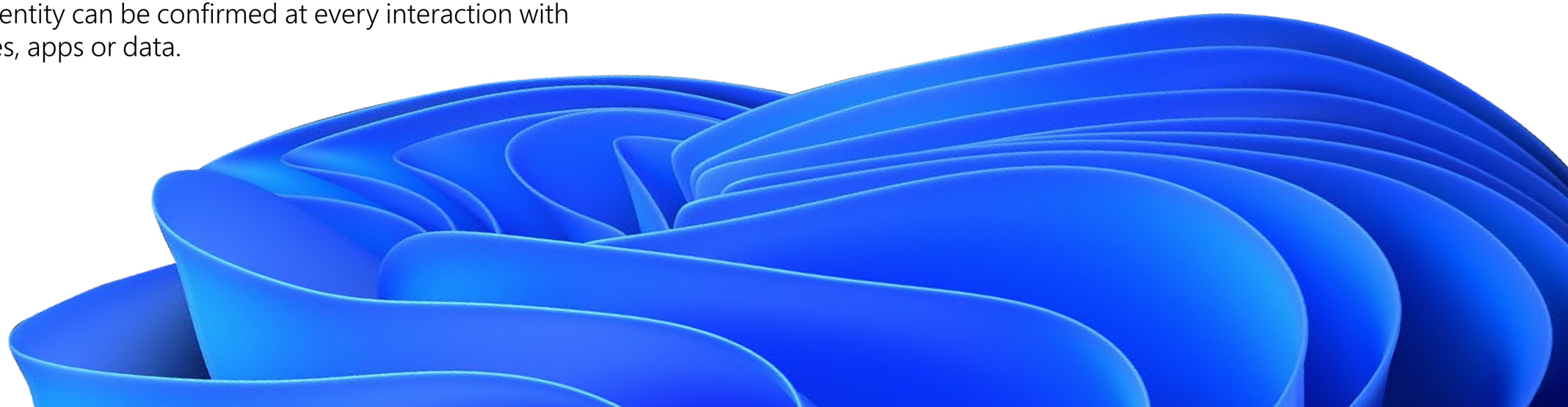
Improving security

For today's cloud-powered hybrid organisations, in which significant workplace traffic occurs over the internet, protecting the 'business perimeter' from threats is no longer enough. A new priority is therefore to secure every touchpoint, from the cloud right down to every endpoint, business or personal, that accesses corporate resources. These endpoints might include office desktops, laptops connecting from home and smartphones used on the move.

Microsoft 'Zero Trust' security model uses identity as the new critical plane of defence. By assuming breach and verifying every access request explicitly, this approach protects people, devices, applications and data, virtually wherever they're located. To help secure all endpoints under a Zero Trust organisational strategy, IT administrators first register and check them against defined policies; after that, user identity can be confirmed at every interaction with network resources, apps or data.

Using the Intel vPro platform, devices can be flexibly configured to tackle even the most demanding workloads reliably and efficiently. And because remote working requires remote management, enhanced cloud-based manageability with Intel® Endpoint Management Assistant (Intel EMA®) enables IT teams to remediate security breaches remotely, with minimal interruptions to end-users – even if they're outside the firewall.

Intel® Endpoint Management Assistant (Intel EMA®) lets IT teams remediate security breaches remotely – even if users are outside the firewall.

