BIZCOMMUNITY

How to achieve the most from your cyber security defences

Issued by HP

17 Jan 2022

The workplace has evolved and so have the threats. Hybrid ways of working mean more endpoints, more remote connections, and more potential access from malicious actors. South Africans have lost around R2.2bn a year because of cybercrime, according to an October 2021 Interpol report. In fact, the report states that between January 2020 and February 2021, the country experienced a total of 230 million threat detections. The first quarter of 2021 saw an uptick in extortionware and ransomware attacks including the Crysis, Nefilim, Ryuk, Clop, and Conti varieties.

The question that IT security teams, and individuals, need to be asking now is what is their best defence against the inevitable? Education, and software applications aimed at detecting, preventing, and recovering from attacks are absolutely important. It’s becoming very clear however, that guarding your core defences inside a hardware-based security bunker - that malware can’t touch - is the best defence.

The wise build on firm foundations

When deciding on the ideal hardware for your teams, ensure you choose a laptop or PC with stable security that can safeguard the root of your protections. You want to make sure that malware can’t touch this central core. That means choosing hardware with an endpoint security controller that is physically isolated, cryptographically protected, and has hardware-enforced, self-healing security as the foundation of your security architecture.

Don’t find yourself out-matched

Understand that you are not dealing with a playground bully, you’re dealing with highly-sophisticated, and organised crime syndicates. Traditional virus protection is in a constant battle to keep up with the more than 350,000 new malware variations that are created by these threat actors every day. You need to be fighting AI with AI. Choose hardware that incorporates deep-learning neural networks to defeat malware that has never been seen before. Make sure this is backed up with robust defences such as a micro-VM container that can isolate any malware that might slip through, before destroying it.

The power to heal

You know how people say it’s not about the number of times you fall, it’s how you get back up that counts? It’s true. It’s important to be confident in your detection defences, but the reality is that even the strongest and most complete solutions may experience a breach. Destructive firmware attacks can devastate a PC, fundamentally corrupting it by attacking it at the BIOS level. An OS-level attack can cost hours or days of worker downtime, and IT attention, before systems are restored and ready to get back to business. If an attack avoids detection, you need to make sure your PCs can fix themselves, quickly recovering their own OS — from anywhere — with or without a network connection.

“Are you suggesting I’m not who I say I am?”

Some of you Gen Xers might recognise this sub-heading as a line from a John Hughes classic film ‘Ferris Bueller’s Day Off’. In the movie, Ferris Bueller, played by Matthew Broderick, jumps through a few clever hoops to essentially steals the identity of Abe Froman, to secure a table at an expensive restaurant. While he used other actors to help him convince the maître d' that he was Abe, not once did he show any form of identification. Spear-phishing attacks are a lot like that, tricking users for login information, and the trouble is, a lot of the time, PCs don’t require a strong enough form of proof of identity from those attempting to access them.

Hands up if you haven’t had to hit a “forgot password” button in the past two weeks. These days we have so many passwords to remember that a lot of the time people just don’t, or they have bad hygiene practices using weak, shared, or re-used passwords in efforts to make logging in that much easier for themselves. In doing so, they’re making it easier for anyone else to get in.

Business PCs — and the networks they connect to — are too often compromised when they rely on traditional password protection. It is better to choose PCs that require multi-factor authentication such as password, fingerprint, and facial recognition. These policies should be locked in at the hardware level to ensure no short cuts are taken when it comes to your employee proving that they are in fact who they say they are.

When is a coffee shop not just a coffee shop?

Managing remote devices with a scattered workforce is a major challenge, so having a platform that allows your IT managers to control your PC endpoints and administer security settings from anywhere is important.

More and more workers are operating outside of their home offices, particularly when load-shedding hits, and they go in search of power connections. The trouble with coffee shops (anywhere that's not your secure office environment really) is that unwanted eyes can watch your workers — and what they're working on — from either side of the screen, compromising sensitive and confidential data. Choose hardware that can end visual-hackers' line of site with built-in privacy tools such as physical shutters on cameras, one-touch privacy shields that make the screen unreadable to those nearby and identify confirmation that can unlock that PC hands-free.

Security for people working on the go

The threat environment is constantly evolving which means we all need to as well. It entirely possible to create a robust security environment by combining education, security applications and services, and secure hardware. The key to successful prevention is ensuring that all the necessary building blocks are there to construct a stable security foundation.

The available choices can be overwhelming so it's wise to partner with a solutions provider that has your best interests at heart.

The Solution

The HP Elite Dragonfly G2 (358VEA), featuring an Intel® Core™ i7 processor, layers on the aforementioned security features in and above the operating system. Featuring multi-factor authentication, HP Sure View technology to protect sensitive information from prying eyes and HP Sure Run to guard from malicious malware attacks, we guarantee this is the most secure business PC available today.

HP understands that the ways of working are forever changed. We are constantly innovating to ensure your enterprise can enjoy peace of mind with secure-by-design PCs with hardware-enforced endpoint security software and endpoint security services perfectly suited to people working on the go.

For more information about our cybersecurity features, visit:
https://www.hp.com/za-en/security/pc-security.html

About HP Inc.

HP Inc. is a technology company that believes one thoughtful idea has the power to change the world. Its product and service portfolio of personal systems, printers, and 3D printing solutions helps bring these ideas to life. Visit http://www.hp.com.