



Sikkerhed & Cybertruster

FACE THE FUTURE

WITH

CONFIDENCE

HP PCs ARE DESIGNED FOR RESILIENCE AGAINST THE ATTACKS
OF TOMORROW

Ric Jakobsen

AG EN DA



- 01 State of Cyber Security
- 02 Layers Of Protection
- 03 Resilient Hardware
- 04 Proactive Management
- 05 HP Security Stack Overview
- 06 Conclusion

AG EN DA

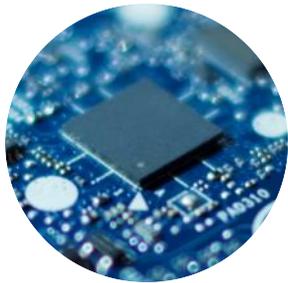


01 State of Cyber Security

- What is resilience?
- HP Unique Hardware

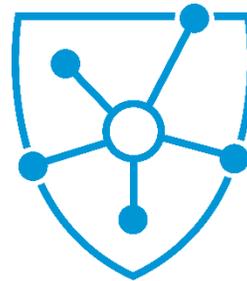
TODAY:

CAPTURING HP'S UNFAIR ADVANTAGE WITH UNIQUE SECURITY FEATURES



HP PC SECURITY 2020

WORLD'S MOST SECURE,
MANAGABLE, and RESILIENT PCs⁷



HP SURE SENSE⁸

DEEP LEARNING AI
MALWARE DEFENSE



HP DaaS

PROACTIVE SECURITY

SECURITY AT SCALE

IN 2020, ITDMs FACE 3 MAIN TRENDS

7.2 Billion Malware Attacks, 151.9 Million Ransomware Attacks in the first 3 qtrs. of 2019²⁶



RISE OF
DESTRUCTIVE
ATTACKS

IN 2020, ITDMs FACE 3 MAIN TRENDS

LOJAX

BIOS-level attack
discovered in 2018....
And still alive

Over 600,000 devices' firmware
captured by Mirai botnet²⁵



INCREASE IN
FIRMWARE
ATTACKS

September 27, 2018

The lowdown on LoJax: Researchers detect a UEFI rootkit in the wild

Bradley Barth Senior Reporter
[Follow @bbb1216bbb](#)

SC Media [link](#)

Malware News

Beware this malware: it can even survive operating systems being reinstalled

November 2, 2018

Panda Security [link](#)

IN 2020, ITDMs FACE 3 MAIN TRENDS

Over 350,000 New Malware Variants
Every Day²⁷



RAPID
EVOLUTION
OF MALWARE

WORLD'S MOST SECURE AND MANAGEABLE PCs¹²

2017



PROTECTION BELOW, IN, AND ABOVE THE OS

- HP Sure View¹⁶
- HP Sure Start with Runtime Intrusion Detection¹
- HP Multi-Factor Authenticate^{10,37}
- HP Sure Click⁵

2018



HARDWARE-ENFORCED SECURITY

- HP Endpoint Security Controller
- HP Sure Run²
- HP Sure Recover³

2019



RESILIENCE AGAINST GROWING THREATS

- Expanded Hardware Enforced Security
- HP Sure Sense⁷
- HP Proactive Security²⁴

2020



ADVANCING SECURITY FOR UNKNOWN THREATS

- HP Sure View Reflect¹⁶
- HP Pro Security Edition²³
- HP Sure Click Enterprise²⁶
- HP Sure Admin³⁵
- HP Tamper Lock³⁶

UNIQUE HARDWARE - UNMATCHED PROTECTION



HP SURE START¹

The world's first
SELF-HEALING BIOS
Others can detect, but HP Sure Start can **RECOVER!**



HP SURE RUN²

Built-in
HARDWARE-ENFORCED RUNTIME PERSISTENCE
for your PC's key security processes



HP SURE RECOVER³

SECURE AND AUTOMATED RECOVERY
on the world's first and only PCs with a firmware-embedded self-healing system image²⁸



HP SURE CLICK⁴

SECURE WEB BROWSING
to protect against most common attack methods and attachment viewing



HP SURE VIEW⁵

INTEGRATED PRIVACY SCREEN⁶

HARDWARE-ENFORCED RESILIENCE AGAINST...

BIOS Rootkits
like
LoJax

Viruses that take down OS
defenses like
H1N1

Wiper attacks
like
NotPetya

Web-borne or Office
malware like
WannaCry

Shoulder surfing
and
Visual Hacking

WHAT IS RESILIENCE?

EVERY ORGANIZATION SHOULD HAVE
A PLAN FOR
RESILIENCE



RESILIENCE:

PROTECT + DETECT + RECOVER



THERE ARE

400M PCs

GREATER THAN 4 YEARS
OLD THAT ARE
VULNERABLE

OUTDATED OS security, **INADEQUATE** for today's threat
landscape

NO BIOS protection from persistent, stealthy malware

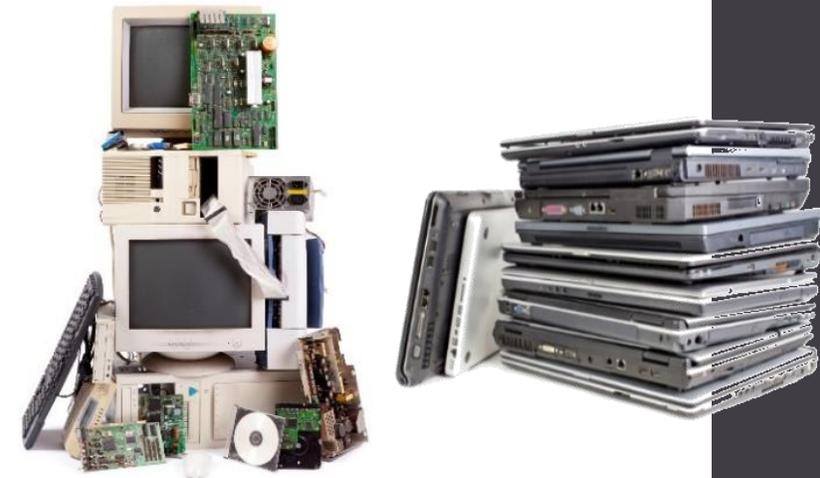
VULNERABLE to visual hacking

NO security policy enforcement

WEAK and **VULNERABLE** password protection

NO automated recovery

NO RESILIENCE





PROACTIVE MANAGEMENT

Enforce security policies and actively monitor and respond to malicious activity



RESILIENT HARDWARE

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



HOW HP CREATES THE WORLD'S MOST SECURE AND MANAGEABLE PCs⁷

HP & INTEL's Security Leadership

HP Elite PCs

The world's most
secure and
manageable PCs¹

COMPREHENSIVE SECURITY STACK

Securing below, in, and above the OS

BUILT-IN NOT BOLTED ON

Security out of the box

SECURITY THAT IS MANAGEABLE

Managed Security Policies and Deployment across Endpoint Devices

WITH WORLD'S FIRST INNOVATIONS

Self-healing BIOS with Run-time Protection

Self-healing Intel ME Protection

Integrated Privacy Screen

Self-healing re-imaging

Who Wants to Play?

