HP WOLF SECURITY

RESILIENT SECURITY

INFLUENCED BY ZERO TRUST.

HARDENED IN EVERY PC.

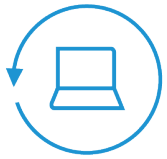
HP WOLF SECURITY

MOST SECURE AND MANAGEABLE PCs


Sure Start


Sure Run


Sure Admin


Sure Recover


Tamper Lock


Sure Click

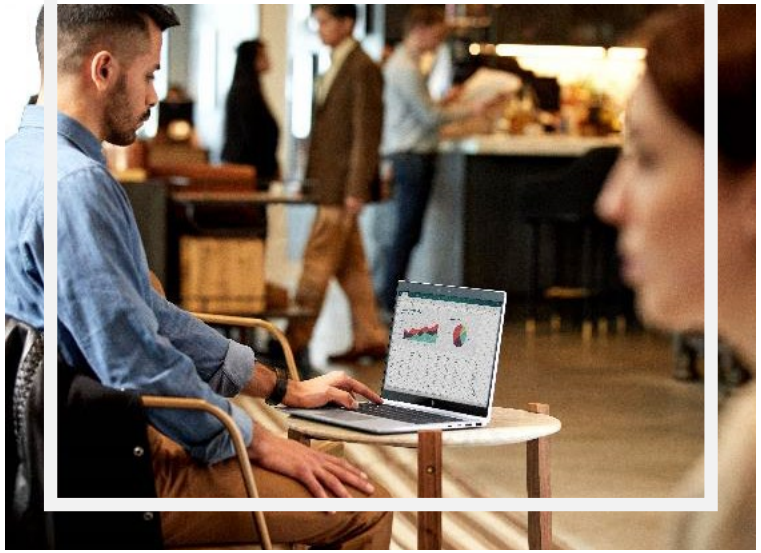

Sure Sense


Sure View (optional)

EVERY ORGANIZATION SHOULD HAVE A

PLAN FOR RESILIENCE

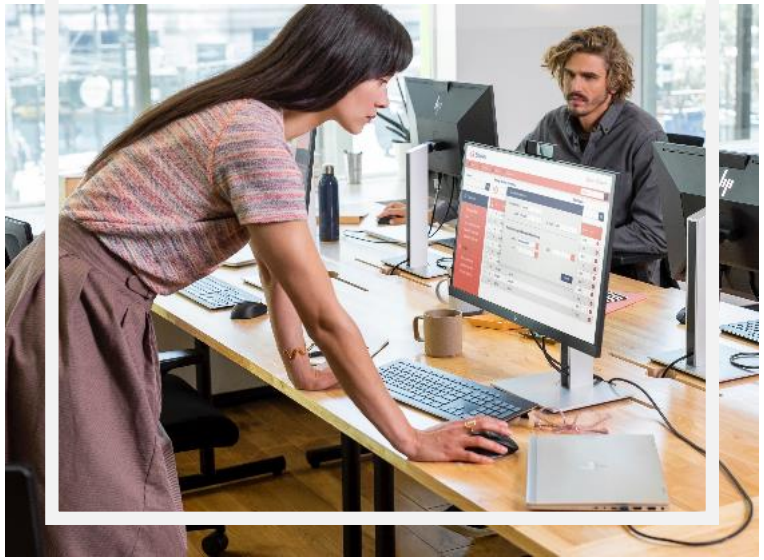
PROTECT



HOW LONG

would it take to recover
1,000 PCs?

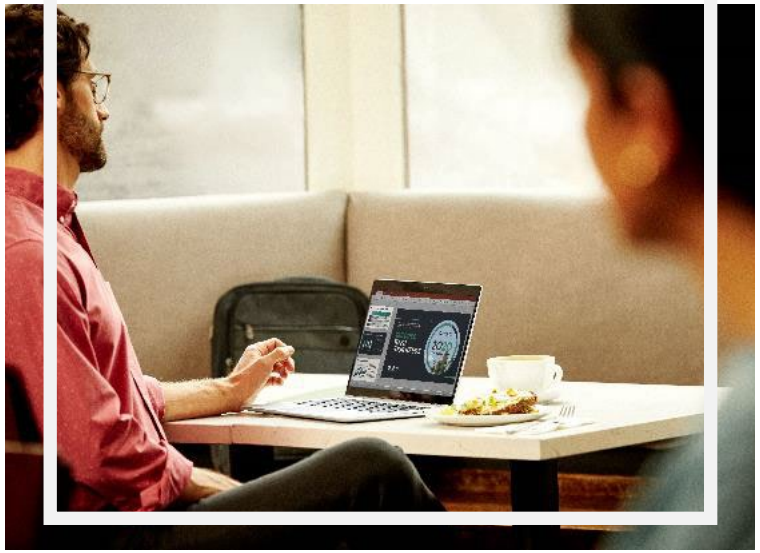
DETECT



HOW DO YOU PROTECT

against malware
you've never seen before?

RECOVER



HOW DO YOU KNOW

when your fleet is
under attack?

