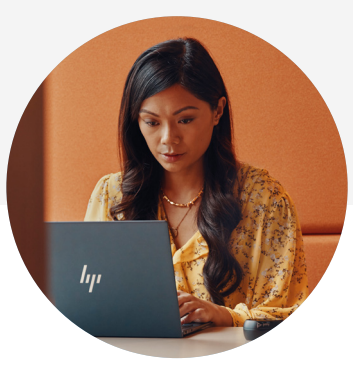
HP Wolf Security and HP Workforce Solutions present:

A not very fun, really bad day for IT



Meet Mei, an IT manager for a company with 12,000 employees. Her team oversees thousands of users and devices that are used in the office, at home, and on the road. Strap in, and let's join Mei for a day that's one wild ride.

6:43 AM at home

CEO gets malware from public Wi-Fi

While on her first cup of coffee, she gets a call with a code red. Their CEO is overseas, and his laptop started "acting funny" after he logged into public Wi-Fi at an airport.

The Prognosis:

- ✓ This simply wouldn't have happened with the right browser isolation
- ✓ And the right digital workspace tool might have kept the CEO off the bad network

43%

of people have had their online security compromised on public Wi-Fi[1]

7:05 AM at home

Malware corrupts laptop OS

After having the CEO restart his laptop with no change, Mei coordinates with her security director to troubleshoot the issue.

The Prognosis:

- ✓ This wouldn't be a big deal with system startup recovery
- ✓ And right now, they could sure use a worldwide repair and replacement plan

8:07 AM at home

Company-wide firmware update initiated

It's officially an "all hands on deck" cluster, so Mei heads into the office to do damage control. The security director recommends everyone's laptops be updated "just in case".

The Prognosis:

- ✓ They could have handled this easily with remote firmware updating
- ✓ And Endpoint Security Solutions help keep everyone everywhere up to speed

65%

of IT leaders say hybrid workers being compromised is their greatest cyber security weakness[2]

$1.3M

Businesses reported losing an average of $1.3 million from cybersecurity incidents.[3]

3:23 PM in the office

A laptop goes missing

With the CEO's problem sorted, Mei's thoughts turn to lunch when a missing bag with a laptop inside alert comes in. Bonus, the password is written on a sticky note in the bag.

The Prognosis:

- ✓ A suspicious system log in has already occurred
- ✓ This could be nipped in the bud with remote device lock and wipe

8:04 PM still in the office

A major security issue exposed

The missing laptop is finally deactivated, but damage has been done that requires extensive mitigation. Mei resigns herself to another long night and calls her neighbor to feed her fish.

The Prognosis:

- ✓ Mei and her team need better PC protection
- ✓ Mei could feed her own fish if they had hardware-enforced, full-stack, endpoint security
- ✓ A good predictive analytics system could also help get Mei home with her fish more often

HP WOLF SECURITY

HP Wolf Security

Get powerful devices with extensive security built in and turn even your worst bad day into just another productive day at the office

Ways HP could save that day

Wi-Fi Drama

- ✓ Browser isolation at all times: HP Sure Click
- ✓ Security of collaboration: HP Digital Workspaces

Remote rescue

- ✓ System startup recovery: HP Sure Recover
- ✓ Repair and replacement worldwide: HP Support Services

All hands on deck

- ✓ Remote firmware updating: HP Sure Admin
- ✓ Seamless updates across the fleet: HP Endpoint Management Services

M.I.A

- ✓ Remote device lock and wipe: HP Tamper Lock

Prepare ahead

- ✓ Hardware-enforced, full-stack, endpoint security
- ✓ Predictive analytics: HP Workforce Insights & Analytics

GET MORE DETAILS ON HP WOLF SECURITY AND HP WORKFORCE SOLUTIONS

1 Forbes, "The Real Risks Of Public Wi-Fi; Key Statistics And Usage Data," July 25, 202. https://www.forbes.com/advisor/business/public-wifi-risks/

2 HP, "A New Era: Securing the Hybrid Workforce: HP Wolf Security Report," March 2023.

3 IBM, "Cost of a Data Breach Report 2023," July 2023, https://www.ibm.com/downloads/cas/E3G5JMBP

XXX.XXX.XXXX November 2023