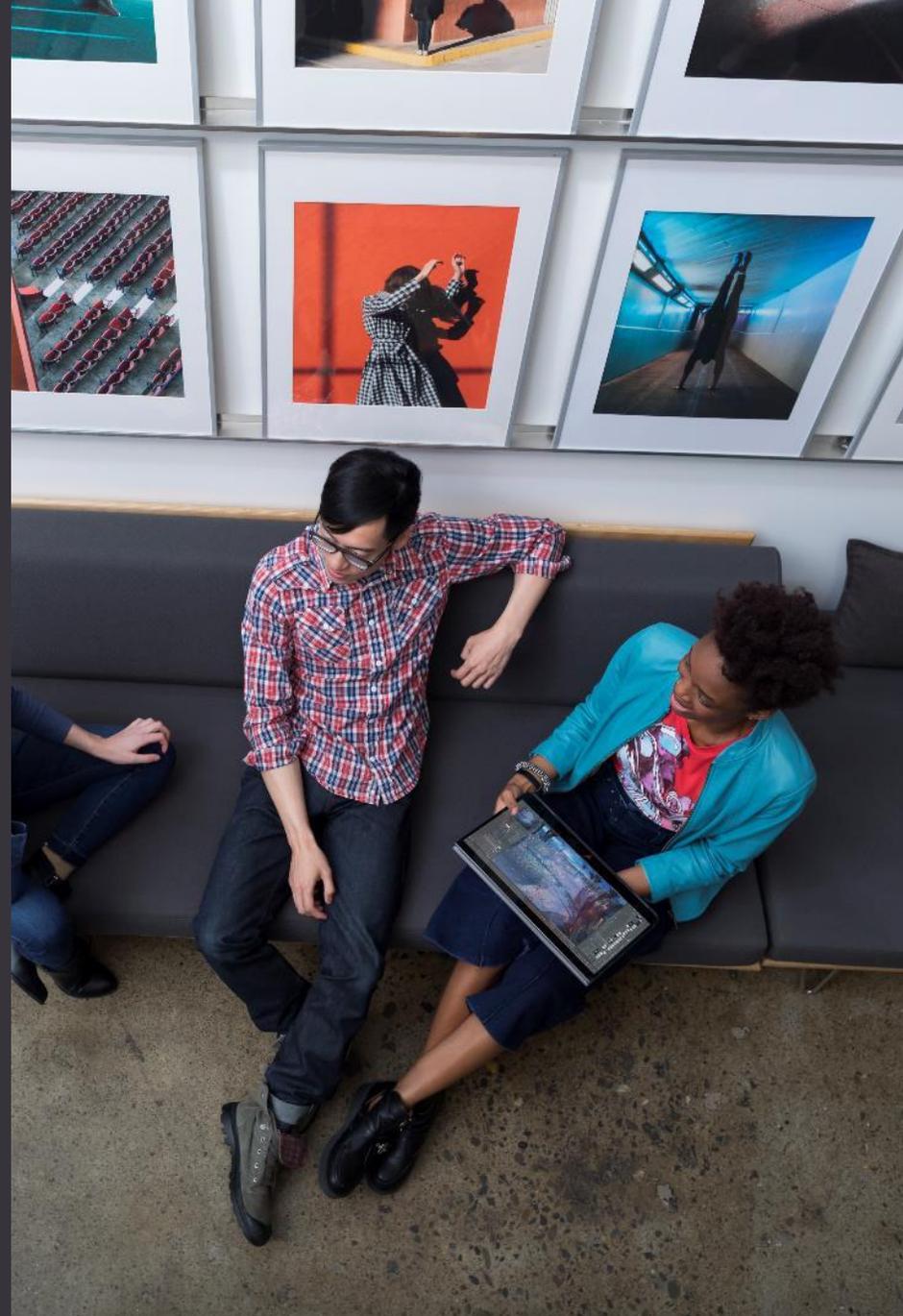


AG EN DA



- 01 State of Cyber Security
- 02 Layers Of Protection
- 03 Resilient Hardware
- 04 Proactive Management
- 05 HP Security Stack Overview
- 06 Conclusion

AG EN DA



02 Layers Of Protection

- HP Sure View
- HP Multi-Factor Authenticate
- HP Sure Click
- HP Sure Sense





PROACTIVE MANAGEMENT

Enforce security policies and actively monitor and respond to malicious activity



RESILIENT HARDWARE

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

- HP Sure Start¹
- HP Sure Run²
- HP Sure Recover³



LAYERS OF PROTECTION

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

- HP Sure View¹²
- HP Multi-Factor Authenticate¹¹
- HP Sure Click⁴
- HP Sure Sense⁸



3RD & 4TH GENERATION INTEGRATED PRIVACY

FOR THE MOBILE WORKER AND THE OPEN OFFICE



AiO 800 G4



HP EliteBook x360
1030/1040 G7



HP EliteDisplay E243p

HP Sure View Gen1

- ✓ World's First integrated privacy screen³

HP Sure View Gen2

- ✓ Better performance in light and dark environments
- ✓ Improved privacy protection
- ✓ Flexibility for thinner designs

HP SURE VIEW Gen 3²

- ✓ Improved battery life over Gen2
- ✓ Better Visuals

HP SURE VIEW REFLECT

- ✓ Improved visuals in bright environments vs Gen3
- ✓ Improved image clarity vs Gen3
- ✓ Same exceptional privacy



PROTECT YOUR IDENTITY WITH ADVANCED BIOMETRICS

90% of data breached by phishing are
credentials¹⁶

Protect your identity with the hardened policies
and manageable protection of
HP Multi-Factor Authenticate Gen3⁵

- UP TO 3 SIMULTANEOUS FACTORS
- THROUGH MIK & CLIENT SECURITY MANAGER
- HARDENED FACTORS AND POLICIES

A photograph of two men in a workshop or office setting. The man on the left is wearing a blue denim shirt and has a beard. The man on the right is wearing a blue and white plaid shirt. They are both looking at a laptop screen, which is partially visible on the left side of the frame. The background is slightly blurred, showing what appears to be a desk and some equipment.

