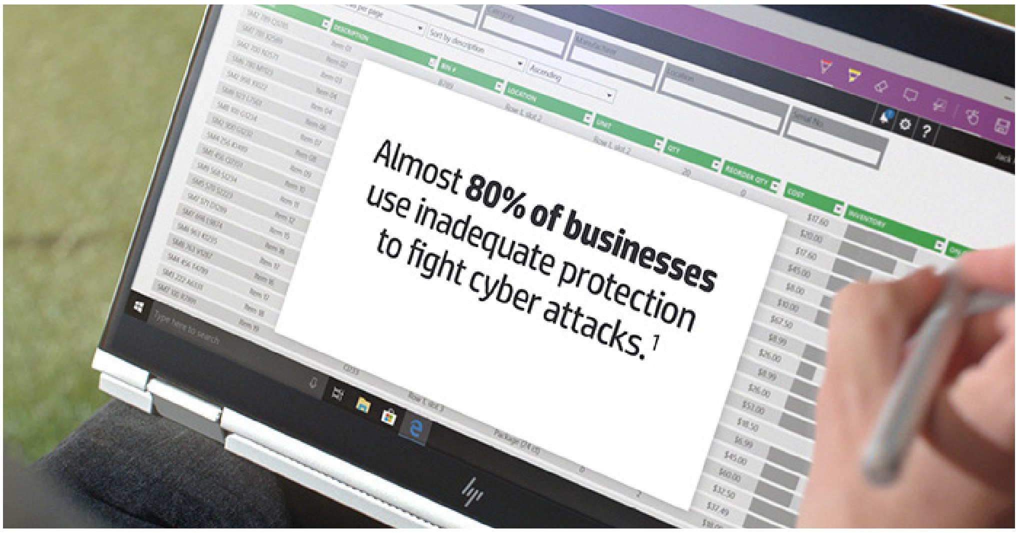
How automatic defences can save your business devices

Learn more


Almost 80% of businesses use inadequate protection to fight cyber attacks.1

How do you fight a threat that hides under your defences? You automate.

$600 billion a year. That was the cost of cybercrime across the world in 2017[2]. That number gets bigger and bigger as hackers become more sophisticated and capable. Recently it was reported that 20% of SMBs had to cease business operations immediately, and 12% lost revenue after a cyberattack[3]. One of the latest sneak attacks to become the bane of IT managers are those that target the firmware during a PCs booting process: BIOS attacks.

Millions of machines have basic BIOS vulnerabilities, meaning they could be hacked into by someone with even moderate hacking skills. Researchers Xeno Kovah and Corey Kallenberg presented a new type of attack at a conference a few years ago, revealing that within a few hours they could remotely hack and infect the BIOS of multiple systems[4]. Because most BIOS share the same code, once the first had been cracked, it was only a matter of time before the same skills were able to topple the defences of so many more machines.

This type of attack is so dangerous because it targets somewhere that hasn't been protected. There's a hidden space between the operating system and the hardware, which used to be ignored. And while your network might appear watertight and your device is protected behind the best anti-virus security software in the world, there's still a brief moment during booting up and your defences firing up that a hostile BIOS attack can wreak havoc.

As most cyber-security software sits on/at the operating system level, malware injected into the BIOS (before bootup and passed into the System Management Mode) will be undetectable to endpoint cyber-security software. From there, the hackers will get total control over your system. They will be able to steal your data, render it unreadable, or spread new malware across your company's network. Worst of all, it can be almost impossible to discover that the breach and infection have occurred.

The best way to protect your company devices is to use multi-layered security. The capabilities of your IT team shouldn't be wrapped up in constant scanning and manual fixes. HP provides an automatic response – as part of a range of security solutions – HP Sure Start[5].

"This is part of a joint effort with HP Labs to help businesses better manage risk and protect user and IT productivity against malicious attacks, a failed update, or any other accidental or unknown cause,"

- Vali Ali, Chief Technologist for Security and Privacy in the HP PC Business Unit.

How automatic defences can save your business devices

HP Sure Start is a self-healing BIOS level protection. We call this approach cyber-resilience. The system works by creating a 'gold master' of the BIOS, which is directly encrypted on the device. So, if someone tries to hack the BIOS, it automatically reboots itself and then loads the 'gold master', wipes the infected file and lets you and your team know about the attack. Essentially, the machine heals itself.

That means uninterrupted productivity. It means lower costs. It means more compliant devices. Above all, it's an easier way of working.

If you're wondering what the easiest way to get cutting-edge devices with HP Sure Start in front of your users is, then consider HP Device as a Service (DaaS)[6]. It's a modern-day PC service model that simplifies how commercial organisations equip their employees with the right hardware and accessories, manage multi-OS device fleets, and get additional lifecycle services. HP DaaS offers simple, yet flexible plans, at one price per device to keep everything running smoothly and efficiently.

Endpoints and access points need to be monitored at every level. It's time to stop avoiding the hidden parts of our devices. Every person, business and organisation around the world can become safer and more resilient with HP's portfolio of product offerings, including the HP EliteBook x360, with optional 8th Generation Intel® Core™ i7 processors. As part of the HP Elite family, this device offers security technology thanks to its built-in security features, like HP Sure Start.

Discover the benefits of HP security solutions to your business.

Sources:

1. Statista Survey ID 622857, "Small and medium sized enterprises in the U.S by Statista, October 2016
2. https://www.mcafee.com/enterprise/en-gb/solutions/lp/economics-cybercrime.html
3. Osterman Research, sponsored by Malwarebytes "Second Annual State of Ransomware Report: US Survey Results" July 2017
4. https://www.wired.com/2015/03/researchers-uncover-way-hack-bios-undermine-secure-operating-systems/
5. Various generations of HP Sure Start are available on select configurations of HP Elite and HP Pro systems.
6. HP DaaS plans and/or included components may vary by region or by Authorized HP DaaS Service Partner. Please contact your local HP Representative or Authorized DaaS Partner for specific details in your location. HP services are governed by the applicable HP terms and conditions of service provided or indicated to Customer at the time of purchase. Customer may have additional statutory rights according to applicable local laws, and such rights are not in any way affected by the HP terms and conditions of service or the HP Limited Warranty provided with your HP Product.

4AA7-3218EEE, April 2019