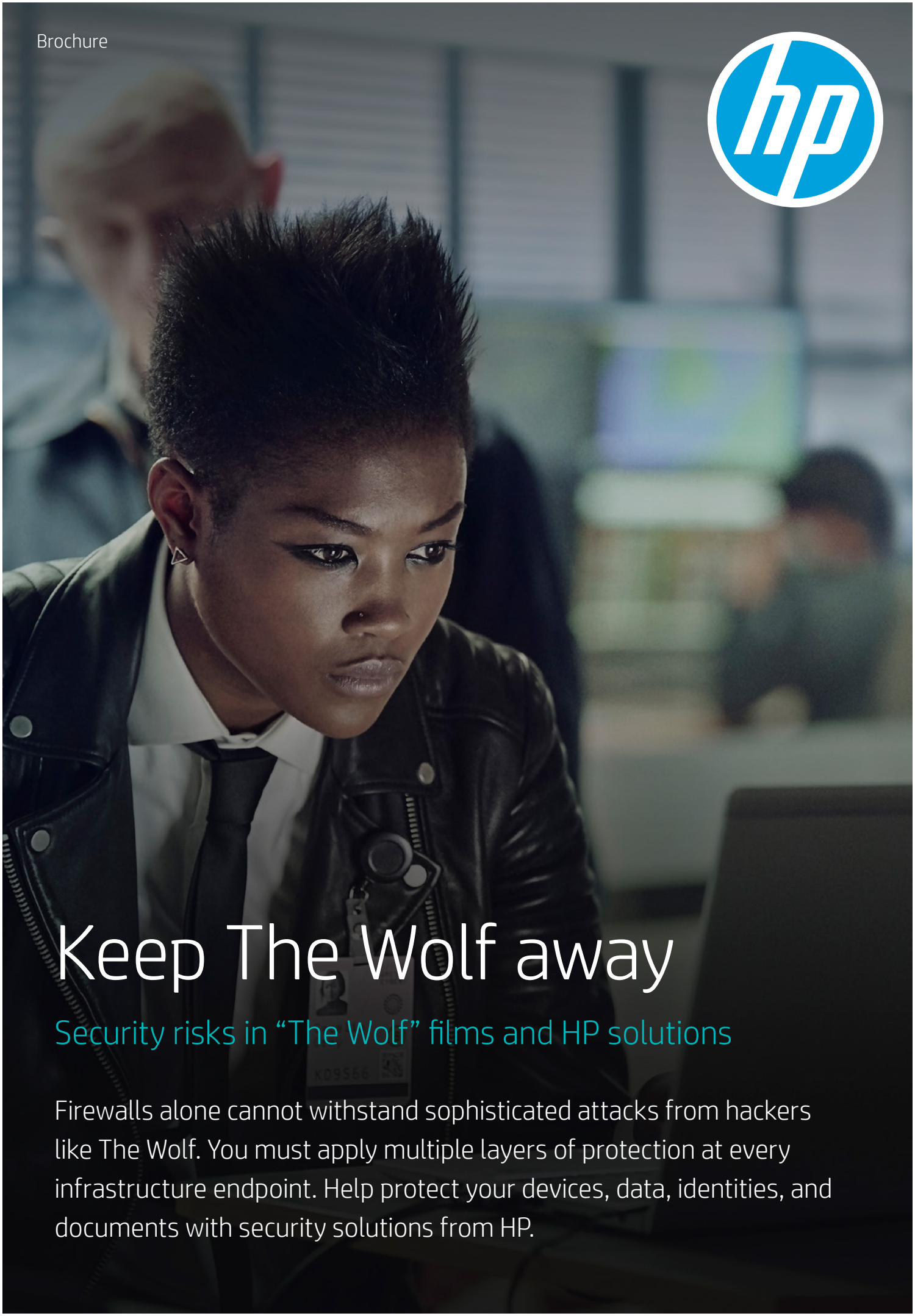
Brochure



Keep The Wolf away

Security risks in “The Wolf” films and HP solutions

Firewalls alone cannot withstand sophisticated attacks from hackers like The Wolf. You must apply multiple layers of protection at every infrastructure endpoint. Help protect your devices, data, identities, and documents with security solutions from HP.

Season 1 The Wolf

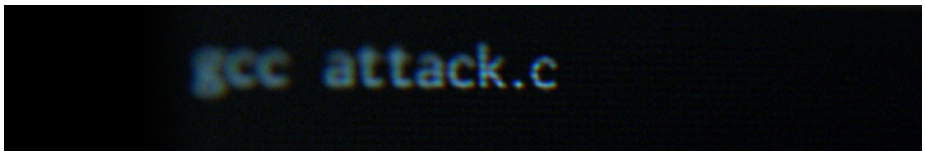
The Wolf brings down a global financial institution by exploiting its vulnerable endpoints. He uses a mobile device to access a printer and inject malware to intercept and read data. The Wolf's "phishing" email then tricks a user into sending malicious code hidden within a PDF to a printer.