WHAT is « HARDENING »?

PLATFORM SECURITY “HARDENING” BY INTEL

Hardening

Is security & privacy protection starting in the HARDWARE

...

below the operating system beyond the reach of software attacks

HARDWARE-BASED SECURITY CHANGES THE GAME

1



Numeric keypad Fingerprint Bluetooth

Authentication

2



IT Policy management

3



Data & certificate mgt

JET TRAINING



The easiest way to attack your organisation:

INSECURE BROWSERS and MALICIOUS OFFICE FILES



1 IN 10
WEB REQUESTS LEAD TO
TO MALWARE¹²



USERS RECEIVE AN AVERAGE OF
16
MALEVOLENT EMAILS
PER MONTH²

56%
2018 INCREASE OF ENDPOINT
WEB ATTACKS¹³



HP SURE CLICK⁴: CLICK WITH CONFIDENCE

Open attachments and work online with HP Sure Click⁴



PROTECT AGAINST MALICIOUS WEBSITES

- ✓ Isolates each tab in a secure virtual container
- ✓ Just close the tab, and the malware is gone
- ✓ Easy to use: integrates with IE and Chrome



PROTECT AGAINST BAD ATTACHMENTS

- ✓ Infected files are a common attack vector
- ✓ Protection for Word, Office, Excel and PDF files viewed in read only mode



HP SURE SENSE

HARNESSING
DEEP LEARNING AI
FOR REAL-TIME PREVENTION OF
NEVER BEFORE SEEN
MALWARE⁸



OVER

350,000

NEW PIECES OF MACHINE
GENERATED MALWARE
EVERY DAY¹⁵

HACKERS USE

ARTIFICIAL
INTELLIGENCE

TO DESIGN MORE
SOPHISTICATED ATTACKS

ZERO-DAY ATTACKS ARE

4X

MORE LIKELY TO
COMPROMISE
ORGANIZATIONS¹⁶

LEGACY PROTECTION

CANNOT CATCH ZERO-DAY ATTACKS

15. AV-Test Institute, <https://www.av-test.org>

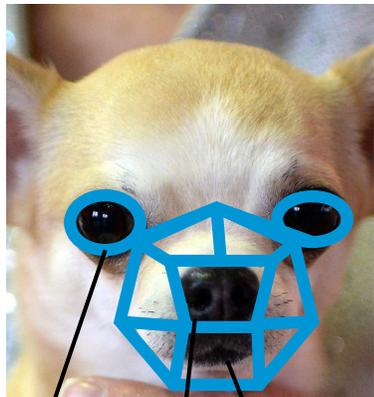
16. Barkly and Ponemon Institute 2018 State of Endpoint Security Risk Report, 2018

A photograph of two men in a workshop or office setting. The man on the left is wearing a blue denim shirt and has a beard. The man on the right is wearing a blue and white plaid shirt. They are both looking at a laptop screen, which is partially visible on the left side of the frame. The background is slightly blurred, showing what appears to be a desk and some equipment.

WHAT IS DEEP LEARNING?

DOG OR MUFFIN?

Machine Learning



Eyes = Round
Nose = Elliptic
Mouth = Triangular

Blueberry = round
Chocolate = transparent
Crack = Linear

Deep Learning



DOG

MUFFIN

DOG OR MUFFIN?





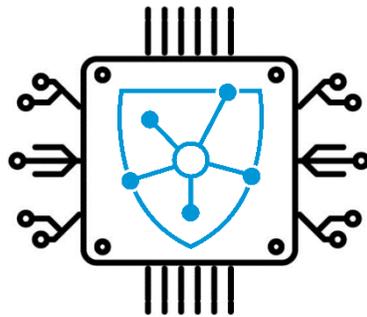
CREATING HP SURE SENSE⁸

FROM TERABYTES OF INSIGHTS TO MEGABYTES OF INSTINCT



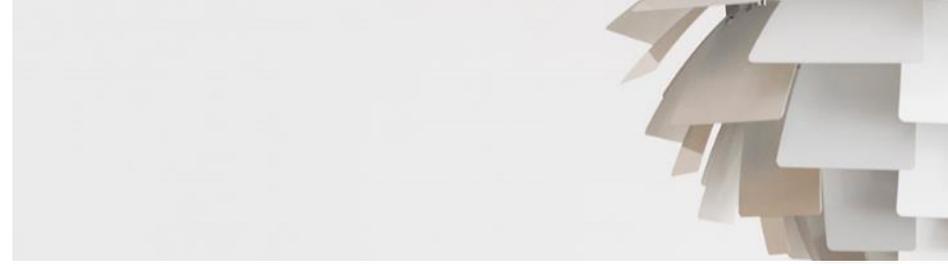
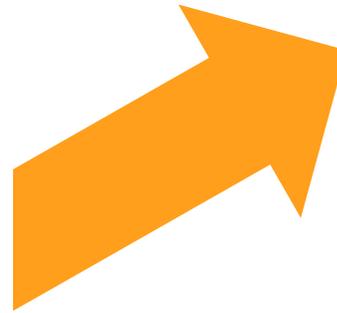
TRAIN THE BRAIN

Deep learning neural network trained on **HUNDREDS OF MILLIONS** of malware samples



CREATE THE AGENT

Brain distilled into the lightweight agent, turning Terabytes of learning into Megabytes of instinct.



PROTECT THE ENDPOINT

HP Sure Sense agent scans files and quarantines likely malware – with minimal performance impact or need for updates.





