5 REASONS YOUR ENDPOINT SECURITY COULD BE AT RISK

Cybersecurity threats are always-on. Your endpoint security has to be, too.

IT MUST ADAPT TO A DISRUPTED WORKFORCE.

Keeping your endpoints protected has always been a challenge, but it got even tougher when users shifted to working from everywhere—and not just users, but IT, too. With 90% of IT cybersecurity professionals now working remotely,[1] more than a third of them say they feel the hybrid-work arrangement leaves their organizations more compromised and exposed to security threats.[2]

ENDPOINTS ARE MORE TARGETED THAN EVER BEFORE.

With users and devices scattered far and wide, hackers see new opportunities: 68% of respondents say the frequency of attacks has increased[2] and that they have experienced one or more successful endpoint attacks in the past two years.[3] That means IT security must be more vigilant than ever. With more than half of organizations reporting a lack of in-house endpoint protection expertise and resources,[3] 57% of cybersecurity professionals anticipate spending more on endpoint security.[2]

IN THE EVOLVING WORLD OF CYBERSECURITY, HERE ARE FIVE WAYS YOUR ENDPOINTS ARE AT RISK...

ONE—

THE WORKPLACE IS NOW DECENTRALIZED—AND SO ARE THE THREATS.

Employees who used to be confined to the boundaries of an office are now spread across locations and time zones: At least half of employees are currently working 100% from home.[4] That hybrid-work environment increases the attack surface,[4] with 23% of surveyed IT pros saying their organizations have experienced an increase in cybersecurity incidents since transitioning to remote work; some have tracked as many as double the number of incidents.[1]

AT LEAST

50 %

OF EMPLOYEES ARE WORKING 100% FROM HOME[4]

TWO—

CYBERATTACKERS VIEW UNWITTING EMPLOYEES AS AN UNLOCKED DOOR.

Although there are many avenues for cyberattacks, most of them intersect with this one element: a low level of cybersecurity awareness among employees.[5] More than 99% of email messages distributing malware require human intervention—such as following links, opening documents, accepting security warnings, and other behaviors—for them to be effective.[6] And after the cyberpathogen is in, it's in, spreading from one user system to another.

60 %

OF ORGANIZATIONS HAVE HAD ONE COMPROMISED EMPLOYEE INFECT OTHER USERS[7]

THREE—

ANTIVIRUS PROGRAMS ARE NO LONGER ENOUGH.

There are 102 million new malware threats each month. That's 360,000 per day, or 4.2 each second.[8] And what's worse is that not only are 80% of these attacks zero-day threats, but 60% of attacks are missed by antivirus programs.[3] That's why a total of 85% of organizations say they prefer advanced IT security products with features like: AI, machine learning, behavior monitoring, and proactive isolation.[5]

ABOUT

33 %

OF ORGANIZATIONS PLAN TO INVEST MORE IN ADVANCED ANTIVIRUS/ANTI-MALWARE[5]

FOUR—

YOU CAN'T FIGHT A BREACH YOU DON'T SEE.

Without oversight of device security, it takes a while to know that you even have a problem. Traditionally, organizations take an average of 315 days to identify and contain a breach caused by a malicious attack[9]—and only 97 of those days are spent actually patching the weak spot.[3]

But with the shift to remote work, organizations say they expect that working from home could increase the time it takes to identify and contain a data breach, as well as increase the cost of the breach by 70%.[9]

AVERAGE COST OF A DATA BREACH:[9]

