Servium

ENHANCING THE MODERN WORKPLACE WITH HARDWARE-ENFORCED SECURITY

Opinion White Paper

Building a modern workplace

The modern workplace is evolving at breakneck speed. Distributed teams, brand new business models and complex security issues are shaping the direction of travel for businesses of all kinds and sizes. For most, it means big steps to transform the way technology functions in order to confront these trends and capture the extraordinary benefits of new digital tools that connect and support employees. Business leaders are turning to technology to help create attractive places to work and maximise on the potential of their people.

An exceptional user experience, no matter where work gets done is fundamental to the modern workplace. Balancing this pursuit and the freedoms it entails with robust security is tough for IT teams. Yet security must be embedded into the workplace experience from day one for transformation to be successful.

In this paper we explain why a different approach to security is needed to support the modern workplace and why organisations should be looking more closely at the devices they choose as part of their transformation. In particular, we reveal the value of hardware-enforced security and why this should feature in any plan for modernising the workplace with Microsoft.

Microsoft's toolkit for teamwork

Naturally, Microsoft technologies are playing a massive role in how the workplace is transforming. Developments in the user experience thanks to the Windows 10 Pro operating system and Office 365, plus the introduction of Microsoft 365, means businesses have a universal toolkit to improve teamwork and productivity. All organisations can now enjoy a complete and intelligent solution that empowers people to be creative together and do so more securely.

The role of security in the modern workplace

Windows 10 Pro comes with rich in-built security features that most organisations will choose to activate, alongside third-party security solutions like anti-virus. However, these measures are only as good as the device hardware hosting them and alone are often not enough to protect from the most advanced attacks.

Threats to information security are everywhere, growing in frequency, variety and scope, resulting in a rising cost of breach. The modern workplace advocates a culture of freedom, mobile working, choice of device and new apps, but this also expands the attack surface. Even with the latest software, the modern workplace remains difficult to secure.

The approach to security therefore needs careful consideration in order to keep pace with the threats you now face. In no way can security get in the way of the experience as obstructed users embark on shadow IT, discovering workarounds that could expose vulnerabilities. Prohibitive security also undermines the workplaces' ability to deliver the value originally sought from modernisation.

Unfortunately, as IT teams wrestle with their security posture, time, resource and money is inadvertently misdirected to perimeter defences, while cyber criminals hunt out the weak links, which is increasingly user behaviour and the devices in their possession.

Windows 7 mandates device refresh

The recent End of Support for Windows 7 further illuminates the importance of security and has been the major reason for recent device upgrade. Many prudent organisations have updated their device estate to Windows 10 Pro ahead of time in order to continue receiving security updates, as well as equipping themselves with technology capable of maximising the user experience the new operating system makes possible.

HP recommends Windows 10 Pro for business

Organisations yet to make the move need to migrate to Windows 10 Pro and upgrade their hardware as a matter of urgency. Even organisations who have chosen to continue with Extended Security Updates for Windows 7 have to upgrade by 2023.

Windows 7 End of Support has driven, and continues to drive, large scale hardware replacement. So, if end user devices are to be updated, why not make the choice to improve security at the same time?

Choosing a PC is a security decision

It's easy to think that device hardware has no part in strengthening security posture, but the reality is very different. Savvy IT professionals are recognising the value of hardware-enforced security in their device estate as a means of enhancing the security measures and management services already present in Windows 10 Pro and other technologies from Microsoft.

Security Matters

$3.86m[1]
The average cost of data breach.

4X[2]
More likely to be breached by zero-day attacks.

1-in-3[3]
Web requests lead to malware.

197 days[4]
Average time to identify a data breach.

91%[5]
Visual hacking attempts successful.

What is hardware-enforced security?

Hardware-enforced security embeds hardened security protection into the heart of a PC, offering the strongest defence possible against the most serious incursions.

It does not work independently of the protection included in Windows 10 Pro, in fact it is critical that hardware and operating system work together to enable robust counter measures against the correct types of attack.

Using integrated hardware components within devices, a secure system architecture is created capable of tackling a variety of tasks including permission checks, authentication and encryption. Regrettably, most PC manufacturers have been slow in recognising the importance of hardware-enforced security beyond the on-chip protections being developed by Intel and AMD respectively.

