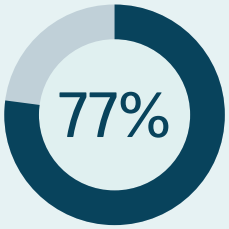
A new era: Securing the U.S. Federal hybrid workforce

Evaluating the challenges and opportunities for hybrid work security

In late 2022, HP surveyed almost a thousand IT leaders in hybrid organizations, including a cross section of the public sector, across the US, UK, France, Germany, and Japan. One of the key findings is that many IT leaders realize hybrid work will likely cause gaps in their security posture. From the survey results, we've identified two core areas where government agencies need to focus when it comes to securing data with a hybrid workforce: device proliferation and off-network access.

A proliferation of devices and software

Hybrid work means more staff on more devices using a wider variety of apps. This creates an ever-growing number of endpoints cybercriminals can use to try to gain access to agency networks, so every one of these endpoints needs to be secured.



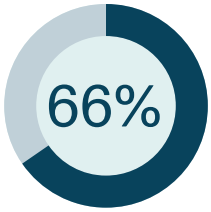
believe cyberattacks will accelerate as endpoint numbers grow[1]

7 in 10

agree hybrid work increases the risk of lost or stolen devices[1]

People working outside the agency network

Even in government, the workplace is no longer a closed-network system. IT security now needs to include endpoint and data protection solutions for staff who use home internet and even public Wi-Fi to access the agency network.



agree compromised hybrid workers pose the greatest cybersecurity threat[1]

Nearly 2/3

find it challenging to have threat detection keep pace with hybrid employee behavior[1]

National Cybersecurity Protection System

The U.S. Cybersecurity & Infrastructure Security Agency has established the National Cybersecurity Protection System to combat and mitigate cyberthreats to the Federal Civilian Executive Branch.[2]

Tools to build hybrid workplace resilience

Technology is the key enabler in hybrid work. It also plays a primary role as an attack vector and defensive tactic. Deploying the right tools is the most effective action you can take to prevent and remediate endpoint breaches.

Endpoint detection and response (EDR)

Monitor system activity on all user devices, trigger alerts when suspicious behavior is detected, and even take action to contain the threat.

Cloud access security broker (CASB)

Manage and control access to cloud resources by simplifying employee access while restricting access to unauthorized or malicious users.

Application isolation

Protect endpoints from known and unknown threats by isolating high-risk activities inside temporary virtual containers.

Next-gen antivirus

Use AI and machine learning to identify anomalous endpoint behavior to stop threats.

File integrity monitoring (FIM)

Scans an organization's critical files, systems, databases, and applications to detect unexpected modifications.

Security information and event management (SIEM)

Collect and analyze data for security threats. Build a detailed log to improve security management and demonstrate compliance.

"Zero trust. We see less focus on limiting network access, and more focus on new architectures that enable security and freedom for hybrid workers."

Alex Thatcher, Director of Cloud Clients, HP Inc.

LEARN MORE AT HP.COM/WOLF

HP WOLF SECURITY

[1] HP survey of 984 IT leaders in hybrid organizations of 100 to 2,499 employees, across five markets (the US, UK, France, Germany, and Japan), from July to August 2022.

[2] Cybersecurity & Infrastructure Security Agency, "Securing Federal Networks: National Cybersecurity Protection System," accessed August 25, 2023, https://www.cisa.gov/securing-federal-networks-national-cybersecurity-protection-system

4AA8-3262ENUS, September 2023