REINVENTING ENDPOINT PROTECTION

DEEP LEARNING IN ACTION

>99%
EFFECTIVE¹⁷

<20ms
AVG TIME TO DETECTION¹⁸

1%
CPU LOAD¹⁹



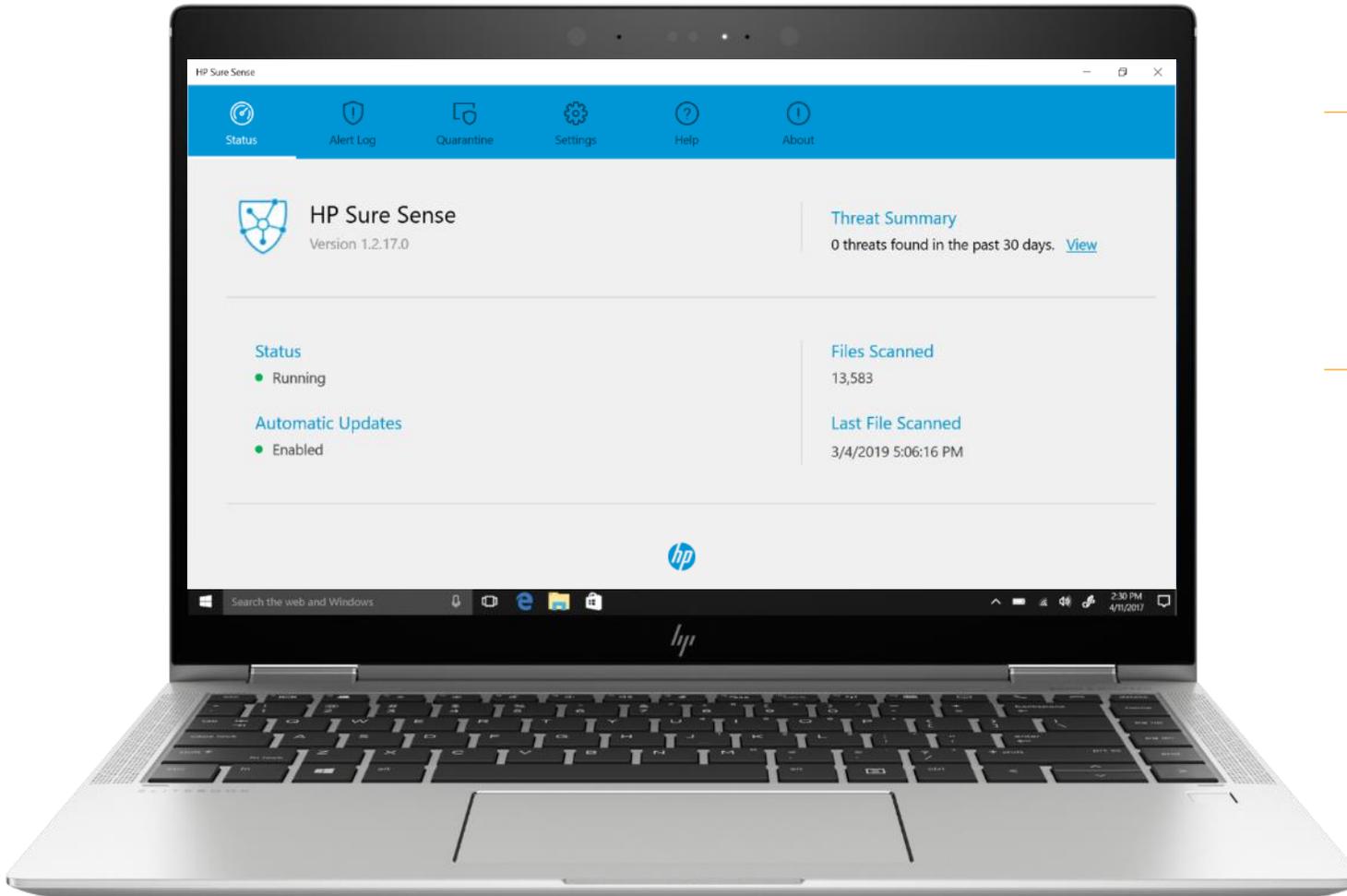
HP SURE SENSE⁸

HARNESS THE POWER OF DEEP LEARNING

Protect against **never before seen**
attacks before they happen

Minimal performance impact

Works **online or offline**, with minimal updates

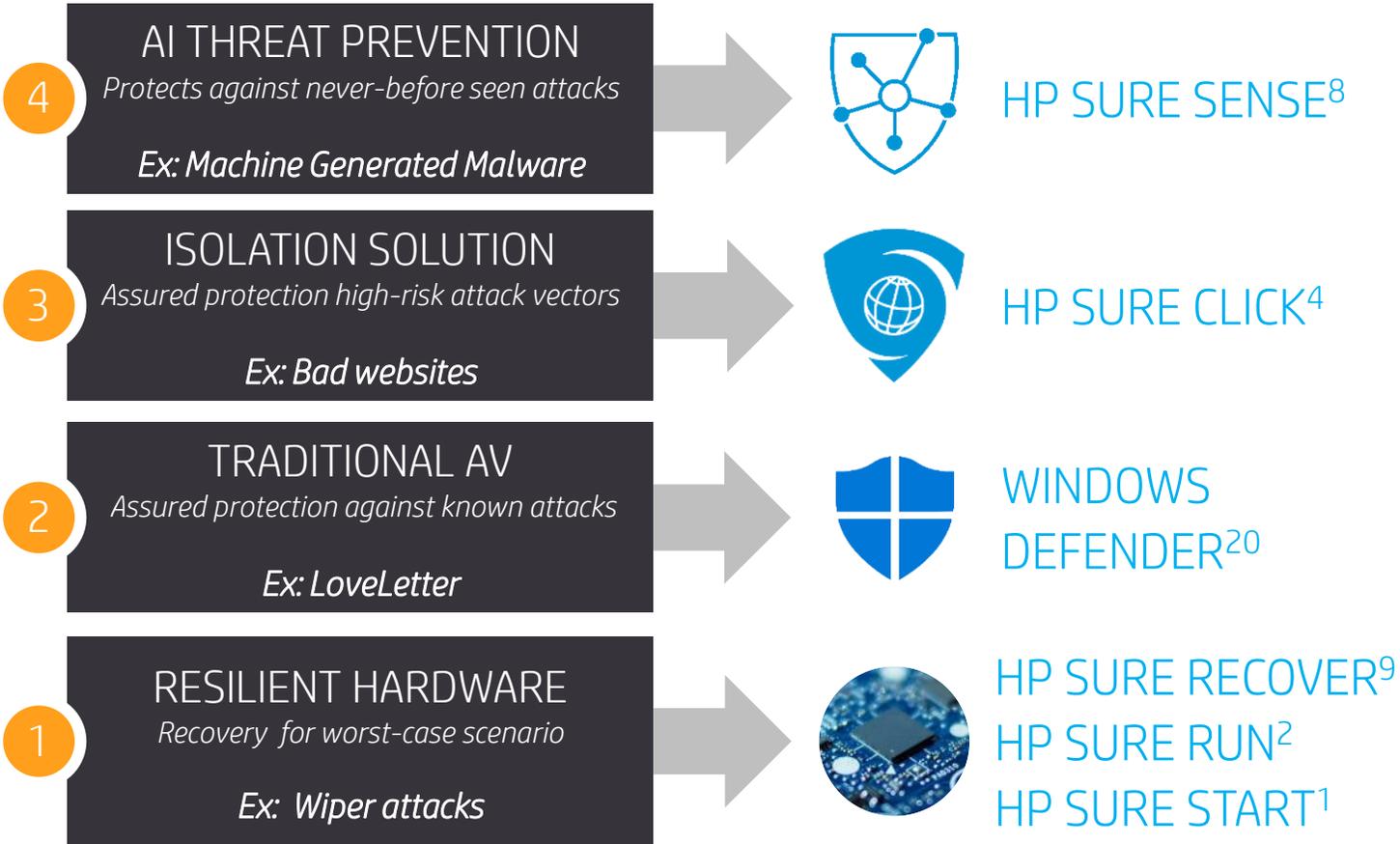


LAYERS OF PROTECTION

FOR ENDPOINT RESILIENCE

EVERY COMPANY NEEDS:

HP DELIVERS:



AG EN DA



- 01 State of Cyber Security
- 02 Layers Of Protection
- 03 Resilient Hardware
- 04 Proactive Management
- 05 HP Security Stack Overview
- 06 Conclusion

AG EN DA



03 Resilient Hardware

- HP Sure Start
- HP Sure Run
- HP Sure Recover





PROACTIVE MANAGEMENT

Enforce security policies and actively monitor and respond to malicious activity



RESILIENT HARDWARE