HP WOLF SECURITY

IS BUILT USING

ZERO TRUST PRINCIPLES

HARDWARE-ENFORCED RESILIENCY

Hardware that can self monitor and self heal if an attack gets in

LAYERS OF PROTECTION

Proactively prevent threats – below, in, and above the OS

ADVANCED LEVELS OF SECURITY

Advanced security with application isolation and AI Deep Learning technology

"Zero Trust is a core set of principles in the design and operation of systems and their security."

HP WOLF SECURITY FOR BUSINESS

HP WOLF SECURITY

HP CLIENT SECURITY MANAGEMENT
HP MIK or HP CONNECT FOR MEM

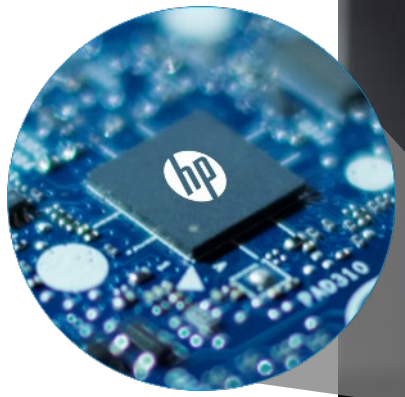
HARDWARE-ENFORCED PROTECTION

	DEVICE	IDENTITY/PRIVACY	DATA
ABOVE THE OS		HP SURE VIEW Built-in Privacy Screen	
		HP PRIVACY CAMERA / HP SURE SHUTTER Built-in Webcam Privacy Shutter	
IN THE OS	MICROSOFT SECURED-CORE PC Best In Class OS Security	HP PRESENCE AWARE Auto Login/Logoff	HP SURE CLICK Hardware-enforce secure browsing/viewing solution
			HP SURE SENSE Protect from never-before-seen malware
BELOW THE OS	HP BIOSPHERE Comprehensive BIOS Management		HP SECURE ERASE Permanent Data Removal on HDD/SSD
	HP SURE START Self-Healing Endpoint Security Controller Protection		CERTIFIED SELF-ENCRYPTING DRIVES HW Data Encryption
	Update HP SURE RUN Protect Applications with Persistence & Kill Prevention		
	Update HP SURE RECOVER Embedded Image Recovery		
	New for 2021 HP SURE ADMIN Cryptographically Secure BIOS Management		
	New for 2021 HP TAMPERLOCK Tamper Protection		

HP ENDPOINT SECURITY CONTROLLER

HP ENDPOINT SECURITY CONTROLLER

UNIQUE HARDWARE ENABLES RESILIENT DEVICES



PROTECT WHERE ANTIVIRUS DOESN'T !!!

Protection starts at the lowest level of the PC

- Hardware-enforced technology only on HP PCs
- ESC always running, even when the system is powered off
- Hardware Root of Trust: protection, detection & recovery
- Physically isolated

Protection continues during runtime

- Ongoing monitoring for health of HP's security system
- HP Wolf Security cryptographic functions secured by hardware

HP SURE START[6]

