

ENHANCING PRODUCTIVITY WHILE PREVENTING CYBERATTACKS

# Empowering and Protecting DoD's Hybrid Workforce

## DoD - World Leader in Hybrid Workforce

*With a hybrid workforce spread across the globe and facing rapidly evolving cyberattacks against virtually every element of its digital enterprise, The U.S. Department of Defense (DoD) is fighting a constant battle to provide its warfighters and other personnel with the productivity tools they need while countering all cyber threats.*

In 2021, it was estimated that about 60% of DoD employees were engaged in some form of remote work. This number fluctuates based on operational needs, specific job roles, and security clearances required for specific positions.

It is safe to say that the DoD has more end-users permanently or temporarily deployed in more locations around the globe than any other Federal Department.

For years, hackers have targeted networked printers and scanners that had been susceptible to various forms of exploitation due to unpatched software vulnerabilities, weak or default passwords, or inadequate security measures.

In 2020, a hacker gained access to a network of printers worldwide, printing unsolicited advertisements. Ransomware groups have also targeted printers, either locking them down or leveraging them as entry points into more secure parts of the network.

Data exposure is also a risk as cyberattacks can steal sensitive print jobs or intercept print data in transit.



## HP – World Leader in Printer Security

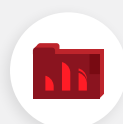
HP has placed significant emphasis on security in its printers, recognizing the growing need to protect sensitive information in a digital-first environment. Some of the key features that HP promotes include:



**SECURE BOOT** which ensures the firmware is genuine and has not been tampered with during the boot-up process.



**DEVICE ACCESS CONTROL FEATURES** such as user authentication help limit who has access to the printer, ensuring only authorized personnel can use specific printer functions.



**NETWORK SECURITY** with strong support for network protocols and configurations, including secure network wiring and wireless protocols (e.g., WPA3) to protect against unauthorized access.








**RUNTIME INTRUSION DETECTION** which monitors the printer's operating system and firmware for unauthorized changes while the printer is running. If a threat is detected, it can immediately shut down the affected components.



**AUDIT LOGS** that provide comprehensive logging of device usage and access, allowing organizations to track activities and identify potential security incidents.

## UNIQUE SOLUTIONS FOR ADDITIONAL SECURITY

-  **HP Sure Start** which is a unique feature that helps protect the firmware from attacks. If a malicious firmware attempt is detected, it automatically reverts to a known good state.
-  **Secure Firmware Updates** in which HP provides a pathway for automatic updates to the printer's firmware that is secure, ensuring that all devices are protected against the latest vulnerabilities.
-  **Job Retention** is an option that allows users to hold print jobs securely until the user is physically at the printer.
-  **Data Encryption** to protect sensitive data sent to and from the printer with strong encryption protocols, safeguarding information from interception during transmission.
-  **HP JetAdvantage Security Manager** which is a cloud-based platform that simplifies the management of security policies and compliance across multiple HP devices.

## The Power of Partnership

Together, this powerful suite of printer and network security tools provide an integrated and comprehensive approach to empowering DoD's global hybrid workforce while ensuring that bad actors cannot use the Department's networked printers to gain unauthorized access and disrupt mission delivery.

**Contact us today** to discuss how V3Gate in partnership with HP can give the Department of Defense the most powerful set of printer security features to enable the DoD's hybrid workforce to maintain productivity while preventing cyberattacks.