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

- HP Sure Start¹
- HP Sure Run²
- HP Sure Recover³



LAYERS OF PROTECTION

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

- HP Sure View¹²
- HP Multi-Factor Authenticate¹¹
- HP Sure Click⁴
- HP Sure Sense⁸



HOW LONG WOULD IT TAKE YOU TO RECOVER 1000 PCs?



HP ENDPOINT SECURITY CONTROLLER

UNIQUE HARDWARE ENABLES RESILIENT DEVICES

- ✓ Physically isolated
- ✓ Cryptographically secured



3RD PARTY CERTIFIED

by an accredited independent test lab
(Overseen by ANSSI)



HP Sure Start¹



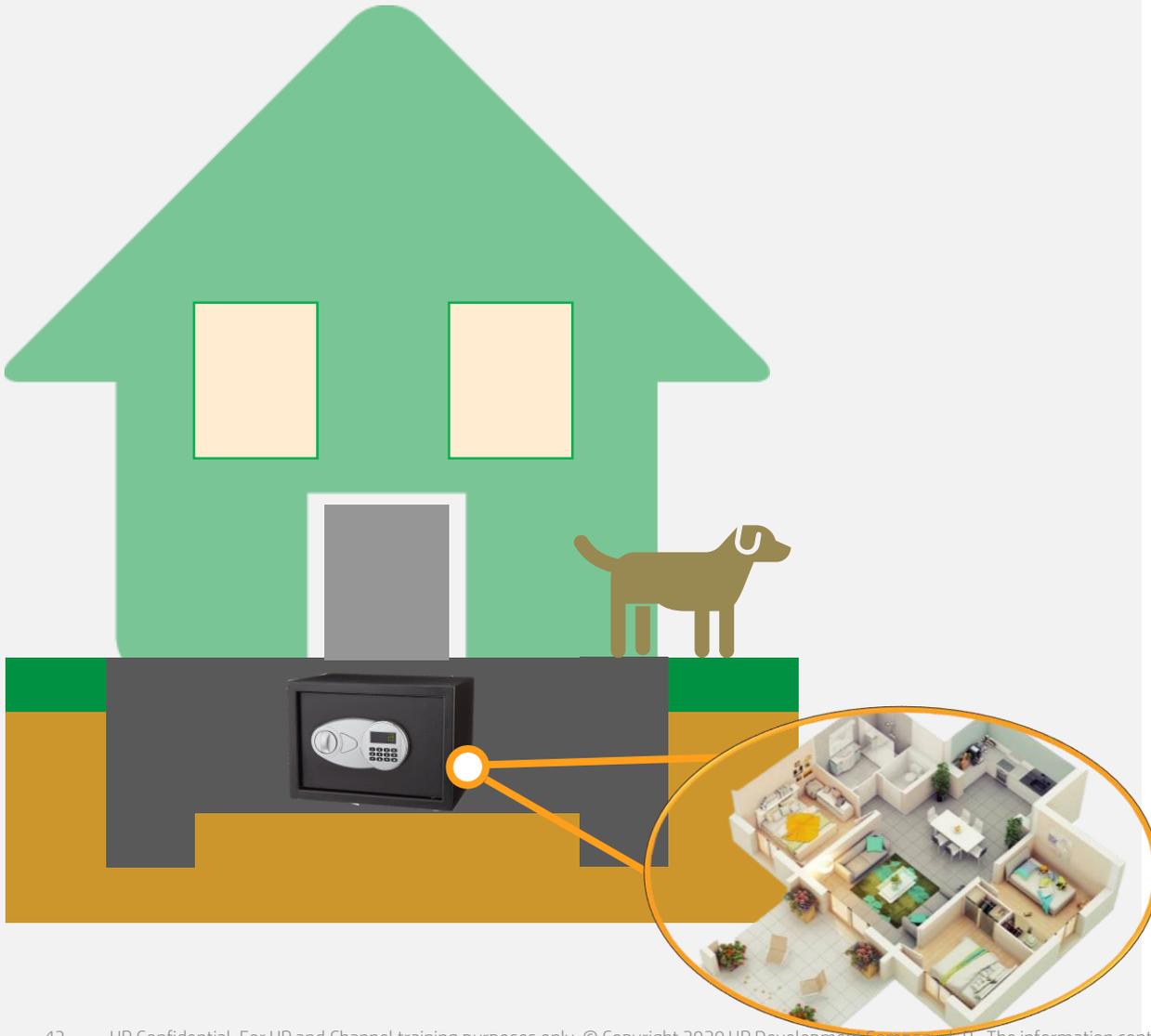
HP Sure Run²



HP Sure Recover³

KEEPING IMPORTANT INFORMATION SECURELY PROTECTED

TO ENABLE RECOVERY WHEN SOMETHING BAD HAPPENS

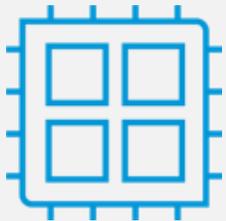




HP SURE START IS THE WORLD'S ONLY SELF-HEALING BIOS

OTHERS MAY PROTECT OR EVEN
DETECT ATTACKS ON THE BIOS.