BEHIND THE TECHNOLOGY

Always-on and run-time persistence

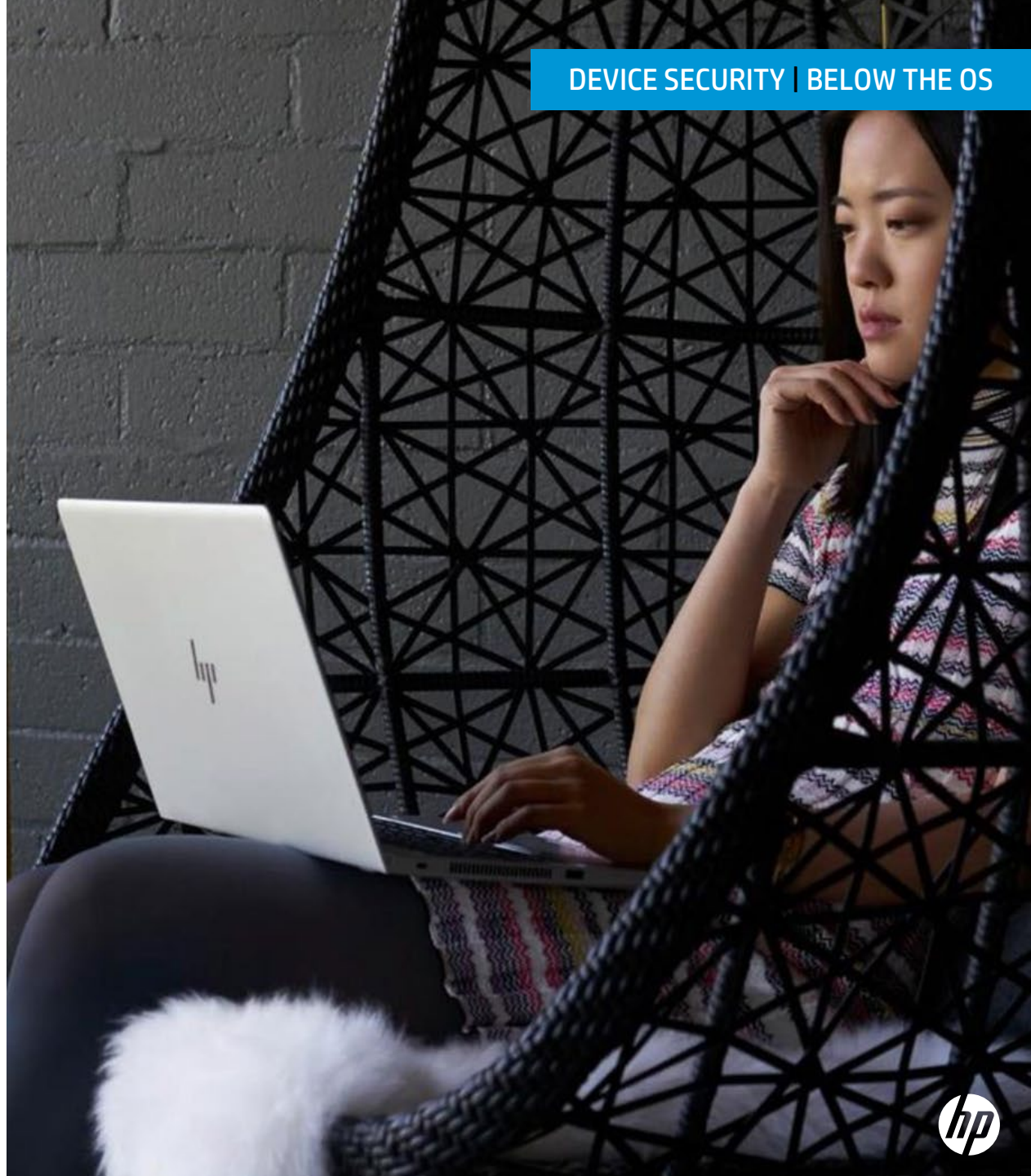
Resilience: Protects, detects, and recovers

Independent Hardware Enforced protection tied to the HP Endpoint Security Controller. Not dependent on OS or CPU.

Protects the BIOS settings

Protection for pre-boot DMA attacks

HP SURE RUN



PROTECTS AGAINST ATTACKERS TURNING OFF CRITICAL CUSTOM APPS

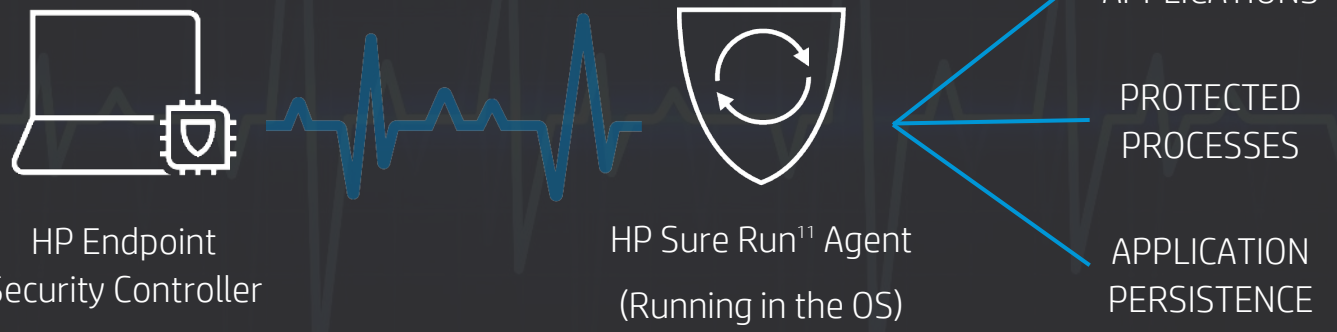
HP Sure Run leverages the HP Endpoint Security Controller to:

- **MONITOR** key processes.
- **ALERT** of any changes.
- Dynamic **PERSISTENCE.**

TRUST IS PART OF OUR DNA

PERSISTENCE TO PROTECT YOUR PC'S KEY SECURITY PROCESSES

HARDWARE-ENFORCED HEARTBEAT



HP SURE RECOVER[12,13]

DEVICE SECURITY | BELOW THE OS

REMOVE THE RISK OF A TIME-CONSUMING BUSINESS DISRUPTION FROM A DESTRUCTIVE MALWARE ATTACK

HOW LONG WOULD YOU NEED TO RECOVER 1,000 MACHINES?