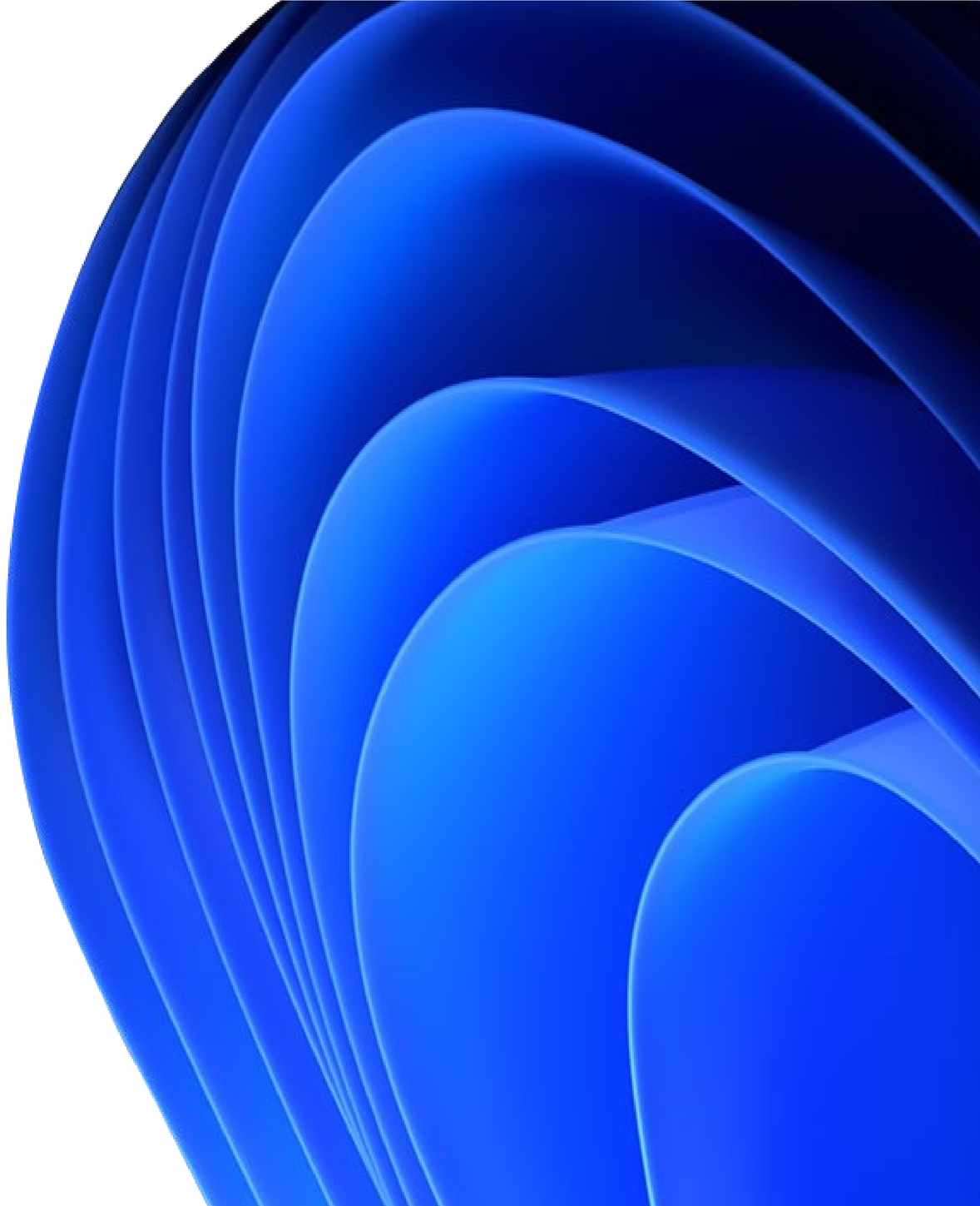


In addition, Microsoft Endpoint Manager helps IT managers protect corporate data and assets while making it easier for employees to do their jobs from almost anywhere. Designed to drive security throughout the hybrid organisation, it gives the IT team visibility into cloud apps being used across the company. It also lets them set policies to ensure staff are using critical security applications, such as Microsoft Defender for Endpoints, which includes anti-virus protection.

Microsoft Windows 11 devices featuring Intel vPro technology also include the BitLocker encryption tool, so IT administrators can easily protect company data, even if a device is lost or stolen. In this case, Microsoft Endpoint Manager will also let you wipe all business data from the device, easily and remotely.