HP SURE START CAN **RECOVER**
FROM THEM.



HP Sure Start Gen5¹ expands the self-healing protection of HP Sure Start to the **Intel Management Engine (ME)**



3RD PARTY CERTIFIED

by an accredited independent test lab
(Overseen by ANSSI)



HP UNIQUE ADVANTAGE: N.I.S.T. STANDARDS



2011:
BIOS PROTECTIONS
NIST SP 800-147



2019:
FIRMWARE RESILIENCE
NIST SP 800-193

UNIQUE!

HP SURE START GEN5¹
**MEETS AND
EXCEEDS**
NIST SP 800-193
FOR ALL CORE EMBEDDED
PLATFORM FIRMWARE



LEARN MORE:
Details in the HP Sure
Start Whitepaper
**See HP Sure Start
whitepaper for details.*

HP SURE RUN² KEEPS YOUR PCs SECURITY POSTURE STRONG

FIGHTS BACK AGAINST ATTACKERS BY:

- **MONITORING** KEY PROCESSES
- **ALERTING** YOU OF CHANGES
- **RESTARTING** PROCESSES AUTOMATICALLY IF THEY'RE STOPPED



Sure Run Gen2² includes **NETWORK ISOLATION** to quarantine noncompliant machines and prevent the spread of malware





HP SURE RECOVER: SECURE, AND AUTOMATED RECOVERY FROM DESTRUCTIVE MALWARE

HP SURE RECOVER WITH
EMBEDDED REIMAGING³

RECOVER YOUR OS IN
AS LITTLE AS **5 MINUTES**⁶

HP Sure Recover Gen2⁹ offers:

- ✓ Easier set up of custom images
- ✓ Better network reliability
- ✓ Better event logging
- ✓ Intel® Optane™ compatibility

HP TAMPER

LOCK³⁶

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, and **rich policy controls** to configure what action is taken if this has occurred.
- Other physical attack protections, such as **DMA attack protection** and protected storage via the **HP Endpoint Security Controller** hardware.

Attacks previously available only to nation states/highly skilled attackers are becoming democratized and readily available via open source.

FLASH
REPLACEMENT
ATTACKS

SIDE
CHANNEL
ATTACKS

MEMORY
PROBING (DMA)
ATTACKS

TPM
PROBING
ATTACKS

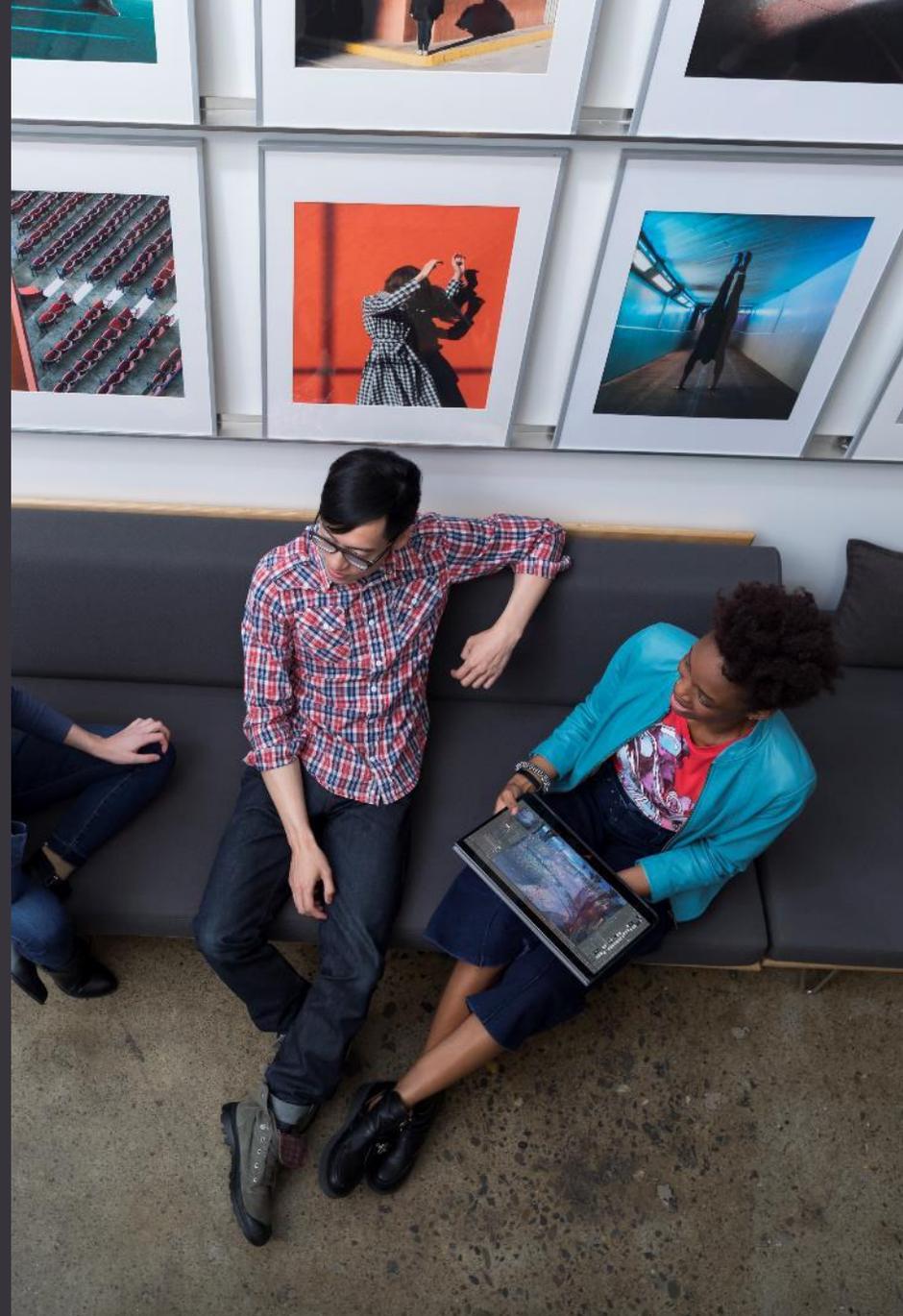
Tamper Lock is available on select Mobile Workstations, and more platforms in 2021

AG EN DA



- 01 State of Cyber Security
- 02 Layers Of Protection
- 03 Resilient Hardware
- 04 Proactive Management
- 05 HP Security Stack Overview
- 06 Conclusion