SECURE REIMAGING
For trusted systems

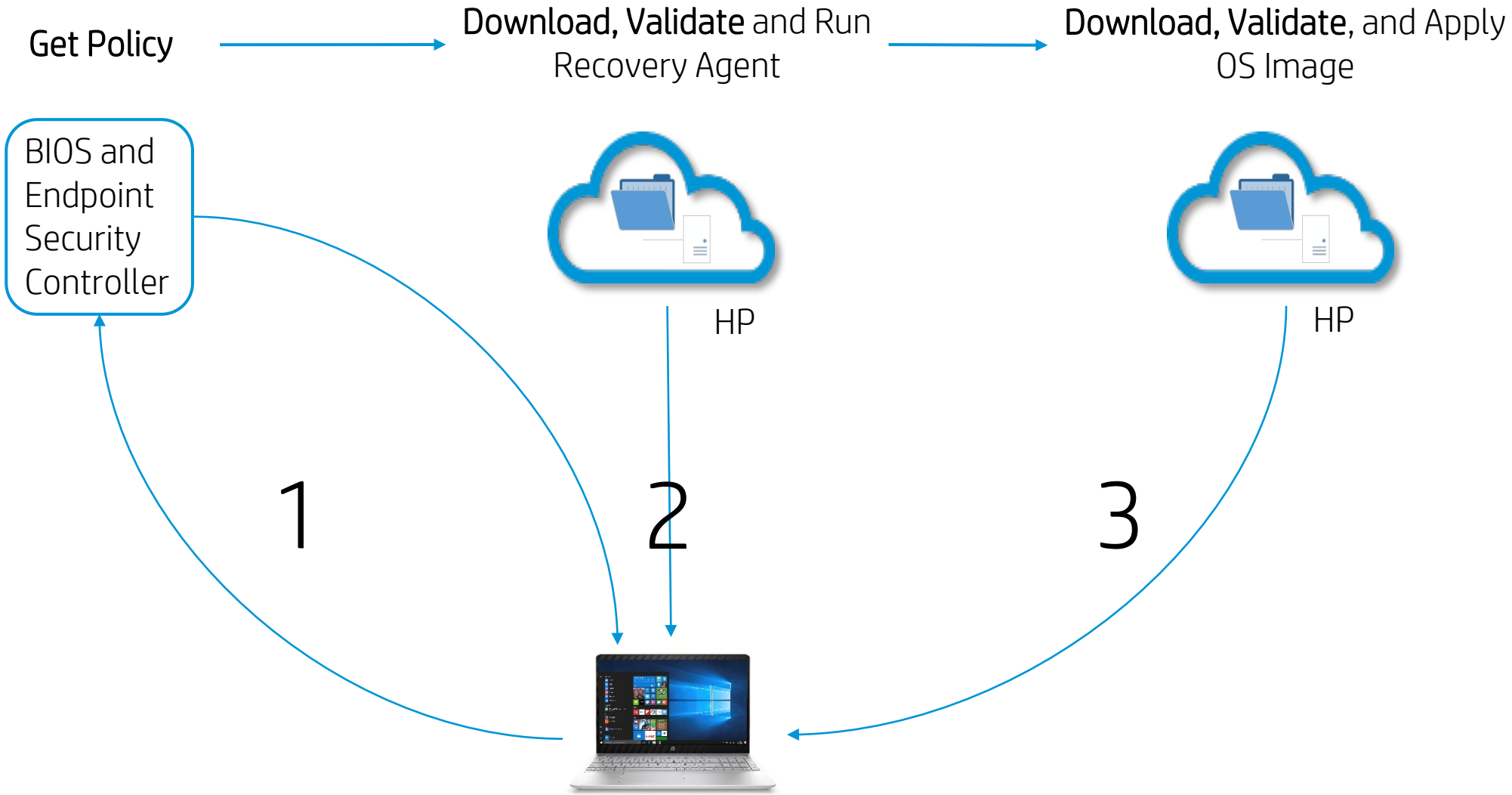
RECOVER QUICKLY
In minutes instead of hours

SUPPORT BUSINESS CONTINUITY
with user-enabled reimaging

"Continual trend of destructive attacks, wipers, malware, and new threats are coming out regularly"