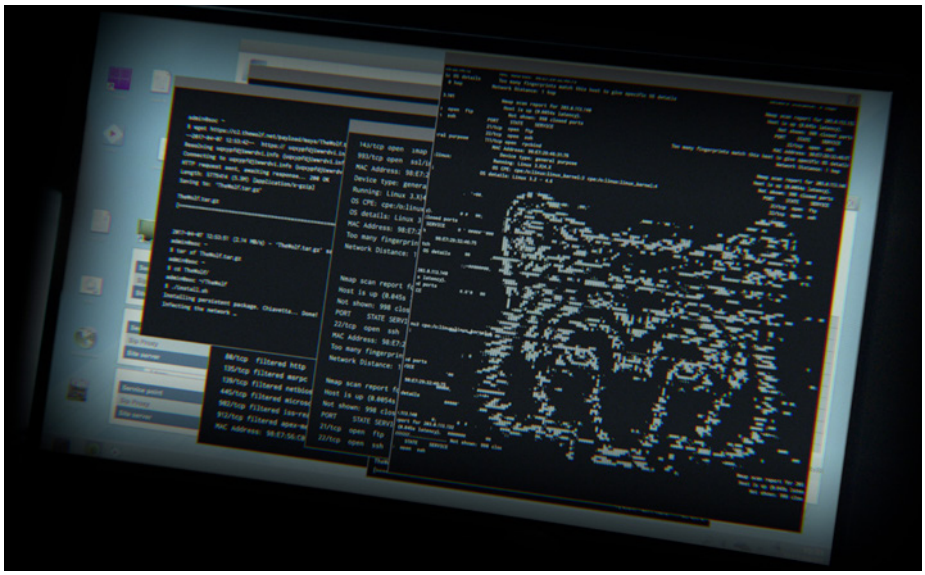
The malware on the printer breaches the firewall and reaches the BIOS level of the company's PCs, so it can collect data and even reinstate itself after network defences deploy.

The Wolf takes an abandoned print from a printer output tray and sabotages the firm's next stock deal—which devastates stockholder confidence.

Vulnerabilities

- Printer Wi-Fi or Bluetooth® is open without requiring user authentication
- Printer data files are not encrypted
- Users do not recognise suspicious emails or print files
- Printers and PCs do not have BIOS-level malware protection
- Sensitive documents are exposed in output trays





Season 2 The Hunt Continues

The Wolf targets patient records stored by one of the medical world's biggest records management companies. He hacks into a PC, then uses a printer's USB port to upload malware behind the firewall to search for connected devices to compromise.

Because the printer resides on an unsegmented network, The Wolf can access servers connected to databases filled with sensitive information. He steals millions of confidential patient records, which are readable because the data is not encrypted.

Both the hospital and the software company are liable and face significant fines and damage to their reputation.

Vulnerabilities

- Printer USB port does not require authentication
- Data files are not encrypted
- Printers do not have malware protection
- Printers are not monitored for security incidents

Season 3 True Alpha

The Wolf disrupts operations at one of the world's largest shipping companies and at an international airport.

By emailing an innocent-looking PDF, he gets an office clerk at the shipping company to send a weaponised Postscript file to a printer. Hidden malware spreads throughout the network when the file is sent to the printer, where it remains undiscovered. Soon, The Wolf has access to the CEO's high-profile conference presentation, cranes loading cargo at a port, and the autopilot software of vessels at sea.

Next, The Wolf focuses on a major airport, showing off his ability to control the lights—and potentially multiple critical systems in the airport's network. HP printers helped IT staff investigate and stop the attack.

Vulnerabilities

- Printers in temporary locations are added to the network without adequately configuring for security
- PCs do not have web-browsing protections against accidental downloads
- IoT devices are not monitored and do not include malware detection capabilities
- Printer syslogs are not connected to threat-monitoring tools

How can you protect against similar attacks?

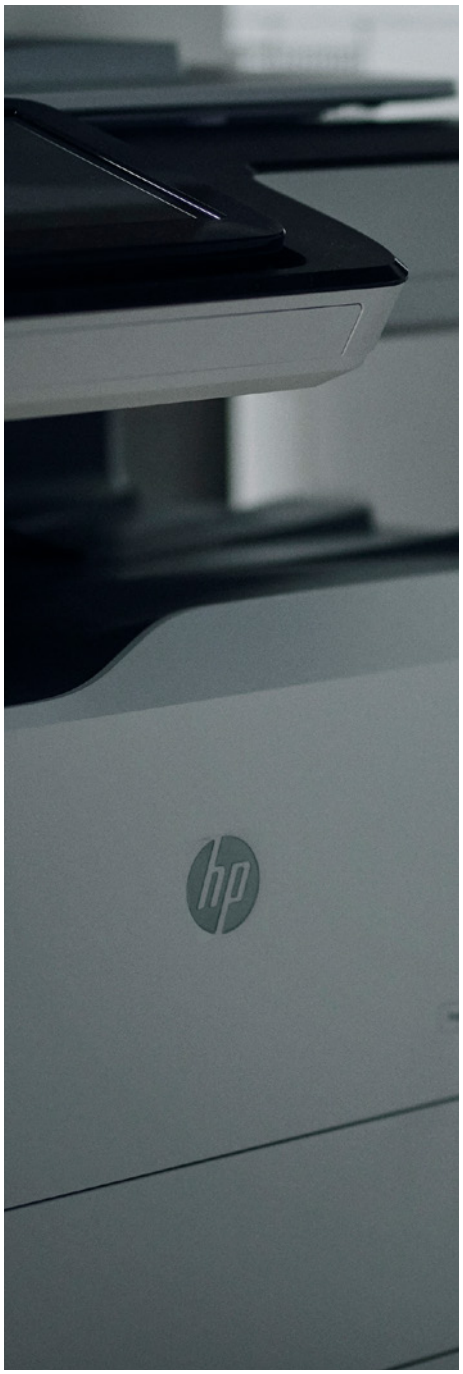
Protect identity: Improve login security with hardened multi-factor authentication on HP Elite PCs.