HP leads the way

HP is heavily innovating in hardware-enforced security and has consequently created some of the world's most secure PCs, simultaneously offering devices perfectly set up to help people capitalise on all the features of Windows 10 Pro and Office 365, and keeping them safe while they're at it.

To combat modern cyber threats, HP's business PCs are designed with layered security that is built-in, hardware-enforced and simple to manage. These measures span four key areas:

How HP Protects

Around The OS

Above The OS

In The OS

Below The OS

1 Protection below the OS

BIOS protection with HP Sure Start

Your BIOS is vulnerable because antivirus can't protect firmware. The BIOS is the first lines of code your PC reads and is responsible for securely booting your operating system. If an attacker can infect it, they can gain unlimited control over your device. Trying to remove malware from a compromised BIOS often means a new motherboard or even a replacement PC.

HP Sure Start offers unique BIOS protection. In the event of an attack, Sure Start notifies the user and restores the BIOS to its last good state. It works by detecting unauthorised changes instead of trying to detect known malware, which means it can protect you against attacks even if they have not been seen before.

2 Protection within the OS

Application and processes protection with HP Sure Run

All sorts of software processes and applications keep your PC secure while you work - everything from antivirus software to cryptographic services. These processes help protect your PC against malware, secure your data, guard against unauthorised access, and more. Malware often targets these key defences in its attacks, attempting to turn them off or disable them in order to gain greater access to your PC.

HP Sure Run keeps these processes and applications running even if malware tries to disable them. In the event of an attack Sure Run notifies the user of any changes and restarts them automatically if they are stopped. This goes beyond Intel Boot Guard which many devices will use to detect a corruption only. In comparison, Sure Run will recover the BIOS and self-heal, not only guarding key Windows processes like anti-virus and firewall protections in Windows Security Center – but also other software security that may be considered important.

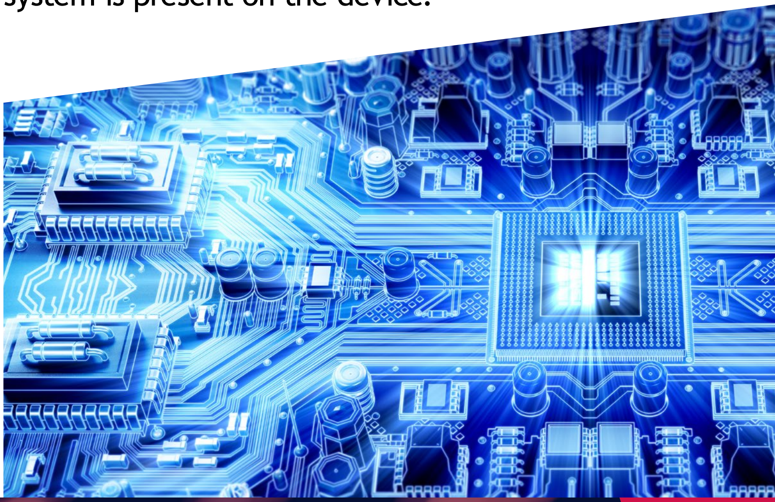
Meet the HP Endpoint Security Controller (ESC)

A separate piece of silicon that sits inside HP PCs, the ESC performs a host of security-based tasks. It features a general-purpose processor core, HP's custom hardware IP blocks, and embedded software. The result is this unique bit of hardware enabling very resilient devices.

- Physically isolated and cryptographically secured
- Drives hardware enforced resilience for HP Sure Start Gen, HP Sure Run, and HP Sure Recover
- Creates a hardware root of trust

Quickly reimage devices with HP Sure Recover

Whether you're recovering from an attack or need to reimage for other reasons, the process can be time-consuming and disruptive to the user, impacting their ability to work. HP Sure Recover enables an employee to reimage their own device to the latest operating system over a wired connection, eliminating the need to call on IT. Where reimaging needs to occur more frequently, fleet-wide actions can be scheduled by IT. And because Sure Recover is enabled by the HP Endpoint Security Controller and executed through the BIOS, PCs can be reimaged even from a blank hard drive or if no operating system is present on the device.