HP Sure Recover is as Easy as 1-2-3 HP's Out of Box setup

Apply Policy, Automate, and Enhance Security



HP TAMPERLOCK

PEACE-OF-MIND FROM PHYSICAL INTRUSION THREATS

SENSORS DETECTION
For case intrusion, and configurable rich policy controls

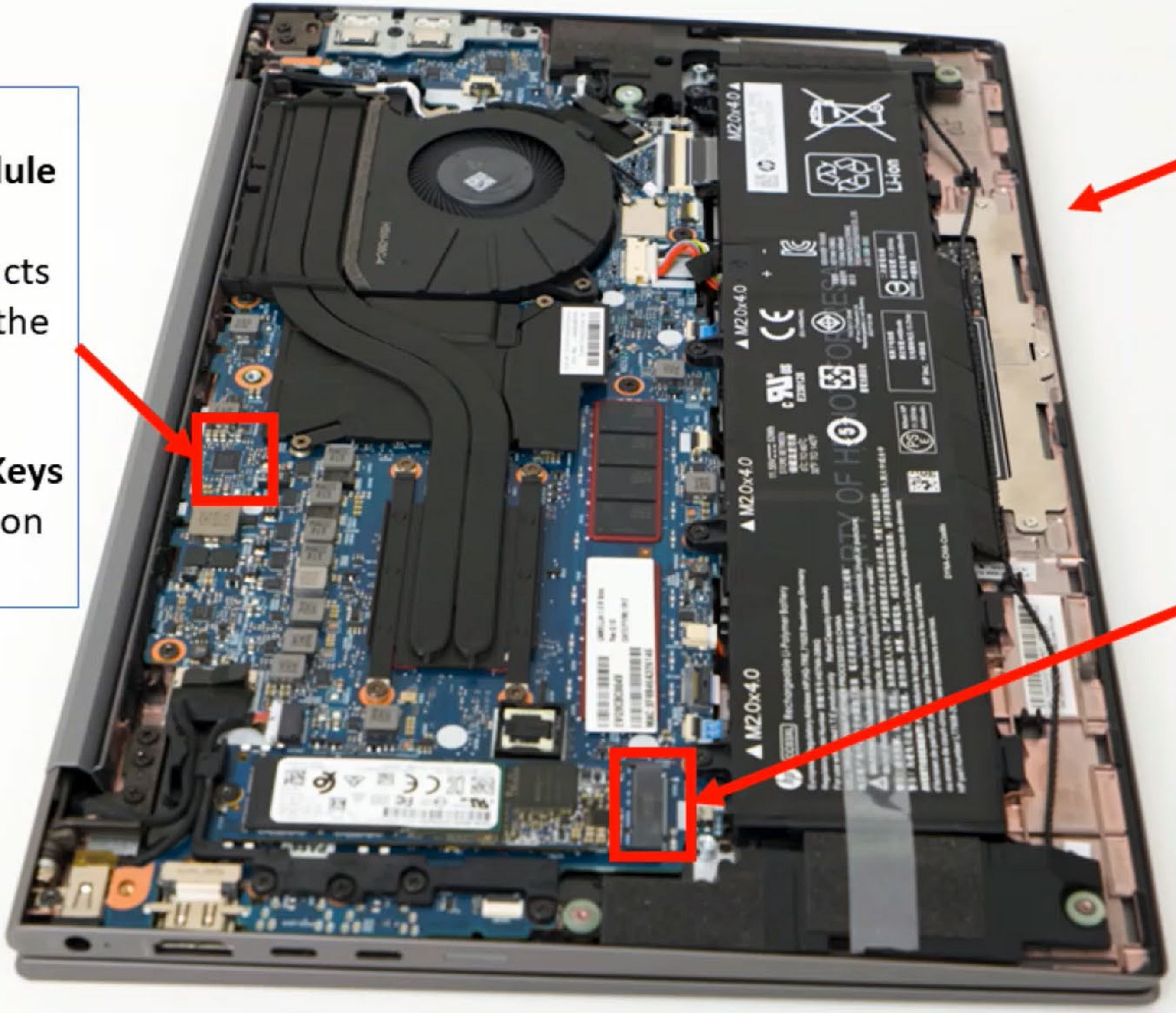
PHYSICAL ATTACK PROTECTIONS
Against DMA attacks, flash replacement attacks, side channel attacks, TPM probing attacks
+ HP Endpoint Controller storage protection

2021 EliteBook 800/1000 G8 and Zbooks Launch HP Tamper Lock

TPM
Trusted Platform Module

Securely storing artifacts used to authenticate the platform

Probing for Bitlocker Keys that protect the data on the Drive (SSD)



Flash Memory

Replacing flash memory to install malware, remote access and control applications.

Internal Ports

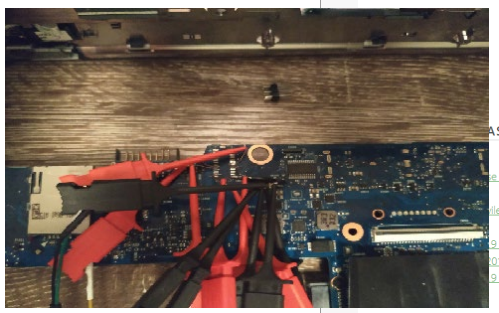
M.2 slot, WWAN card module slots

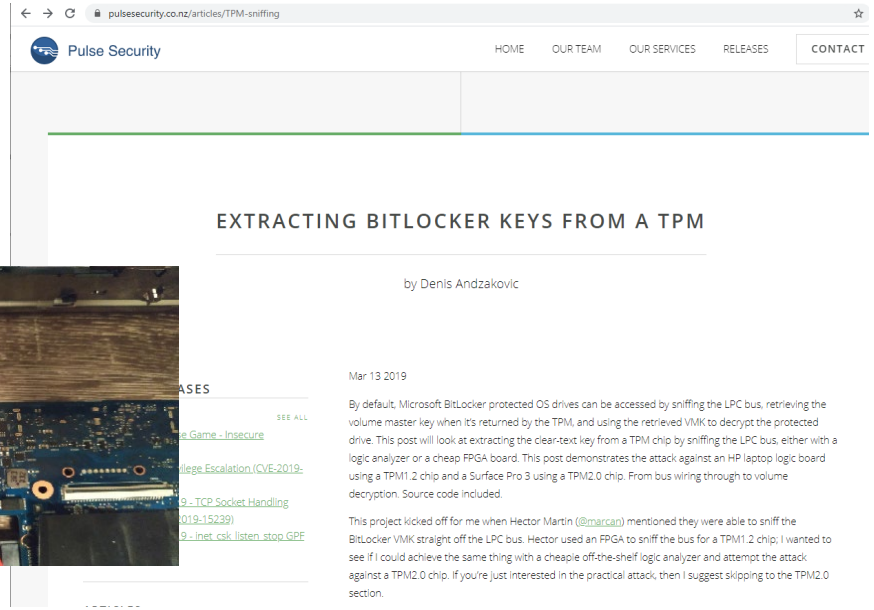
Connecting to internal port to access Memory for passwords and other critical information

