HP WOLF SECURITY

LEADER IN DIGITAL MEDIA SETS SIGHTS ON MODERN ENDPOINT MANAGEMENT AND SECURITY

HP DELIVERS BEST-IN-CLASS PC PLATFORM SECURITY AND IT OPERATIONS AT SCALE, WITHOUT THE HASSLE

INDUSTRY:
DIGITAL MEDIA

REGION:
EUROPE

OBJECTIVES

Lower IT operational overhead, while maintaining PC platform security and resiliency

IMPACT

- Reduced IT operational overhead
- Decreased cyber-security risk
- Higher employee productivity
- More robust disaster recovery (cyber security attack recovery)
- Better support for remote working

OBJECTIVES

OPERATIONALLY EFFICIENT IT AND PC SECURITY OPERATIONS

As a leader in digital content delivery, this European company has a long history of innovation in digital security and content delivery. With over 3,000 staff spread across more than 20 countries, it delivers piracy threat management technology for many of the world's best known media brands.

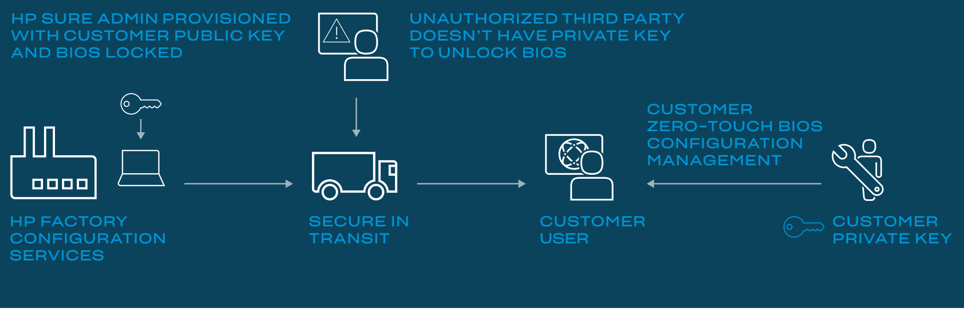
To lower IT overhead and improve the user experience for remote staff in particular, the firm decided to move away from loading 'corporate gold images' on its endpoint PCs, and instead implement modern management centered on Microsoft Intune and Windows Update. An implication of this new strategy was that it needed a scalable, reliable way of onboarding new PCs to Intune, and to re-install a clean software image if a PC was compromised or repurposed. Only after that image was in place and its integrity validated could it rely on Windows Update and Intune respectively to update the OS and install business applications.

A parallel challenge was BIOS security. The primary requirement was to have a robust and operationally efficient way of keeping the BIOS up to date in a hybrid environment, where the device might be never be in the office. The firm had been using per-PC BIOS passwords to secure endpoints, but managing the passwords themselves was a manual, error-prone effort. Unfortunately, the incumbent PC vendor was unable to supply solutions to any of these BIOS management challenges, leading it to consider HP.

"Our goal is to get to a stage where we have zero-touch provisioning of all devices, and HP device security and services are helping us achieve that."

GLOBAL ENDPOINT MANAGEMENT SERVICES, DIGITAL MEDIA COMPANY

SUPPLY CHAIN SECURITY AND ZERO-TOUCH MANAGEMENT


HP SURE ADMIN PROVISIONED WITH CUSTOMER PUBLIC KEY AND BIOS LOCKED
UNAUTHORIZED THIRD PARTY DOESN'T HAVE PRIVATE KEY TO UNLOCK BIOS
CUSTOMER ZERO-TOUCH BIOS CONFIGURATION MANAGEMENT
HP FACTORY CONFIGURATION SERVICES
SECURE IN TRANSIT
CUSTOMER USER
CUSTOMER PRIVATE KEY

20+

COUNTRIES

3K+

EMPLOYEES WORLDWIDE

HARDWARE-BASED PROTECTIONS

ELIMINATE PASSWORD ATTACKS

SOLUTION

HP TECHNOLOGY AND SERVICES FOR SCALABLE, SECURE PC MANAGEMENT

After a relatively brief scan of the market, the company identified HP as a potential replacement vendor. The nature of its requirements meant that IT processes would have to change, and so workshops were conducted with HP prior to vendor selection to understand these changes and the required infrastructure. Because the firm was moving to Microsoft Intune, it had already committed to Azure Active Directory, aligning with HP's cloud infrastructure options.