Browser and Microsoft Office file protection with HP Sure Click

Insecure web browser and innocent files are a growing means of intrusion. HP Sure Click isolates applications in their own virtual containers - trapping any malware and deleting it as soon as the application is closed. Hackers may also use phishing emails to link to malicious sites or infect "watering holes", including online Office documents that a victim may routinely visit. Sure Click is enabled on Internet Explorer and Chrome, ensuring there is no need to learn a new browser, and because untrusted websites are opened in their own isolated micro-VM, whitelisting is eliminated.

Zero-day malware protection with HP Sure Sense

Legacy protection will often not catch zero-day attacks. What's more, hackers are using AI to increase sophistication and velocity of release. Because of this, HP Sure Sense harnesses deep learning for in-built protection against never seen attacks. The protection is trained on real data and is ready to identify known and unknown threats in milliseconds, with next to no ongoing management overhead or impact on device performance. When Sure Sense identifies a threat it is instantly quarantined.

3 Protection above the OS

Visual hacking protection with HP Sure View

Visual hacking occurs when sensitive information is displayed in public places, where competitors, identity thieves, and other unscrupulous individuals can see, capture, and exploit it. Passwords, account numbers, financial data, and other confidential information might be safely stored, but no amount of security software can prevent someone from simply reading over your shoulder. The simplicity of visual hacking and absence of protection against it means success rates are very high.

HP Sure View protects against visual hacking using an integrated privacy screen. Enabled at the touch of a button it keeps private information out of public view by obscuring the display to anyone but the user directly in front of the screen – nearby users simply see a white haze. Importantly, this feature is enabled on the thinnest and lightest notebooks so does not impact on portability. The same technology is also now available in HP monitors for use in the office.

4 Protection around the OS

As more organisations choose to use Office 365 and Microsoft 365, identity management in the cloud using Azure Active Directory makes more sense. Here the policies surrounding sign-in and access can be modified for apps and data wherever they reside. Accordingly, it is enabling wider security measures to be introduced to the IT environment covering mobile productivity and information protection.

Because of the hardware protections built into HP PCs, IT teams can unite their ability to create powerful policies in Azure Active Directory with the hardware-enforced security on the device. For example, HP Sure View could be activated every time a particular document is opened outside the office or indeed HP Sure Click could be enabled for all off network browsing.

Similarly, thanks to HP Sure Run, HP devices also offer hardware enforcement for your chosen anti-virus by protecting Windows Security Center from malware that tries to shut it down.

The cost of hardware-based security from HP

Interestingly, features we have discussed in this document are included on all the latest HP EliteBook and EliteDesk devices, while many of them are available in ProBook and ProDesk devices also. Amazingly, except for SureView (which is an optional extra), all of the security features are included free of charge.

References

[1] IBM Cost of a Data Breach Study, 2018.
[2] Barkly and Ponemon Institute 2018 State of Endpoint Security Risk Report, 2018.
[3] Symantec, "Internet Security Threat Report (ISTR) Volume 23", March 2018.
[4] IBM Cost of a Data Breach Study, 2018.
[5] Ponemon Institute, "Global Visual Hacking Experiment," 2016, sponsored by 3M.

The benefits

Modernise with confidence

Embrace mobility, new apps and SaaS, confident your devices are a fortress.

Intelligent built-in security

Connect seamlessly with Microsoft protections to unlock new capabilities and achieve holistic, intelligent security.

Foster secure working habits

Encourage better practices by providing the best apps and devices with built-in security.

Get secured fast

Secure your enterprise fast with an operating system, apps and devices that work together and are familiar to IT teams.

£

Good financial sense

HP-only protections add important value over competitive business devices for a comparable cost.