HP TAMPER LOCK

Providing protection from physical attacks, which involve disassembly of the system to modify the hardware or implant attacker hardware.

- Sensors to detect if the case has been opened, associated to rich policy controls
  Other physical attack protections, such as





CAPABILITIES	MWKS/ELITE G8
Intrusion Detection	√
Lock on intrusion detection	√
BIOS password based unlock	√
Sure Admin Based Unlock (OTP based/No Password)	√
Shutdown System on Intrusion Detection	√
Clear TPM on Intrusion Detection Event	√
Intrusion Detection Event Logging	√
Protection against Policy/Log attack via SPI programmer	√
Protection against lock defeat via DMA attack	√

HP Confidential. For use by HP only.
© 2021 HP Development Company, L.P. The information contained herein is subject to change without notice.

HP SURE ADMIN

COMPATIBLE WITH 2018 AND NEWER HP PCs

CENTRALIZED PROTECTION OF PRIVATE KEYS USED TO AUTHORIZE REMOTE MANAGEMENT AND LOCAL ACCESS

LOCAL ACCESS AUTHENTICATOR

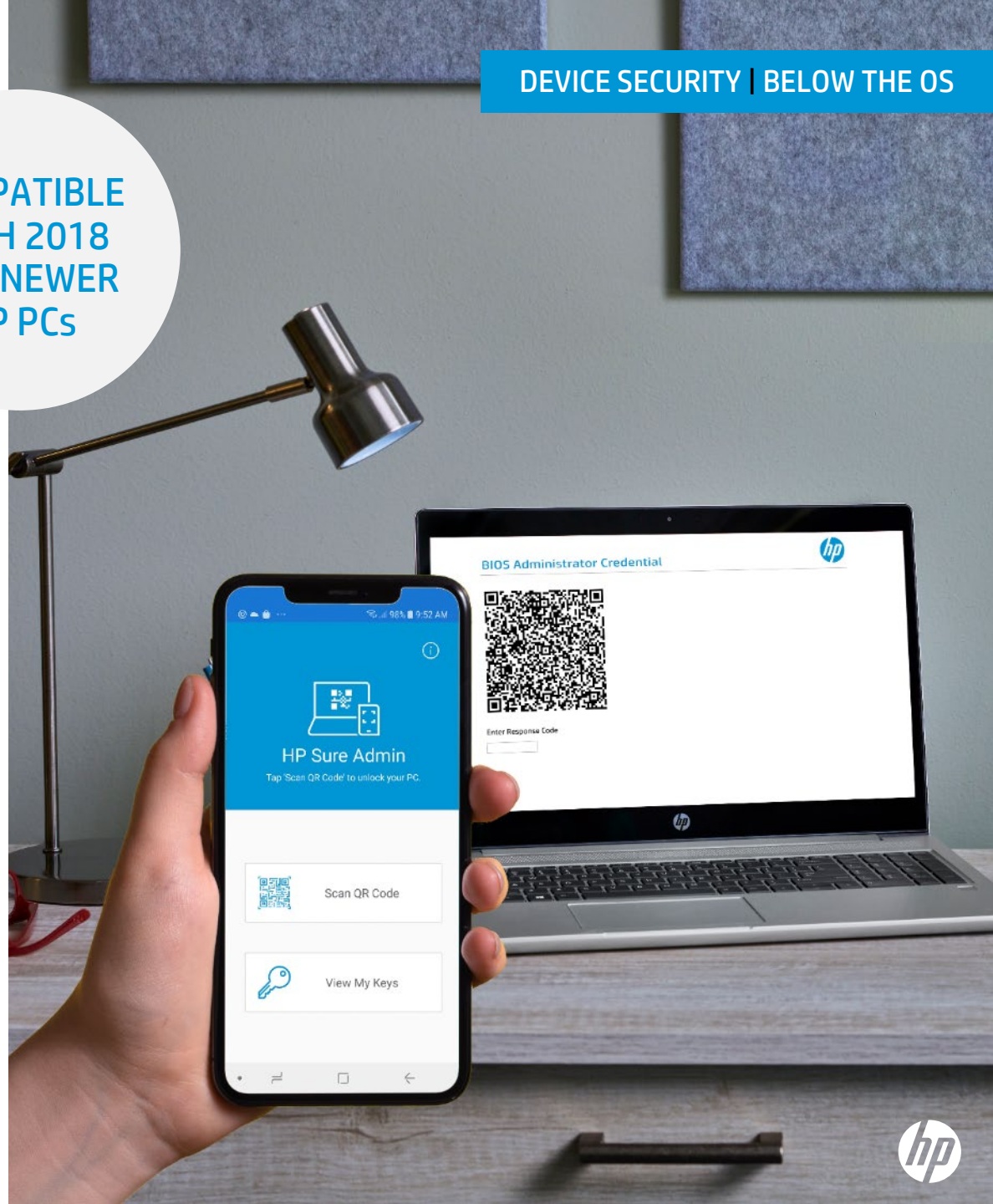
Gain local access to firmware setup using One-Time-Passcodes provided by the HP Sure Admin app

