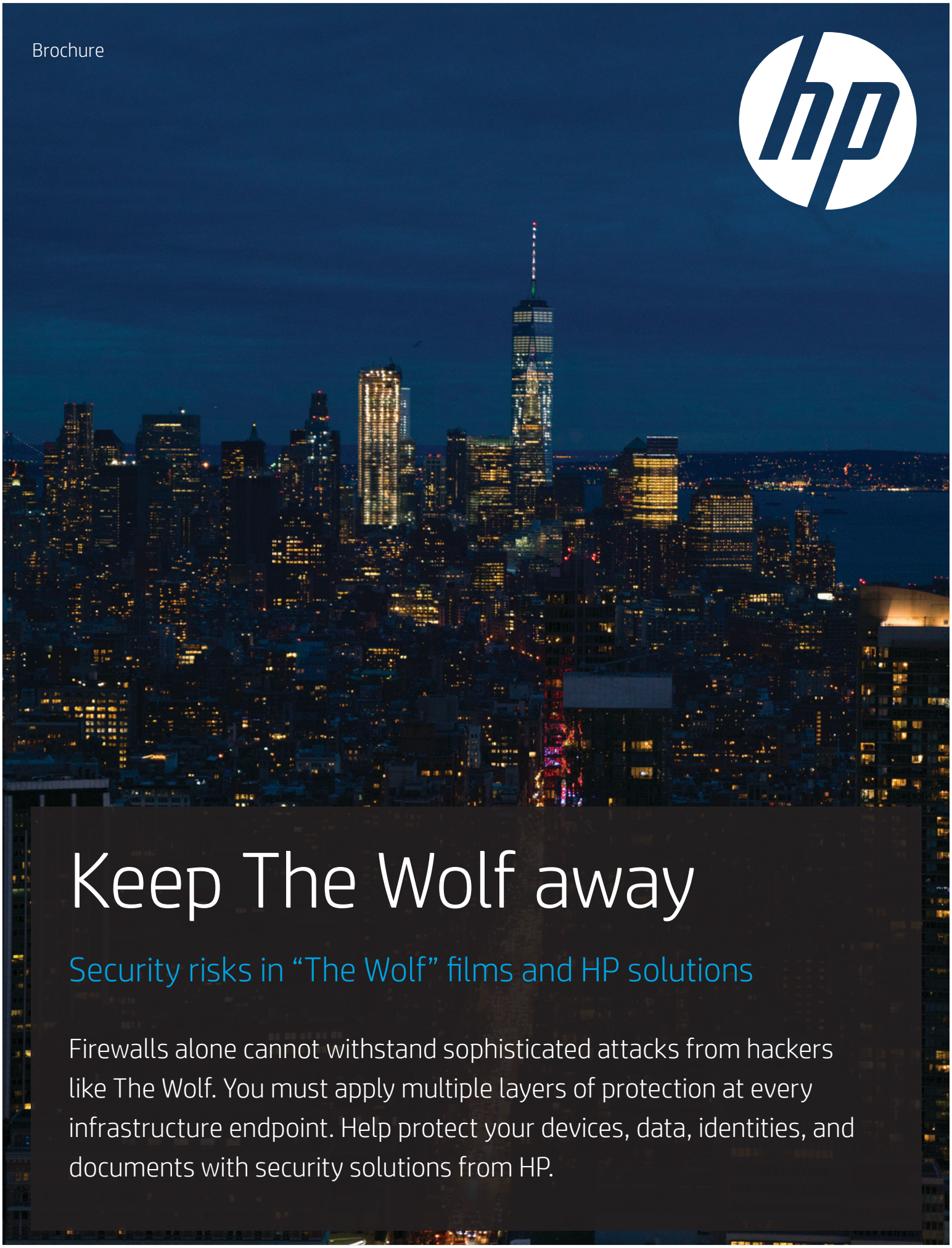
Brochure



Keep The Wolf away

Security risks in “The Wolf” films and HP solutions

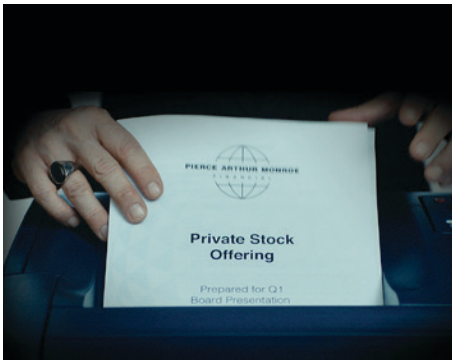
Firewalls alone cannot withstand sophisticated attacks from hackers like The Wolf. You must apply multiple layers of protection at every infrastructure endpoint. Help protect your devices, data, identities, and documents with security solutions from HP.

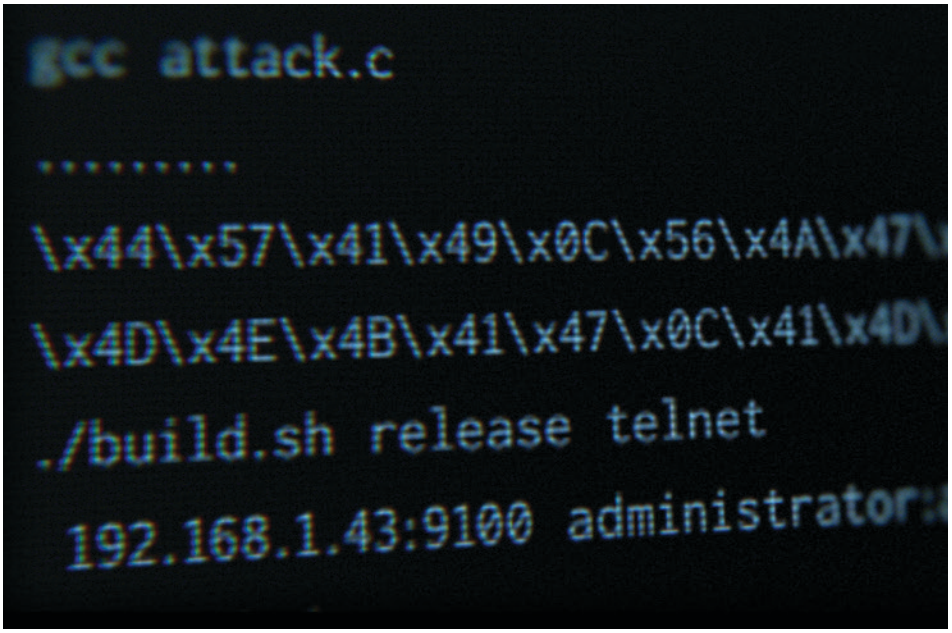
Season 1 The Wolf

In the first film, The Wolf brings down a global financial institution by exploiting its vulnerable endpoints. The Wolf uses a mobile device to access a printer and inject malware to intercept and read data. He then uses a "phishing" email to trick a user into sending malicious code hidden within the print file to a printer.

The malware on the printer breaches the firewall and spreads to the company's PCs. The code resides at the BIOS level, so it can continually supply data and even reinstate itself after network defenses deploy.

Finally, The Wolf discovers a confidential document in the output tray of an MFP. The public leak of sensitive data causes the company to suffer considerable financial and brand damage.





Vulnerabilities

- Printer Wi-Fi or Bluetooth® is open without requiring user authentication
- Printer data files are not encrypted
- Users do not recognize suspicious emails or print files
- Printers and PCs do not have malware protection
- Documents abandoned in output trays may expose sensitive information

How can you protect against similar attacks?

Protect the data: Turn off Wi-Fi/Bluetooth or require authentication; apply a mobile authentication and encryption solution, such as HP JetAdvantage Connect or HP Access Control.