Intel® Hardware Shield provides businesses with the platform assurance and security processes they need to help keep their increasingly mobile workforce safe. Available exclusively on all Intel vPro platform-based devices, it delivers comprehensive hardware-based security with below-the-OS security, application and data protection, and advanced threat detection[4].

Intel Hardware Shield protects below the OS with out-of-the-box protection from firmware-based attacks'



Increasing IT efficiency

We've touched on how Intel® hardware and cloud-powered Microsoft solutions can help drive endpoint security. But when it comes to endpoint deployment and day-to-day management, the Intel vPro platform and Microsoft Endpoint Manager can also significantly lighten the hybrid organisation's IT workload.

Easier deployment

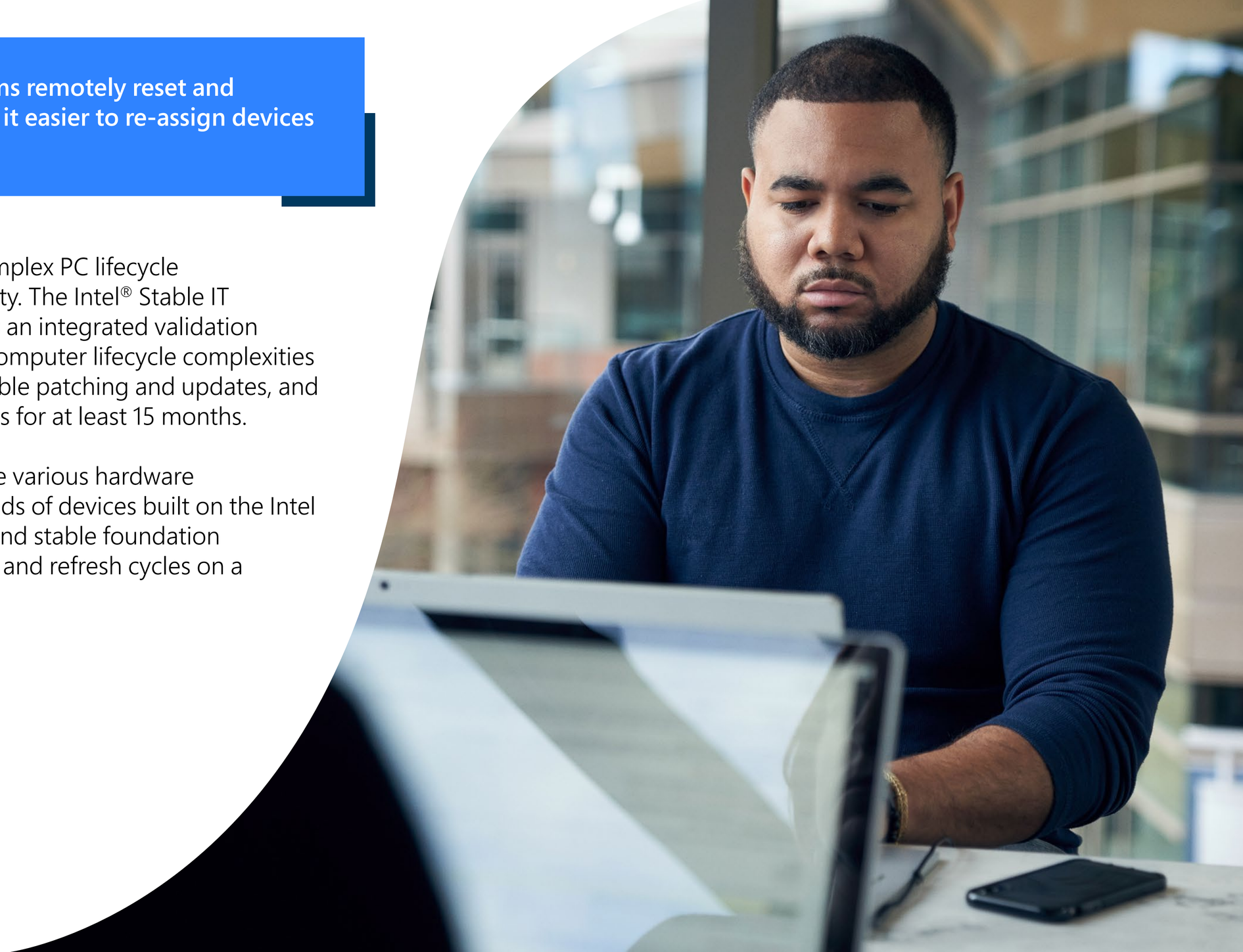
The Microsoft Endpoint Manager platform includes Windows Autopilot, which helps you remotely set up and pre-configure new Windows Pro, Enterprise or Education PCs faster. Autopilot makes it convenient for organisations transitioning to hybrid working, because IT managers don't need to spend time creating images or setting up devices in person. New off-site users can just log in and get to work.