REMOTE MANAGEMENT TOOLS

Remotely Manage firmware settings securely without passwords

FACTORY PROVISIONING

Optional custom service to pre-install customer keys for zero-touch management of firmware settings



HP SURE ADMIN

REMOTE MANAGEMENT

SECURELY MANAGE FIRMWARE SETTINGS REMOTELY

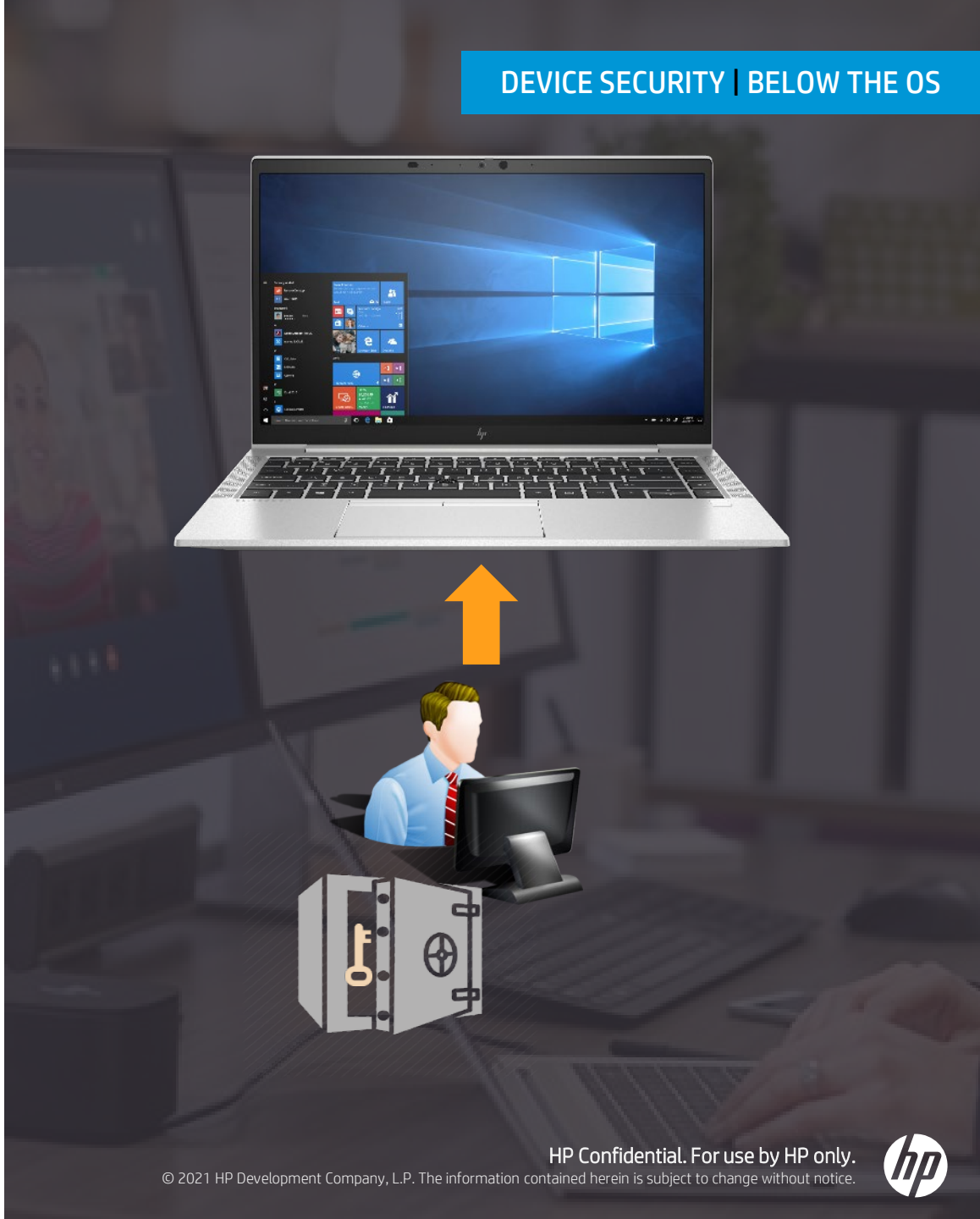
- Uses certificate based strong public key cryptography
- Authorization secret never revealed
- No password required