Protect the device: Upgrade to HP Elite PCs and HP Enterprise printers and MFPs with malware protection to automatically detect, stop, and recover from an attack without IT intervention. HP Sure Start helps devices self-heal by rebooting using a safe copy of their original BIOS code.

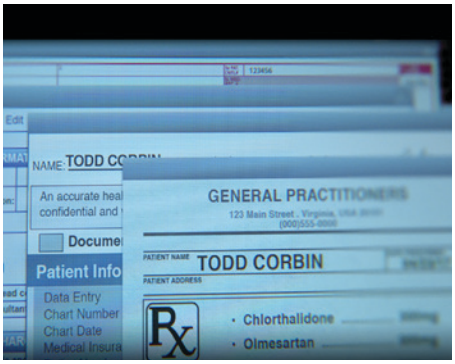
Protect the document: Deploy a pull print solution, such as HP Access Control or HP JetAdvantage Secure Print.

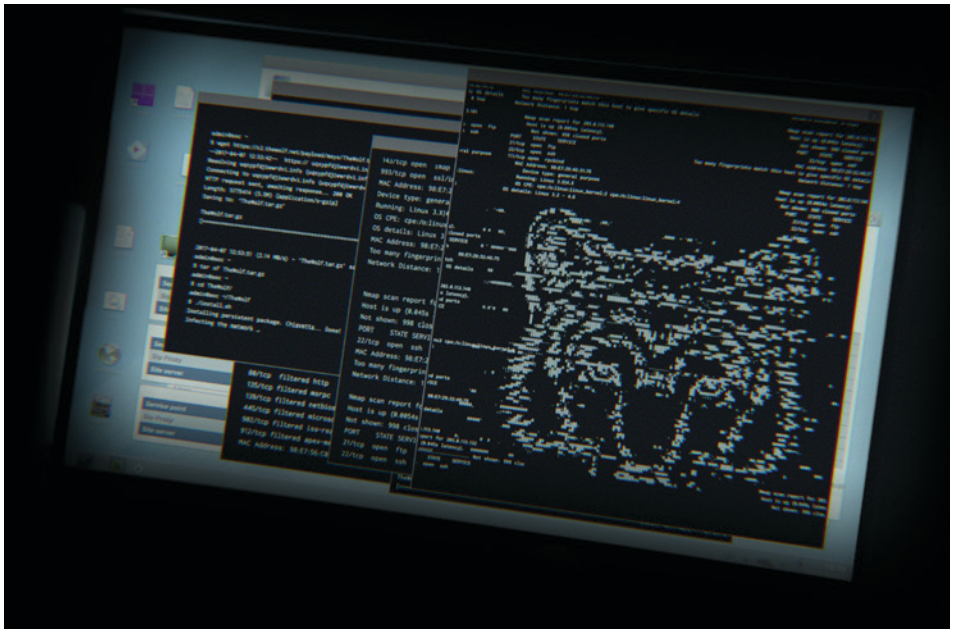
Season 2 The Wolf: The Hunt Continues

In the second film, The Wolf targets patient records stored by one of the medical world's biggest records management companies. He hacks into a PC and later a hospital printer by using the printer's USB port to upload malware.

Since the unsecured printer is connected to the network, the malware is already behind the firewall and can search for other connected devices to compromise. And 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.

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





Vulnerabilities

- PC is unlocked when user walks away
- Printer USB port does not require authentication to use
- Data files are not encrypted
- Printers and PCs do not have malware protection
- Printers are not monitored for security incidents

