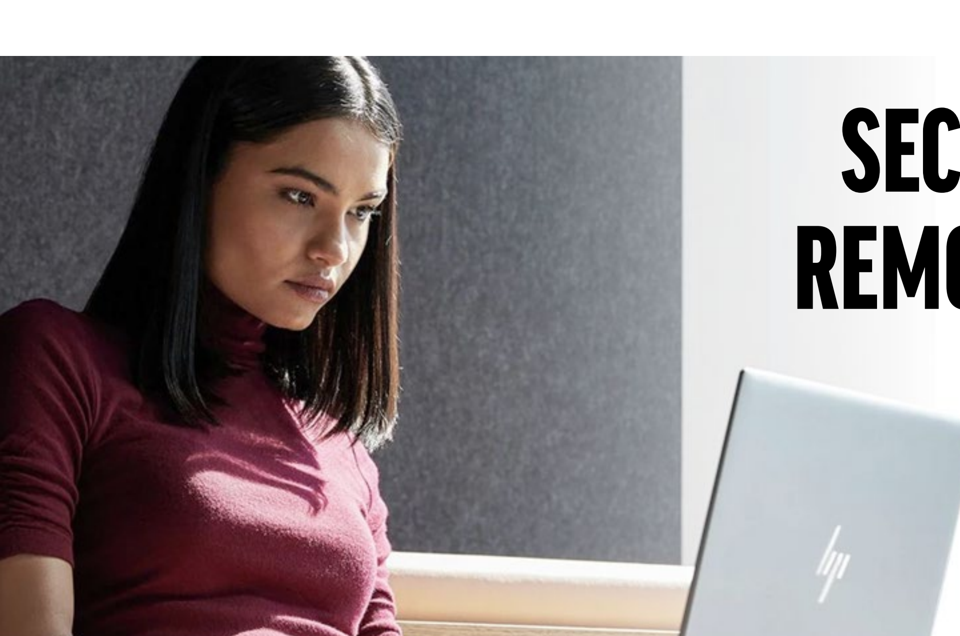
SECURE YOUR REMOTE WORK ESTATE



13%

This year ransomware has continued its upward trend with an almost **13% rise**—an increase as big as the last five years combined.[1]

$1.8B

Phishing was the number-one complaint for individuals and businesses in 2020, leading to **$1.8 billion in business losses.**[2]

40%

40% of office workers surveyed aged 18 to 24 reported clicking on a malicious email.[3]

12x

Executives are **targeted 12X more** than other employees.[4]

82%

82% of breaches involved the human element, including social attacks, errors, and misuse.[5]

Regardless of the amount of training, people keep clicking on phishing emails and opening holes in security. Regardless of the quality or quantity of layers of security deployed, zero-day vulnerabilities, deployment mistakes, and human error can create security gaps that attackers will exploit.

The questions that need to be asked are:

- What does the organisation have in place to prevent a ransomware infection?
- What does the organisation have in place to limit the damage of a successful attack?
- What does the organisation have in place to alert against infection?
- What does the organisation have in place to react to an attack?

MANAGING THE ENVIRONMENT

Risk assessments

- In-house IT security must ensure they are up to date with the current best practices.

Advanced security controls

- Implement 2-factor authentication e.g., Biometrics + PIN, or Password + One-time password (OTP).
- If possible, use Transparent Data Encryption (TDE).
- Provide a VPN for secure access to the corporate network.
- Over and above the VPN, enable network segmentation and Layer-7 access control.
- Patch internal servers and firewalls.

SECURING THE REMOTE ESTATE

Device security for remote/hybrid workers

Personal devices can be a threat vector: avoid BYOD, if possible.

- Provide secure devices for employees.
- Create a blocklist and an allowlist of permissible applications.
- Carry out periodic device scans and updates.
- Consider a 'no public Wi-Fi' policy for remote work.
- IT security must learn to embrace suspected breach reports:
  - Employees must never feel afraid to report suspect activity.
  - False positives are better than unreported breaches.

Locking Windows

- Software can be configured to block or require additional authorisation to permit the download or launch of executable files.
- Similarly, Windows Script Host can be disabled as a defence against JavaScript malware.
- Configure Windows to always show extensions, so employees can learn to identify .exe and other potentially malicious file types.
- Leverage advanced threat prevention capabilities such as antivirus and anti-spyware.

Remote network and endpoint security

All remote access must be authorised and completely secure.

