Servium

PC SECURITY CHALLENGES YOU NEED TO BE READY FOR

HP Security Opinion White Paper

+44 (0)303 334 3000 | www.servium.com | hello@servium.com

THE SECURITY QUANDARY

It's no secret that cybercrime is on the rise. According to the National Cyber Security Centre (NCSC) and National Crime Agency (NCA), 2018 was the year of more cyberattacks than ever before and the most sophisticated threats we've seen to date. Major incidents in the UK over 2016 and 2017 included ransomware, such as the infamous WannaCry attack on the NHS, DDoS attacks, supply chain compromises, and fake news among others. The list is only growing as time goes on. The government's own Cyber Security Breaches Survey revealed that almost half of all UK businesses experienced data breaches or cyberattacks between April 2016 and April 2017, and that's only the tip of the iceberg.

The worrying thing is that the clear majority of these data breaches and cyberattacks are almost always reported by businesses that consider security a low priority, or don't value their online services as a core part of their business. Many of these attacks are a result of poorly executed security policies, or else an entire lack of even the most basic protections. What's concerning about this is the Cyber Security Breaches Survey also reported that the average UK business identified nearly 1,000 breaches over a 12-month period. With figures like that, it's indisputable that cyber security needs to be taken a lot more seriously.

Your people and their PCs

Amongst these security breaches, the PC and how it is used by your people is without question a significant vulnerability for almost any business. Yet many businesses still don't prioritise PC protection, woefully underestimating the measures required or even failing to understand the threats at large that are ready to exploit the device, the user, and the data. This is mostly due to the misconception that a secure core infrastructure must mean every one of your endpoints is covered and indeed that security software like antivirus will offer the necessary defence. This simply isn't the case. Securing your PCs is just as important. Not only will your users be faced with a barrage of different cyber threats on a regular basis, but often unwittingly compromise their devices due to human error, so your PCs need to be prepared for any eventuality. But how do you achieve this? How can you empower your users with smart, streamlined cyber security that doesn't come at the expense of their productivity?

Time to get serious

The HP Premium Family of business laptops are among the world's most secure and manageable PCs. They come with all-important security measures enforced by the hardware which makes for stronger protection and secures the foundation of the PC. They're ready to stand toe-to-toe with every new threat you come up against.

1 BIOS-level attacks

The basic input/output system (BIOS) within your PCs is a frequent target of cyberattacks, the rate of which is only growing. This is because the BIOS is responsible for managing the data flow between a PC's operating system (OS) and any attached devices, as well as booting the OS securely after the PC is turned on. The BIOS is an attractive prospect to hackers as any attacks carried out on the firmware is practically undetectable and cannot be monitored by standard antivirus software. Once in, malware is very difficult to remove, taking up all of your IT team's valuable time and resources to eliminate.

HP Sure Start is the industry's first self-healing BIOS. Hardware-enforced for stronger protection, it quickly detects any potential malware threats, alerts the user and your IT team, and automatically restores the BIOS to its most recent good version, or "gold master", in less than a minute. It will actively identify and report any unauthorised changes to the BIOS, both when you start up your PC and while the OS is running as you work, as well as offering enhanced protection for any critical processes that rely on the PC's runtime memory (SMM). It's so intuitive, it can even defend against threats to the BIOS that it's never experienced before.

2 Public privacy

Users are sometimes unaware of or forget how valuable your business' data is. Consequently, they may become careless when using their devices remotely, which may lead to them unknowingly exposing sensitive information in public places that could be spotted and targeted by prying hackers. While an unsophisticated means of capturing data, public snooping is increasingly common. In many cases, all it can take is a quick glance over an employee's shoulder, and a patient cybercriminal can gain access to all sorts of confidential company data. It's a largely underestimated security risk yet could cause serious damage to a business' reputation if data leaks in this way.

HP Sure View offers data privacy at the click of a button. Thanks to the world's only integrated PC privacy screen, your PC can instantly be protected from prying eyes when you're out and about. By reducing up to 95% of visible light and preventing sideangle viewing, the screen remains completely visible to you alone while ensuring that any opportunity for visual hacking is deterred. This sees that you're able to continue working wherever you are, safe in the knowledge that critical data is for your eyes only.

3 Malware evolution

Malware is sneaky and it's on the rise. Threats are evolving all the time to achieve a better chance of successfully taking over a PC. It will target as many of the software processes and applications keeping your PC secure, find a way to disable them, and then gain sufficient access to worm its way into your systems. It uses your own defences against you, shutting them down in order to make launching an attack that much easier.