AG EN DA



04 Proactive Management

- Manageability
- Proactive Security





PROACTIVE MANAGEMENT

Enforce security policies and actively monitor and respond to malicious activity



RESILIENT HARDWARE

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

- HP Sure Start¹
- HP Sure Run²
- HP Sure Recover³



LAYERS OF PROTECTION

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

- HP Sure View¹²
- HP Multi-Factor Authenticate¹¹
- HP Sure Click⁴
- HP Sure Sense⁸



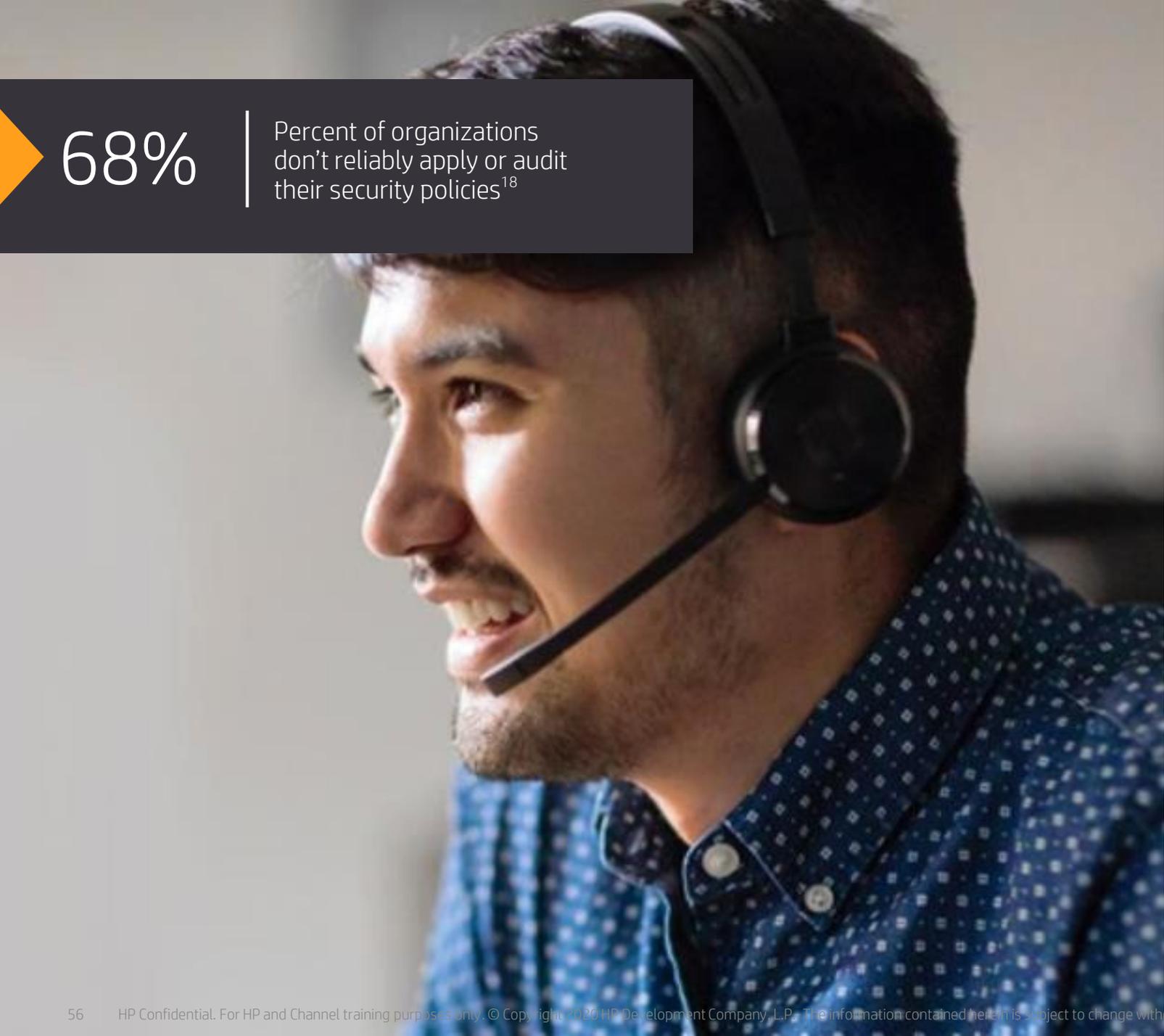
HOW DO YOU PROACTIVELY KNOW WHEN YOUR FLEET IS UNDER ATTACK?



SECURITY AT SCALE

HP services help take our customers from
secure endpoints to **secure organizations**

- ✓ Validate policies are being enforced
- ✓ See where attacks are coming from, and what they're targeting
- ✓ Monitoring and response from security experts



68%

Percent of organizations
don't reliably apply or audit
their security policies¹⁸



ENSURE YOUR SECURITY IS MANAGEABLE

Turn secure endpoints into a secure organization: HP designs all of our security features with manageability in mind

HP Manageability Integration Kit Gen2⁶ is the first and only Microsoft® certified plug in for MS SCCM (MS System Center Configuration Manager)

Now in its second generation, with support for new features, enhanced capabilities, and an updated UI

World's **most advanced isolation security service**²³ for files and browsing on **Windows 10 PCs**



HP DaaS PROACTIVE SECURITY

Extending protection and security intelligence to transform endpoints from your biggest risk to your best defense



Real-time threat protection

Advanced malware protection with isolation technology that contains zero-day e-mail, browser, and file attacks



Enhanced security intelligence

Security analytics and reporting with HP TechPulse



Proactive security management

HP managed service with cybersecurity expertise

AG EN DA



- 01 State of Cyber Security
- 02 Layers Of Protection
- 03 Resilient Hardware
- 04 Proactive Management
- 05 HP Security Stack Overview
- 06 Conclusion