- $2.01M FOR RETAIL
- $3.9M FOR EDUCATION
- $5.85M FOR FINANCIAL SERVICES
- $7.13M FOR HEALTHCARE

FIVE—

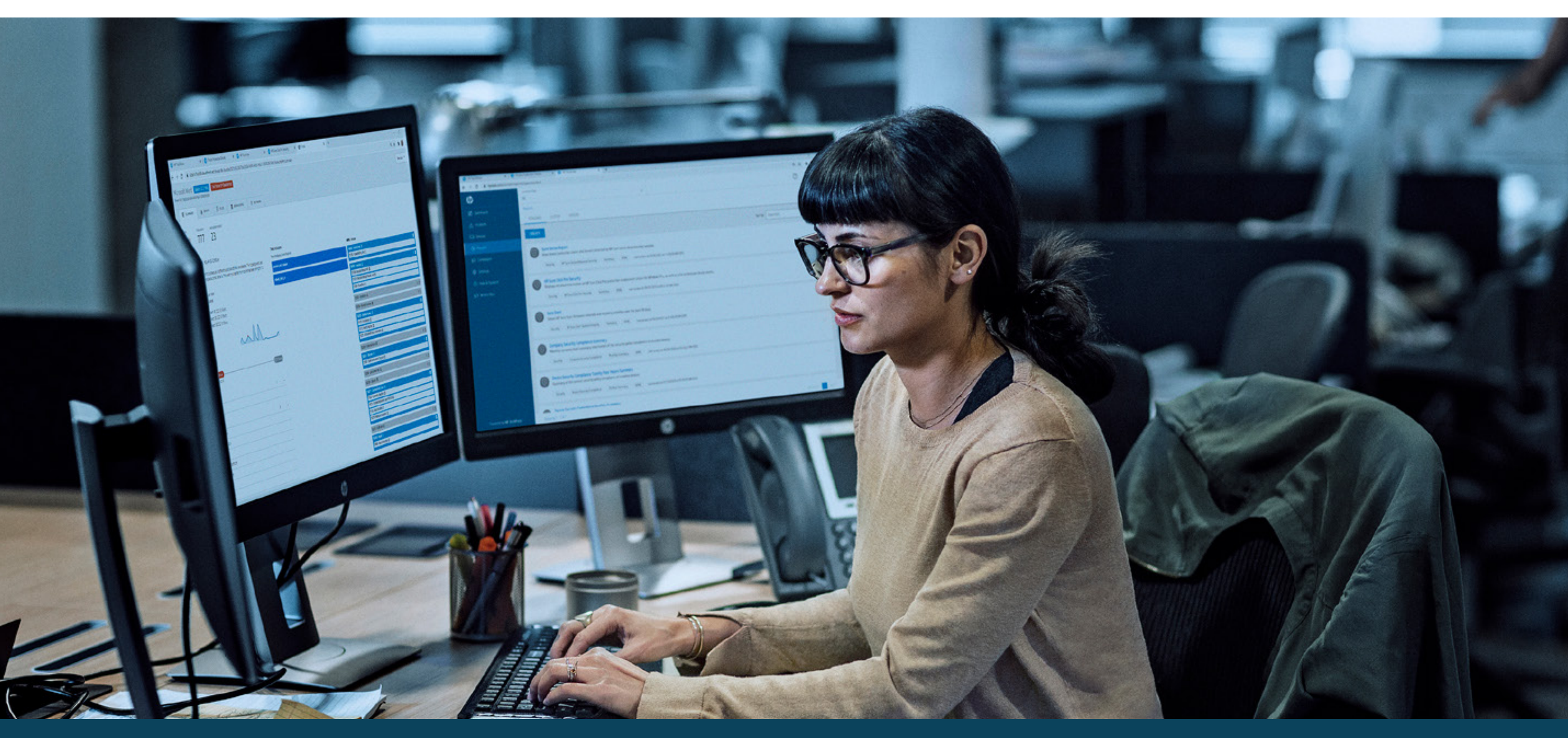
CYBERSECURITY EXPERTISE IS IN SHORT SUPPLY.

As counterintuitive as it seems, companies are hiring sharply fewer cybersecurity experts—even as the threat levels are rising.[1] About 85% of organizations report a shortfall of skilled IT security personnel.[5] Among those who were already in place during the pandemic, 32% report an increased workload,[2] while 47% say their day-to-day activities were changed by being reassigned to other, non-security-related IT duties.[1,2]

SHORTFALL OF

3 MILLION

CYBERSECURITY WORKERS WORLDWIDE[1]



PRIORITIZE PROTECTION WITH HP PCS ADVANCED IN ENDPOINT SECURITY [10]

HP Elite Drogonfly G2 powered by Intel® Core™ i7 processor are made for today's challenges, with hardware enforced security features working together to create an always-on, always-acting, resilient defense. From the BIOS to the browser, above, in and below the OS, these constantly evolving solutions help protect your PC from threats. HP Elite Drogonfly G2 offer security features like Privacy Camera, self-healing BIOS, the latest and fastest Wi-Fi [6] connectivity, long battery life and the power and performance for smooth virtual collaboration. Together with Intel® Core™ i7 processor, you get the latest software and out-of-the-box hardware security features to help defend your devices and your business.

Learn more :
https://www.hp.com/wolfsecurityforbusiness

HP ELITE DROGONFLY G2
358V8EA

1 ((SC)² Cybersecurity Workforce Study, April 28, 2019

2 The Impact of the COVID-19 Pandemic on Cybersecurity, ISSA, July 30, 2020

3 Ponemon Institute 2020 State of Endpoint Security Report sponsored by Morphisec, January 2020

4 HP Proprietary Research, May 2020

5 CyberEdge 2020 Cyberthreat Defense Report, March 2020

6 Proofpoint Human Factor Report 2019, September 2019

7 Mimecast The State of Email Security 2020, Juni 2020

8 AV-Test SECURITY REPORT 2019/2020, 26. August 2020

9 15th Annual 2020 Cost of a Data Breach Study: Global Overview from IBM Security and Ponemon Institute, July 2020

10 Based on HP's internal analysis of isolation backed, deep learning endpoint security services including SaaS and managed services. Most advanced based on application isolation and