MATCHING FLEXIBILITY WITH SECURITY

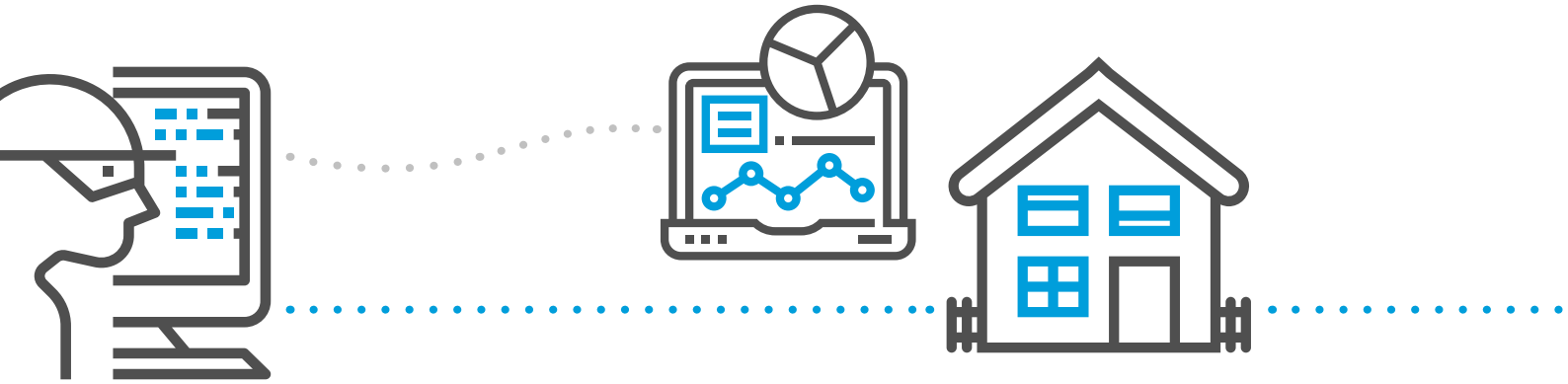
Matching flexibility with security

Flexible and remote working has never been more popular. More than two thirds of people around the world already work from home once a week[i]. And this trend is set to continue. By 2022, 1.87 billion people will be mobile employees – 42.5% of the total global workforce[ii].

It's easy to see why companies are embracing the concept. Remote working allows employees to work in accordance with their lifestyle – not the other way around. Flexible working can help companies cut costs by spending less on in-house facilities. And it can boost productivity.

But there's another consideration for companies that promote remote working, because they unwittingly expose themselves to greater risks. Remote workers tend to be more negligent about security, more willing to open emails and attachments from unknown sources, and more likely to access work files with unprotected personal devices[iii].

From 2016 to 2018, almost a third of organisations were victims of cybercrime[iv]



[i]CNBC, May 2018, https://www.cnbc.com/2018/05/30/70-percent-of-people-globally-work-remotely-at-least-once-a-week-iwg-study.html

[ii]Strategy Analytics, Oct 2016, https://www.humanresourcesonline.net/42-5-of-global-workforce-set-to-be-mobile-by-2022/

[iii]2 Ponemon Institute, 2018 State of Endpoint Security Risk sponsored by Barkly, October 2018.

[iv]PwC, Pulling fraud out the shadows: Global economic crime and fraud survey, 2018.

Endpoint attacks are escalating

To make matters worse, cybercriminals are becoming more sophisticated. Hackers continue to use tried and tested methods – like phishing and Denial of Service (DOS) attacks – to steal information and overwhelm networks. But they are increasingly targeting connected devices, or endpoints, too.

In 2018, Ponemon surveyed 660 IT and IT security professionals from global companies. Almost two thirds reported a major breach that had started at an endpoint, up 17 per cent on the previous year.

60% of personal devices used for work purposes are not monitored for security[v]

It's time to take endpoint security seriously

Five ways your endpoints are at greater risk:

52%

Decentralised workplaces:

52% of employees work remotely at least once a week.

50%

Missed threats:

50% of breaches in small and medium sized businesses are down to human error.

Antivirus is necessary but not sufficient:

Antivirus software misses more than half of endpoint attacks.

Breaches can be invisible:

More than two-thirds (68%) of breaches aren't discovered until months after an attack.

Lack of expertise:

With a global shortfall of three million IT professionals, organisations are under even greater pressure to stay secure.

[v]4 HR Dive, Employees use personal devices for work without much oversight, May 2018

Bulletproof security

To address these issues, HP's Elite PCs are engineered to protect, detect, and recover from cyberattacks from the hardware up, with features such as:

HP Privacy Camera
A physical shutter to protect you from malicious surveillance.

HP Sure View Gen3
A privacy screen to protect against visual hacking. At the touch of a button your screen becomes unreadable to those around you.

HP Sure Sense
An Artificial Intelligence-based malware defence that instantly recognises malware and new attacks.

HP Sure Click
Protects your PC from browser-based attacks hidden in websites and read-only Microsoft Office and PDF attachments.

HP Sure Run
Keeps critical processes running, even if malware tries to shut them down.

HP Sure Recover
Fast, secure, and automated recovery of your OS.

HP Sure Start
Self-healing BIOS that, in the event of a malware attack, automatically detects the change, notifies the user and IT, and restores the most recent version.

In addition to producing products with in-built security, HP works hard to talk to experts across academia, government, and industry. HP's Security Advisory Board brings a trio of security experts together to work inside HP with our own security technologists and strategists.

This advisory board helps HP be as sharp as possible in anticipating the future: understanding the threats today and addressing the problems of tomorrow.

A second unit – the HP Security Lab – ensures that HP devices remain trustworthy and resilient in the face of ever-changing threats from malware and other cyber attacks.

Cybercrime will continue to be a threat long into the future. But with HP, you can work anywhere, anytime, safe in the knowledge that your data and devices are secure.

This article originally appeared on Innovating in Endpoint Security by HP.
Visit https://ij.ext.hp.com/hp-innovation-journal-special-edition-security/0466391001527711595
to read the article in full.