The company decided to use a combination of HP Factory Services[1] and Microsoft Autopilot for onboarding. As each PC is prepared for shipment, HP prepopulates the customer's Autopilot instance with device enrollment information. The PC can then be shipped directly to the end user, without passing through the IT department. The PC will boot up, connect to Autopilot over the public internet, execute the pre-defined security policy associated with the device, and enroll to Intune.

The next area implemented was BIOS security. The company now procures PCs that have BIOS settings preconfigured by Factory Services and locked with the company's allocated password. The PCs also use HP Sure Start[2], which at boot time validates that the BIOS code and settings haven't been tampered with. A side benefit is that the feature also ensures that BIOS updates (which are done from the cloud) never corrupt the PC if there's any problem during the update. Sure Start is enabled by default and requires no IT management, so it was a relatively easy step to take.

The team turned to HP Sure Admin[3] to upgrade its ongoing BIOS password management. Sure Admin replaced the passwords used for local access with an authentication process based on Microsoft Azure Active Directory. To access the BIOS configuration, an authorized user or IT technician uses the HP Local Access Authenticator smartphone app. The PC displays a challenge QR code that embeds an encrypted PIN, which is scanned by the app.

The app in turn communicates with a dedicated HP KMS (key management system) hosted in the company's Azure instance. This process decrypts the PIN and displays it to the user on their phone, who then types it into the PC to unlock the BIOS settings.

> *"We looked at the holistic view—the design, the technology roadmap, the suite of security offerings, modern management tools, Factory Services and overall HP Services—and the decision was easy to select HP."*
>
> GLOBAL ENDPOINT MANAGEMENT SERVICES, DIGITAL MEDIA COMPANY

SOLUTION AT A GLANCE

HP Services and Solutions:

Sure Recover
Sure Admin
Sure Start
Factory Services

SURE START

SURE ADMIN

SURE RECOVER

To improve OS image management and recovery, the firm implemented HP Sure Recover[4]. This solution allows a PC operating system to be easily re-imaged without end-user involvement should it become corrupted, or if it needs to be updated.

The firm's Sure Recover enabled PCs to run a tamper-protected security agent that communicates with HP's cloud recovery service. The company's IT team or the end user can trigger recovery, resulting in the company's preferred software image being downloaded and installed on the PC. Sure Recover will also execute automatically: if it sees that the boot partition is corrupted, it will trigger re-imaging without user intervention. The new image can be hosted either in the cloud (the option used by this firm) or on dedicated secure flash memory. In either case, Sure Recover uses cryptography to ensure OS image integrity. Once the new OS is installed, the PC continues with the recovery process using Intune and Windows Update.

Both Sure Start and Sure Recover leverage HP's Endpoint Security Controller chip on the motherboard. It prevents the OS from starting if the PC has been compromised and contains a tamper-proof data repository for these features to store settings and keys.

BUSINESS OUTCOMES

A WIN-WIN FOR IT OPERATIONS AND SECURITY

Following a four-week transition process, the firm has been able to put Sure Admin, Sure Start and Sure Recover into production, supporting its HP endpoint laptops and desktops.

The company's fundamental requirement of improving IT efficiency with modern endpoint management while maintaining tight infrastructure security has been met. This includes "zero-touch" deployment of new PCs with security assured during shipment.

All new endpoint hardware is enrolled in Intune via Autopilot, and BIOS administration passwords are no longer used. Intune is used to monitor and audit the PC security posture. Furthermore, it has easier procedures for OS updates, and a disaster recovery plan in place that includes handling a catastrophic event, such as a companywide cyber-attack directed at the endpoints.

Learn more about HP Services at hp.com/hp-services
Learn more about HP Wolf Security at hp.com/wolf

HP Services are governed by the applicable HP terms and conditions of service provided or indicated to Customer at the time of purchase. Customer may have additional statutory rights according to applicable local laws, and such rights are not in any way affected by the HP terms and conditions of service or the HP Limited Warranty provided with your HP Product. For full system requirements, please visit www.hpdaas.com/requirements.

[1] HP Services are governed by the applicable HP terms and conditions of service provided or indicated to Customer at the time of purchase. Customer may have additional statutory rights according to applicable local laws, and such rights are not in any way affected by the HP terms and conditions of service or the HP Limited Warranty provided with your HP Product.

[2] HP Sure Start is available on select HP PCs.

[3] HP Sure Admin requires HP Manageability Integration Kit from hp.com/go/clientmanagement and HP Sure Admin Local Access Authenticator smartphone app from the Android or Apple store.

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

Sign up for updates: hp.com/go/getupdated   Share with colleagues

HP WOLF SECURITY

4AA8-0095ENW, February 2022