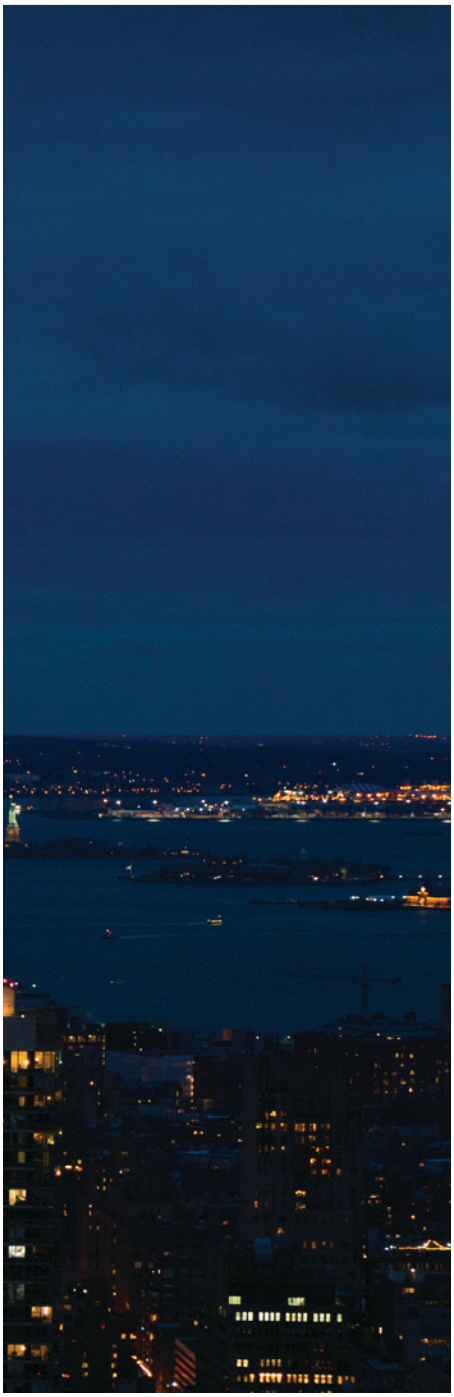
How can you protect against similar attacks?

Protect identity: Use multi-factor authentication on HP Elite PCs.

Protect the data: Apply a printer authentication and encryption solution, such as HP Access Control; close unused ports or control access with user controls; use strong encryption controls for all data at rest and in transit.

Protect the device: Upgrade to HP Elite PCs and HP Enterprise printers and MFPs with built-in malware protection to stop attacks and self-heal down to the BIOS with HP Sure Start.

Improve monitoring and management: Deploy HP JetAdvantage Security Manager (printers) and Management Integration Kit[1] (PCs) to automatically configure device security policies across the fleet; enable syslogs to track security events; connect printers to Security Information and Event Management (SIEM) tools for real-time intrusion notification.



Protect your business with comprehensive security from HP

The world's most secure printing[2]

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

The world's most secure and manageable PCs[3]

HP Elite PCs help protect against the most common threats by securing below, in, and above the OS. HP Multi-Factor Authenticate strengthens identity protection, and the HP Management Integration Kit[1] makes it simpler to manage security across the PC fleet.

HP JetAdvantage Connect

Leverage existing IT network tools and policies to manage printing from smartphones and tablets while providing users with the ability to securely print as easily as from a PC—no app needed.

HP Access Control

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

HP JetAdvantage Secure Print

Protect sensitive documents with cloud-based pull printing. Users authenticate at their chosen print location to pull and print their jobs.

HP JetAdvantage Security Manager

Reduce cost and resources to maintain fleet security with the industry's only policy-based print security compliance tool.[4] Establish a fleet-wide security policy, automate device settings remediation, install and renew unique certificates, and create fleet-wide compliance reports.

Office DEPOT

Contact your Office Depot representative to learn more.

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

[2] Based on HP review of 2016 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.

[3] 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 Intel® Core® Processors, Intel® integrated graphics, and Intel® WLAN.

[4] Competitive claim based on HP internal research on competitor offerings (Device Security Comparison, January 2015) and Solutions Report on HP JetAdvantage Security Manager 2.1 from Buyers Laboratory LLC, February 2015. To learn more, please visit hp.com/go/securitymanager.

Share with colleagues

© Copyright 2017 HP Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Microsoft is a U.S. registered trademark of the Microsoft group of companies. Bluetooth is a trademark owned by its proprietor and used by HP Inc. under license.

4AA7-0231ENW, June 2017