Using Autopilot allows IT administrators to easily auto-configure profiles for certain groups of users or devices. They can also use it to remotely reset and re-purpose endpoints as needed – making it easier to re-assign devices to new employees.

Windows Autopilot lets IT teams remotely reset and re-purpose endpoints, making it easier to re-assign devices to new staff.

Easing the burden of today's complex PC lifecycle management is a business priority. The Intel® Stable IT Platform Program (Intel® SIPP) is an integrated validation platform that helps IT manage computer lifecycle complexities with confidence by offering reliable patching and updates, and no anticipated hardware changes for at least 15 months.

Months of rigorous testing of the various hardware components ensure that all brands of devices built on the Intel vPro platform deliver a reliable and stable foundation for smoother fleet management and refresh cycles on a global scope.



More efficient management

By simplifying the remote monitoring, updating and troubleshooting of PC fleets, the Intel vPro platform minimises the need for the IT team to get hands-on with device hardware, reducing management burdens and cost. Smoother remote fleet management means IT can respond earlier and more effectively to security threats, even with a distributed workforce.

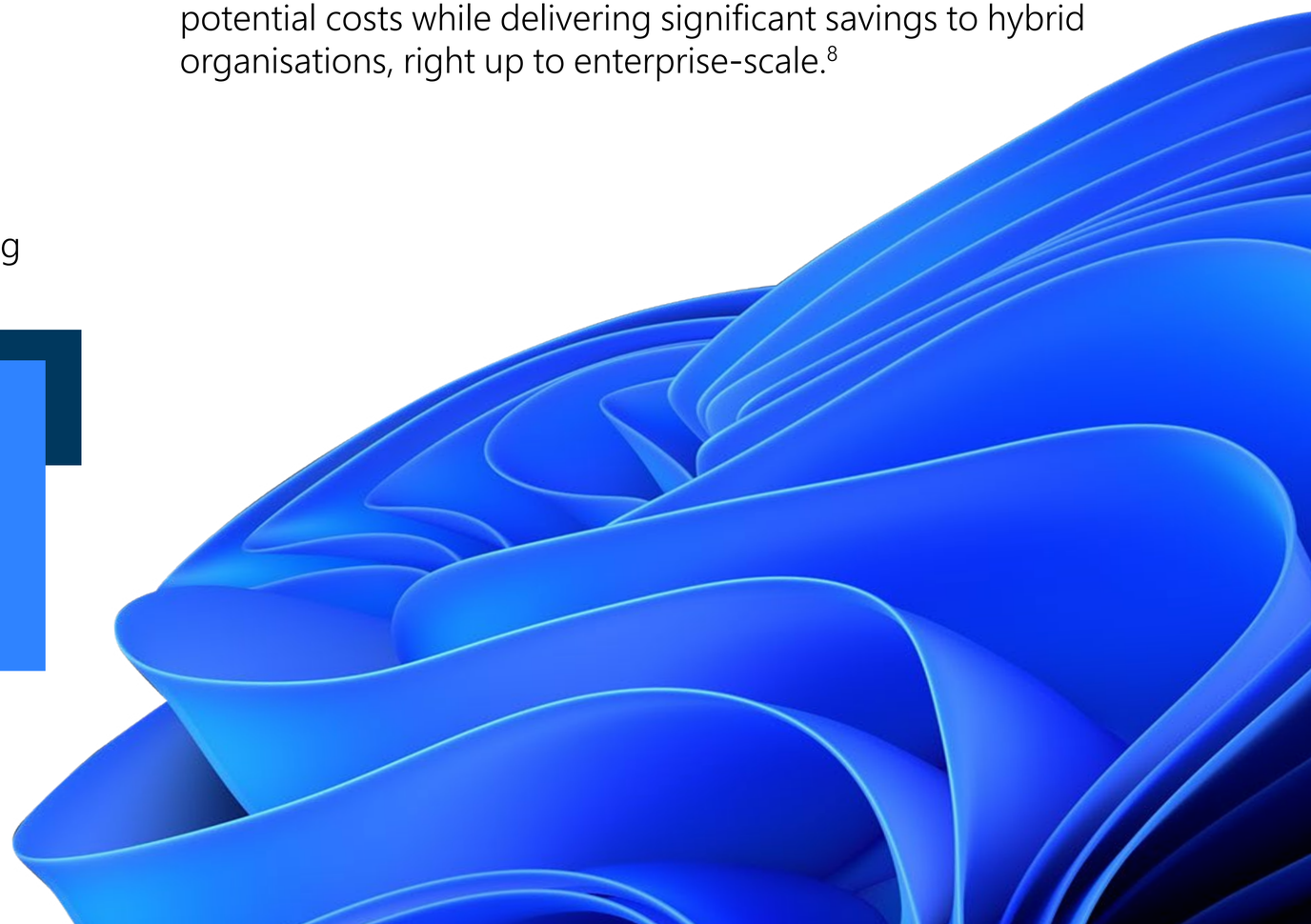
When it comes to working more efficiently, **platform familiarity** is as welcome to IT teams as end-users. A recent Forrester Total Economic Impact™ study commissioned by Microsoft[5] found that the well-known interface and tools of Microsoft Endpoint Manager **reduced the need for IT team training spend**, enabling faster and easier implementation:

> **Interviewees were able to deploy and gain proficiency on Endpoint Manager much more quickly than they would another system simply because it is integrated with their Microsoft 365 licenses, and their teams can make use of their skills from operating other Microsoft products.[6]**

The report also notes that Endpoint **Manager saves time for IT by automating system patches and updates** – freeing the IT team to attend to more upstream business technology needs.[7]

Security, manageability and the bottom line

The latest built-in Intel and Microsoft security technologies protect both endpoint hardware and software, enabling hybrid organisations to work more smoothly, safely, continuously and productively. It's clear that improving the end-user experience, securing corporate assets, improving IT productivity and driving trust are business ends in themselves. But they can also be measured in terms of the bottom line – avoiding actual or potential costs while delivering significant savings to hybrid organisations, right up to enterprise-scale.[8]



References

1. 2021 State of the Cloud Report, Flexera, 2021, p 10
2. The Total Economic Impact™ Of Modernizing Endpoints, Forrester, September 2021, p 8
3. The Total Economic Impact™ Of Microsoft Endpoint Manager, Forrester, April 2021, p 2
4. Intel® Control-Flow Enforcement Technology (Intel® CET) and Intel® Total Memory Encryption (Intel® TME) are not included with Intel® Hardware Shield on 11th Gen Intel® Core™ vPro® S-series processors.
5. The Total Economic Impact™ Of Microsoft Endpoint Manager, Forrester, April 2021, p 3
6. Ibid., p 8
7. Ibid., p 3
8. See 'Analysis of Benefits' in The Total Economic Impact™ Of Modernizing Endpoints