SUPPORTED BY FAMILAR HP BIOS MANAGEMENT TOOLS

- HP Management Integration Kit plugin for Microsoft SCCM
- HP BIOS Configuration Utility
- HP Client Management Script Library support

FACTORY PROVISIONING FOR SIMPLIFIED DEPLOYMENT

- Optional service to provision customer public keys
- Enables Zero-touch management of BIOS settings



HP SURE ADMIN

LOCAL BIOS SETUP ACCESS

GAIN ACCESS TO BIOS SETUP W/O PASSWORDS

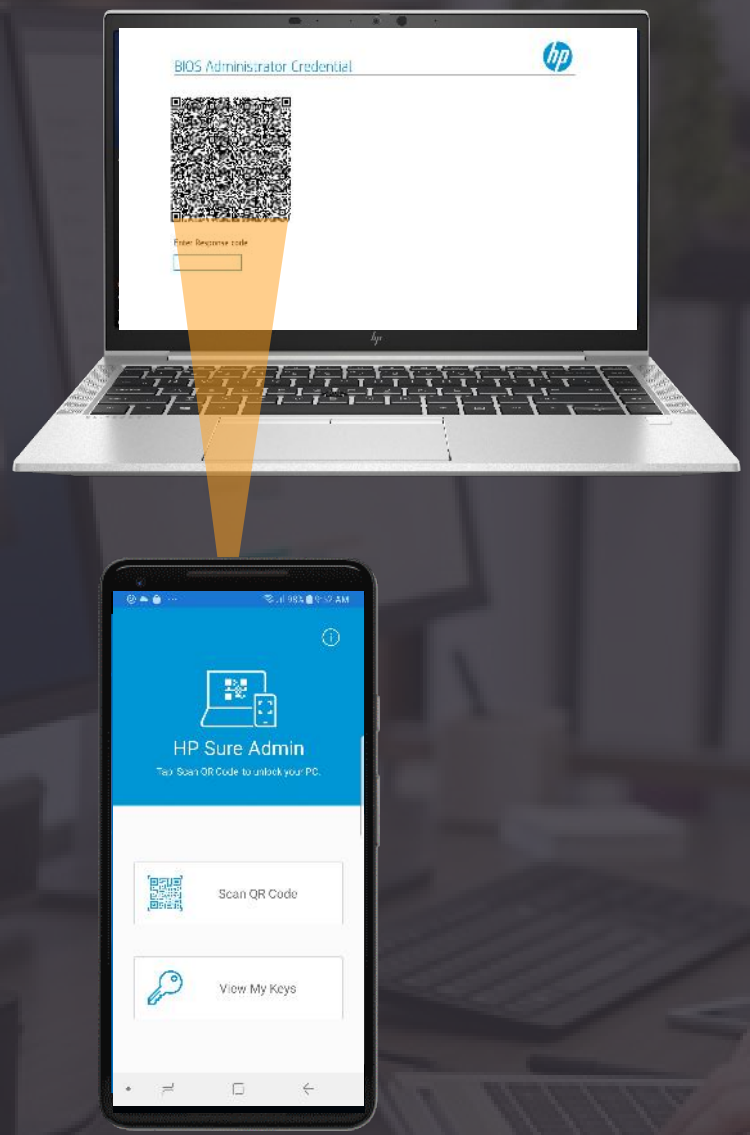
- Via HP Sure Admin Local Access Authenticator
- Decrypts QR-code challenges to obtain one-time-PIN for access to BIOS setup

SEPARATE TRUST DOMAIN FOR LOCAL ACCESS

- Compromise of Local Access key does not compromise remote management key

SECURE FIRMWARE SETTINGS FROM THE FACTORY

- Optional service to provision customer public keys
- BIOS setting protected from point of leaving HP factory.



Video

HOW HP BUILDS THE

WORLD'S MOST SECURE AND MANAGEABLE PCs

2017	2018	2019	2020	2021
				HP WOLF SECURITY
PROTECTION BELOW, IN, AND ABOVE THE OS	**HARDWARE-ENFORCED SECURITY**	**RESILIENCE AGAINST GROWING THREATS**	**ADVANCING SECURITY FOR UNKNOWN THREATS**	**A NEW BREED OF ENDPOINT SECURITY**
• HP Sure View • HP Sure Start with Runtime Intrusion Detection • HP Multi-Factor Authenticate • HP Sure Click	• HP Endpoint Security Controller • HP Sure Run • HP Sure Recover	• Expanded Hardware Enforced Security • HP Sure Sense • HP Proactive Security	• HP Sure View Reflect • HP Pro Security Edition • HP Sure Click Enterprise • HP TamperLock for MWS	• Renaming to Wolf Security • HP Tamper lock • HP Sure Admin • Persistence in HP Sure Run