HP Sure Run does exactly what it says on the tin. It ensures that all of the critical processes defending your PC keep on running, even in the event of a malware attack. Guarding both these processes and any vital HP features from malicious threats, Sure Run monitors your security defences, alerts you to any changes through the Windows Action Centre, and will restart them automatically if they have been stopped. HP's Endpoint Security Controller sees that Sure Run is hardware-enforced, ensuring it always remains active and its security is bolstered.

4 Phishing attacks

Phishing has grabbed a lot of headlines because of its roots in social engineering. The purpose is to deceive and confuse and cybercriminals will play on human emotions to a elicit a response, whether that's greed, vanity, or simply the fear of missing out. While this can take many different forms, the most popular seems to be via fraudulent emails. As a result, phishing emails entice the user to click on a link that leads them through to a malicious website. From here, hackers can easily take control of a PC by installing ransomware onto the device and holding it hostage, demanding money in exchange for control of the data. A big challenge for business IT security is that it's getting harder to tell if a site is safe or unsafe, so phishing doesn't even need to occur through emails anymore. If one of your users were to click through an advertisement on a news website or else engage with a false social media account for example, they could be opening you up to a potential data breach.

HP Sure Click keeps your PC protected from infected websites, malicious ransomware, and other web-based threats by isolating your web browser tabs and locking any attacks inside them. This ensures that the threat is unable to reach any further browser tabs to infect them and has no way of gaining access to infect your wider systems either, dramatically reducing the risk to security. Sure Click is activated every time you open a new browser tab, so whenever you visit a website – safe or unsafe – it's got your back.

5 CEO fraud and password vulnerability

One of the most common cyberattacks affecting users today is business email compromise (BEC) fraud (commonly referred to as CEO fraud), which tricks employees into thinking that they have been sent an email by a person of authority who is requesting sensitive information like bank details or customer data. Your users are only human, so many will fall for this type of attack and open your network up to malicious malware or viruses. Likewise, users will typically create passwords or logins to critical applications that they can easily remember, but these are very rarely secure.

The consequences of a weak password on a stolen computer could result in anything from identity fraud to exploitation of confidential client data. According to Gartner, one laptop is stolen every 53 seconds. Even today, theft of unencrypted, unprotected PCs continues to be one of the largest causes of data breaches worldwide.

The time of traditional logins is over. The password is in the past, and for good reason. Cybercriminals are now more sophisticated than ever and as such have multiple ways of correctly deciphering your credentials, however complicated and random they may be.

Using multi-factor authentication, the login process is streamlined and the potential for a data breach reduced. Thanks to the HP Client Security Manager with Intel Authenticate support, users are able to introduce up to three different authentication factors, from built-in biometric measures such as a fingerprint scanner and facial recognition to smartcard or Bluetooth readers. This makes it incredibly difficult for hackers to find their way into your systems and ensures login credentials are much harder to obtain, deterring BEC fraud. HP Multi-Factor Authenticate makes the login process one million times more secure than a traditional non-hardened password. All of your authentication factors, decisions, and IT security policies are also encrypted and hardware-enforced by Intel's isolated Management Engine.

6 Webcam hacking

All business PCs today, near enough, come with a built-in webcam. This is because, thanks to applications like Skype for Business and Zoom, video is fast becoming a staple of collaboration. Video conferencing is gradually overtaking traditional phone systems as the tool of choice, if only due to the fact that it's a more practical, cost-effective collaborative solution. However, this functionality shouldn't come at the price of privacy. Sadly, webcams are not exempt from hacking. If hacked, cybercriminals could potentially capture evidence of confidential data being carried around an office, or even spy on users who are working in the privacy of their own homes.

The HP Privacy Camera enables users to block their camera lens as required. Using a simple built-in shutter, the camera can be covered and uncovered at will, allowing users to maintain their privacy whenever they like. That way, you can rest assured that you're able to work in complete peace.

'Sure' up your PC security

The HP Premium Family of business laptops is designed specifically with security in mind. Built-in, advanced features defend against sophisticated internal and external threats, giving you peace of mind that your corporate PCs are constantly protected, wherever you are. HP Premium business laptops come equipped with:

- HP Sure Start
- HP Sure View
- HP Sure Run
- HP Sure Click
- HP Sure Recover
- Multi-Factor Authenticate
- HP Manageability Integration Kit
- HP Privacy Camera