Your endpoint security software should have key components to make your networks and devices secure, including:

- Machine-learning classification to detect zero-day threats near real-time and advanced protection from a ransomware attack.
- Antivirus to detect and protect devices and operating systems against malware.
- Proactive web security to ensure safe browsing along with data classification and data-breach prevention.
- Email and disk encryption to prevent data exfiltration. Your endpoint security software is essential as it offers your remote team an email gateway to block phishing attempts*.
- An effective spam filter enhanced by cloud-based threat intelligence can prevent many attacks, and implementing effective DMARC, DKIM, and SPF email security tools can block even more. Email gateways are another effective first line of defence.

(* Notebooks like the HP Dragonfly help protect your PC against cyber-attacks with hardware-enforced security. HP Sure Click opens websites and untrusted documents in a micro-VM to contain potential malware. Scroll down for more.)

SCROLL DOWN TO SEE DEVICES FROM HP THAT ARE BUILT FOR SECURITY

Select HP notebooks are preinstalled with HP JumpStart to ensure users get up and running quickly and securely.

INFRASTRUCTURE STRATEGIES

Securing the back-end with a zero-trust approach

- Utilise EPPs (Endpoint Protection Platforms) to examine every file entering the network and harness cloud solutions for an ever-growing database of threat information.
- Deploy the EDR (Endpoint Detection and Response) component. These allow for more protection against advanced threats like polymorphic attacks, zero-day attacks, and ransomware attacks (malware).
- Implement XDR (Extended Detection and Response) that not only protects endpoints but also helps you to apply analytics across all your data.
- Engage with specialist service providers for managed security services, managed detection and response (MDR), Backup-as-a-Service (BaaS) and Disaster Recovery-as-a-Service (DRaaS).

IoT security

Connected Internet-of-Things and devices can be an attack vector

- Each device must be granted a unique identifier so that it may connect and transfer data over a protected corporate network.
- Utilise third-party solutions.

HP NOTEBOOK SOLUTIONS

Built for Business. Secure by Design.

These select devices come pre-installed with HP JumpStart to help users quickly set up their work environment, install and register recommended software, and ensure their devices are secure.

HP Elite Dragonfly G3 notebook

- Work anywhere with Windows 11 powered by HP's collaboration and connectivity technology.
- Get a fast and reliable connection with Gigabit-speed Wi-Fi 6.
- Instantly block prying eyes' ability to view your screen with HP Sure View Gen3.
- Help protect your PC from cyber-attacks with hardware-enforced security (HP Sure Click).
- Designed for Windows 11 Pro.

HP EliteBook 640 G9 Notebook PC

- Take collaboration to the professional level with optional 4G connectivity and audio/video enhancers powered by HP Presence.
- With an Intel® Core™ 12th-generation processor, this powerful workhorse is easy to service, has long battery life, and includes optional Thunderbolt™ docking.
- HP Wolf Security for Business creates a hardware-enforced, always-on, resilient defence.
- Optimised for video calls in low-lighting conditions, the HD camera provides visual clarity with low pixelation.
- Designed for Windows 11 Pro (downgrade to Windows 10, if required).

CONTACT CDW TO GET PREFERENTIAL PURCHASING ON THESE HP NOTEBOOKS

CDW AND HP: WORKING TOGETHER FOR YOU

Comprehensive solutions

HP solutions are end-to-end adaptable, affordable, and tested. Combined with CDW's expertise, these solutions are ready to be implemented into any marketplace. The solutions can help to modernise business environments and to prepare for the future in a world increasingly reliant on the Internet of Things.

Revolutionary innovation

With a robust community of developers, OEMs, solution providers, and systems integrators, CDW builds solutions that can lead to transforming organisations and improving individual lives.

Improved security

HP Wolf Security Services provides security that is independently validated and tested proactively.

Security is built in at the silicon level, as well as included in the software.

Zero-Trust isolation stops malware regardless of attack vector.

For more information on how HP and CDW can assist and advise on your hybrid/remote work estate, contact your CDW account manager today.

Follow us to stay updated on all our latest announcements, product developments, and relevant industry news.

1. https://www.verizon.com/business/resources/reports/dbir/2022/summary-of-findings/
2. https://purplesec.us/resources/cyber-security-statistics/
3. https://threatresearch.ext.hp.com/out-of-sight-out-of-mind-new-hp-wolf-security-report-reveals-the-cybersecurity-challenges-of-hybrid-workplaces/
4. https://www.verizon.com/business/resources/reports/dbir/2022/summary-of-findings/
5. https://www.verizon.com/business/resources/reports/dbir/2022/summary-of-findings/