Servium

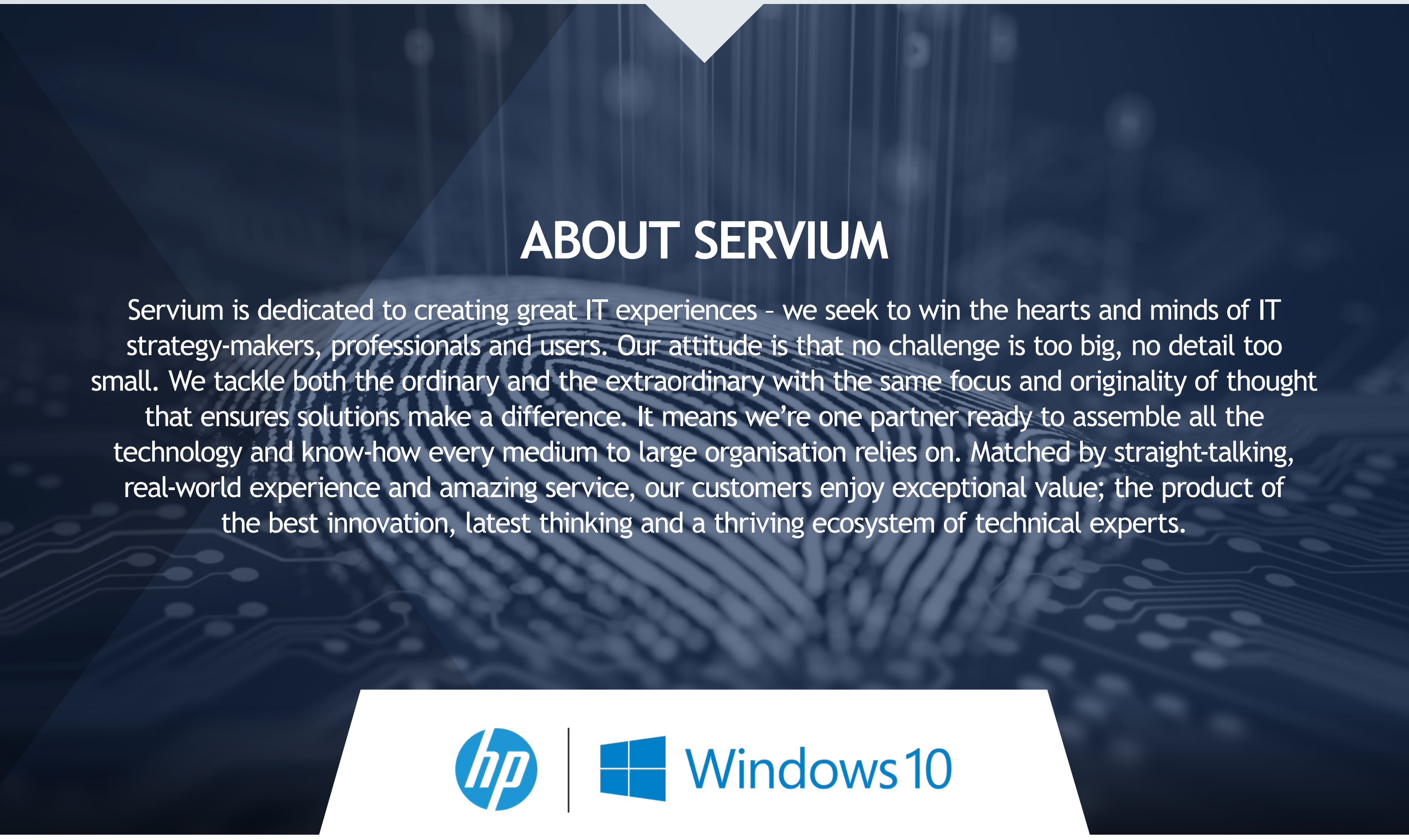
Building a modern workplace

WHAT NOW?

If you're looking to modernise your workplace or are even underway with a project and want to explore HP devices, then get in touch. Servium can arrange evaluation units and proof of concept labs to demonstrate the value of HP technology as part of your transformation programme.

THE NEXT STEP

To arrange a trial, see a demo or talk with an expert, contact your Servium Account Manager, email us at hello@servium.com or call on +44 (0)303 334 3000.



ABOUT SERVIUM

Servium is dedicated to creating great IT experiences - we seek to win the hearts and minds of IT strategy-makers, professionals and users. Our attitude is that no challenge is too big, no detail too small. We tackle both the ordinary and the extraordinary with the same focus and originality of thought that ensures solutions make a difference. It means we're one partner ready to assemble all the technology and know-how every medium to large organisation relies on. Matched by straight-talking, real-world experience and amazing service, our customers enjoy exceptional value; the product of the best innovation, latest thinking and a thriving ecosystem of technical experts.