Protect the device: Upgrade to HP Elite PCs and HP Enterprise printers and MFPs with malware protection to automatically detect, stop, and recover from attacks. Close unneeded USB ports or control access with user controls. Physically isolate browser tabs with HP Sure Click to prevent web-based malware from spreading.[1]

Protect the data: Apply a printer authentication and encryption solution, such as HP Access Control.[2] Require user authentication and encrypt data when using Wi-Fi and Bluetooth printer features. Deploy a mobile authentication and encryption solution, such as PrinterOn Enterprise. Encrypt data at rest and in transit.

Protect the document: Deploy a pull-print solution, such as HP Access Control.[2]

Improve monitoring and management: Automatically configure fleet security policies with HP JetAdvantage Security Manager[3] or HP Printer Security Plug-in for Microsoft® SCCM for printers and HP Manageability Integration Kit (MIK)[4] for PCs. Enable syslogs to track security events and connect devices to Security Information and Event Management (SIEM) tools for real-time alerts. Turn to an HP security trained MPS provider for configuring and maintaining printers for security.



Protect your business with comprehensive security from HP

The world's most secure printing[5]

HP Enterprise printers and MFPs can automatically detect, stop, and recover from an attack without IT intervention, with features like run-time intrusion detection, HP Sure Start, and HP Connection Inspector. Other protections include encrypted hard drives, upgradeable firmware, and the ability to send security alerts to SIEM tools.

hp.com/go/PrintersThatProtect

The world's most secure and manageable PCs[6]

HP Elite PCs help protect against the most common threats by securing below, in, and above the OS. Multi-factor authentication strengthens identity protection, and the HP Manageability Integration Kit[4] makes it simpler to manage security across the PC fleet. Other protections include hard drive encryption, HP Sure Recover,[7] HP Sure Click,[1] and HP Sure View.

hp.com/go/ComputerSecurity

PrinterOn Enterprise

Get dependable, secure in-network mobile printing for enterprise. Connect virtually any desktop or mobile device to printers from multiple vendors both on and off the trusted network.

hp.com/go/businessmobileprinting

HP Access Control[2]

Restore control, reinforce security, and reduce costs by providing role-based print authentication, authorisation, and secure pull printing capabilities across your organisation.

hp.com/go/hpac

HP JetAdvantage Security Manager[3]

Reduce cost and resources to maintain fleet security with a comprehensive policy-based print security compliance tool. Establish a fleet-wide security policy, automate device settings remediation, install and renew unique certificates, and create fleet-wide compliance reports.

hp.com/go/securitymanager

Learn more at
hp.com/go/hpsecure

[1] HP Sure Click is available on most HP PCs and supports Microsoft® Internet Explorer and Chromium™. Supported attachments include Microsoft Office (Word, Excel, PowerPoint) and PDF files in read only mode, when Microsoft Office or Adobe Acrobat are installed.

[2] HP Access Control must be purchased separately. To learn more, please visit hp.com/go/hpac.

[3] HP JetAdvantage Security Manager must be purchased separately. For details, see hp.com/go/securitymanager.

[4] HP Manageability Integration Kit is not preinstalled, available at hp.com/go/clientmanagement.

[5] Based on HP review of 2018 published security features of competitive in-class printers. Only HP offers a combination of security features that can monitor to detect and automatically stop an attack then self-validate software integrity in a reboot. For a list of printers, visit: hp.com/go/PrintersThatProtect. For more information: hp.com/go/printersecurityclaims.

[6] Based on HP's unique and comprehensive security capabilities at no additional cost and HP Manageability Integration Kit's management of every aspect of a PC including hardware, BIOS, and software management using Microsoft® System Center Configuration Manager among vendors with >1M unit annual sales as of November 2016 on HP Elite PCs with 7th Gen and higher Intel® Core® Processors, Intel® integrated graphics, and Intel® WLAN.

[7] HP Sure Recover is available on HP Elite PCs with 8th generation Intel® or AMD processors and requires an open, wired network connection. Not available on platforms with multiple internal storage drives, Intel® Optane™. You must back up important files, data, photos, videos, etc. before use to avoid loss of data.

Sign up for updates
hp.com/go/getupdated

Share with colleagues

4AA7-0231EEW, August 2018, Rev. 1