7 Timely device patching

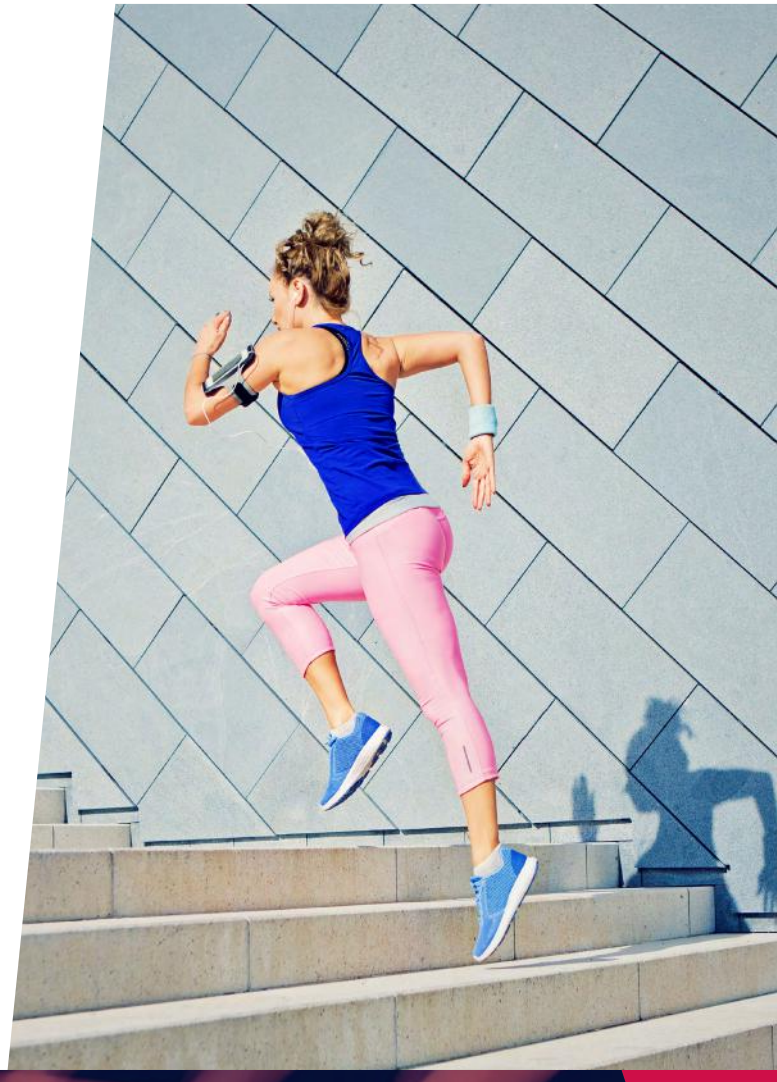
IT security administration is exceedingly time-consuming. But with the overwhelming pressure ofcyber threats constantly knocking at the door, it's important to know all of your PCs are always kept up-to-date, properly patched, and all necessary security settings are correctly configured at all times. Unfortunately, many organisations inadvertently leave the responsibility to complete updates to unassuming users who may ignore or neglect the task. All it can take is one risky PC to bring down the whole fleet, so everything needs to be done right no matter how gruelling the task.

Every one of HP's advanced security features, with the exception of the HP Privacy Camera, is underpinned by the HP Manageability Integration Kit (HP MIK). This certified toolkit for Microsoft's System Center Configuration Manager (SCCM) enables remote management to be extended to HP technology. Through a single intuitive, user-friendly interface, everything from image creation to security policies can be applied and managed remotely for your entire fleet. Any non-compliant security configurations are also remediated automatically without the need for your IT team's involvement. The HP MIK vastly speeds up key security administration processes, streamlines remote PC configuration, and even provides its own added layer of protection.

8 The time to recover

Recovering a compromised device can take a considerable amount of time and remedy frequently involves machine reimaging. Your user may end up without a device for an extended period of time, which harms productivity, and precious technical resource gets tied up performing a thorough restore to ensure malware is completely removed.

HP Sure Recover enables users to quickly and easily reimage their devices to the latest OS image themselves using the HP Endpoint Security Controller. This can be done through a single wired network connection, eradicating the need for your IT team to get involved entirely. What's more, this doesn't have to be limited to a single device, but can be applied to the whole fleet, so reimaging is scheduled on a regular basis. All of this is even achievable from a blank hard drive. Sure Recover makes certain the integrity of the image is authentic, too, with a digitally signed public/private key.



CONCLUSION

Cybercriminals naturally look for the weakest links in your network. As your people obtain greater control over their devices and use them in ever more creative ways, the potential for security vulnerability at the PC increases. It's therefore imperative to be prepared for the worst by investing in the best security technology available, and thanks to the multi-layered defences of HP's Premium business laptops, the world's most secure PCs can be in the hands of your users, helping to keep them safe and protect your data without interfering in work they want to do.

THE NEXT STEP

Servium is one of HP's leading partners in the UK. Our knowledge of the HP portfolio and the security features explored throughout this opinion paper means we are perfectly placed to advise you and help you arrive at the ideal PC solution for your business.

To learn more or discuss any of the aforementioned HP products or security features in more detail, simply speak to your 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.

Servium | hp