AG EN DA

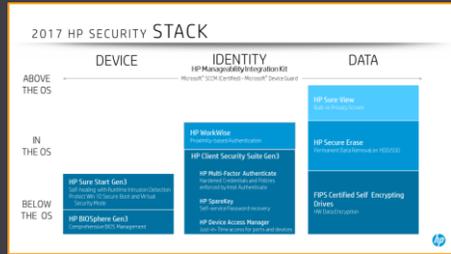


05 HP Security Stack Overview

- Security Up-Sell

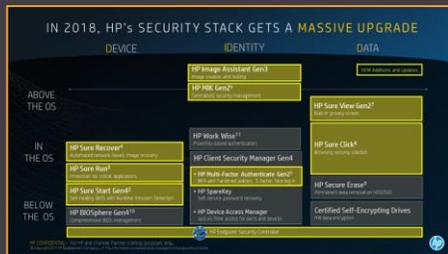
HP SECURITY STACK EVOLUTION

2017 Launch of World's Most Secure & Manageable



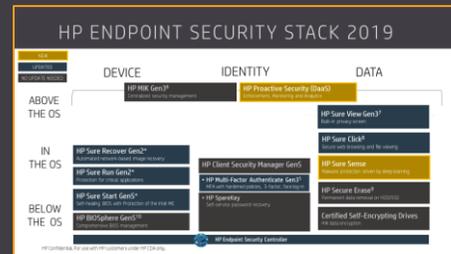
11 Solutions

2018 Massive Upgrade



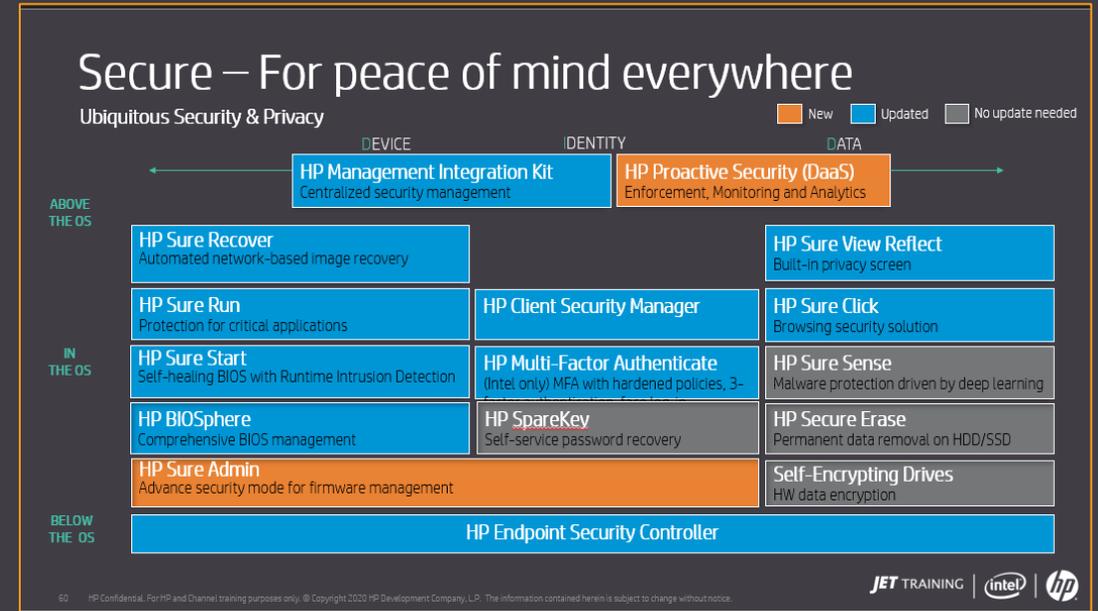
15 Solutions (4 new)

2019 Resilience, AI come to HP Security



16 Solutions (3 new, 2 End of life)

2020 Security Personalized for you and your business



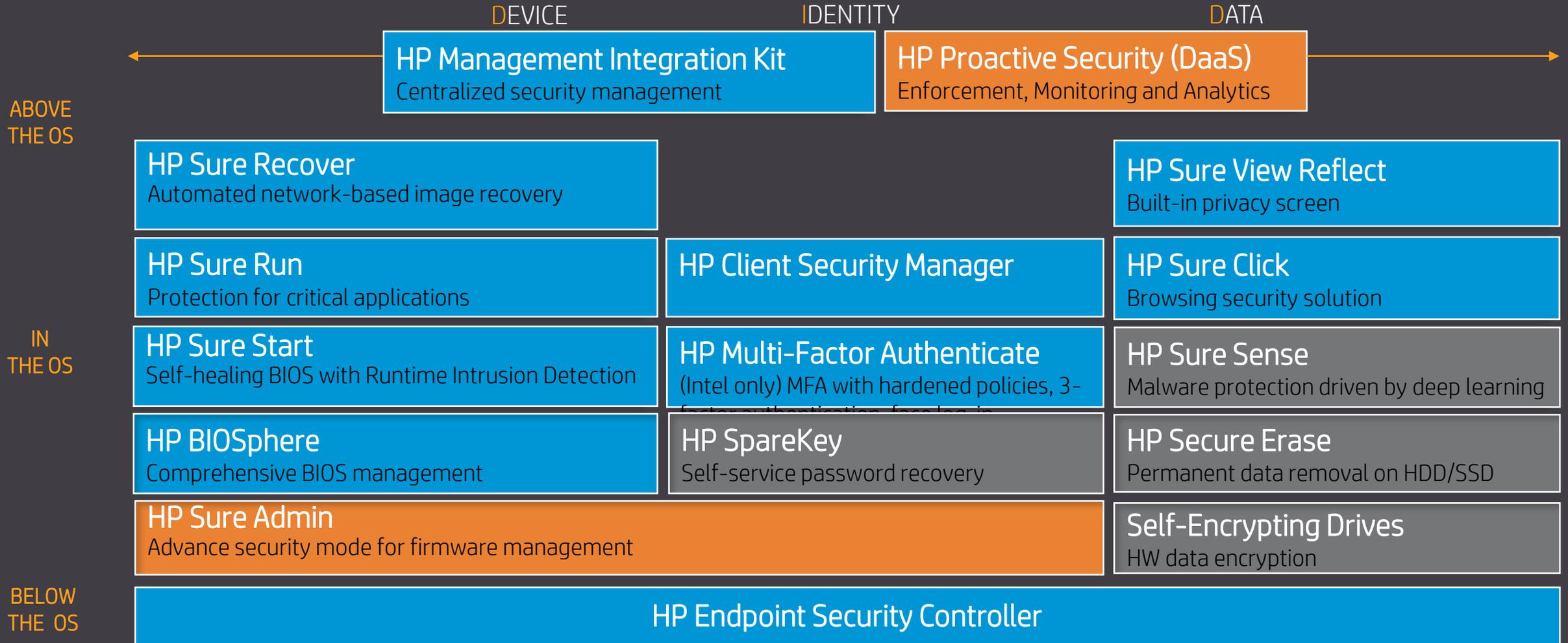
17 Solutions (2 new, 1 End of life)

Raising the Bar on Security, With Every Release

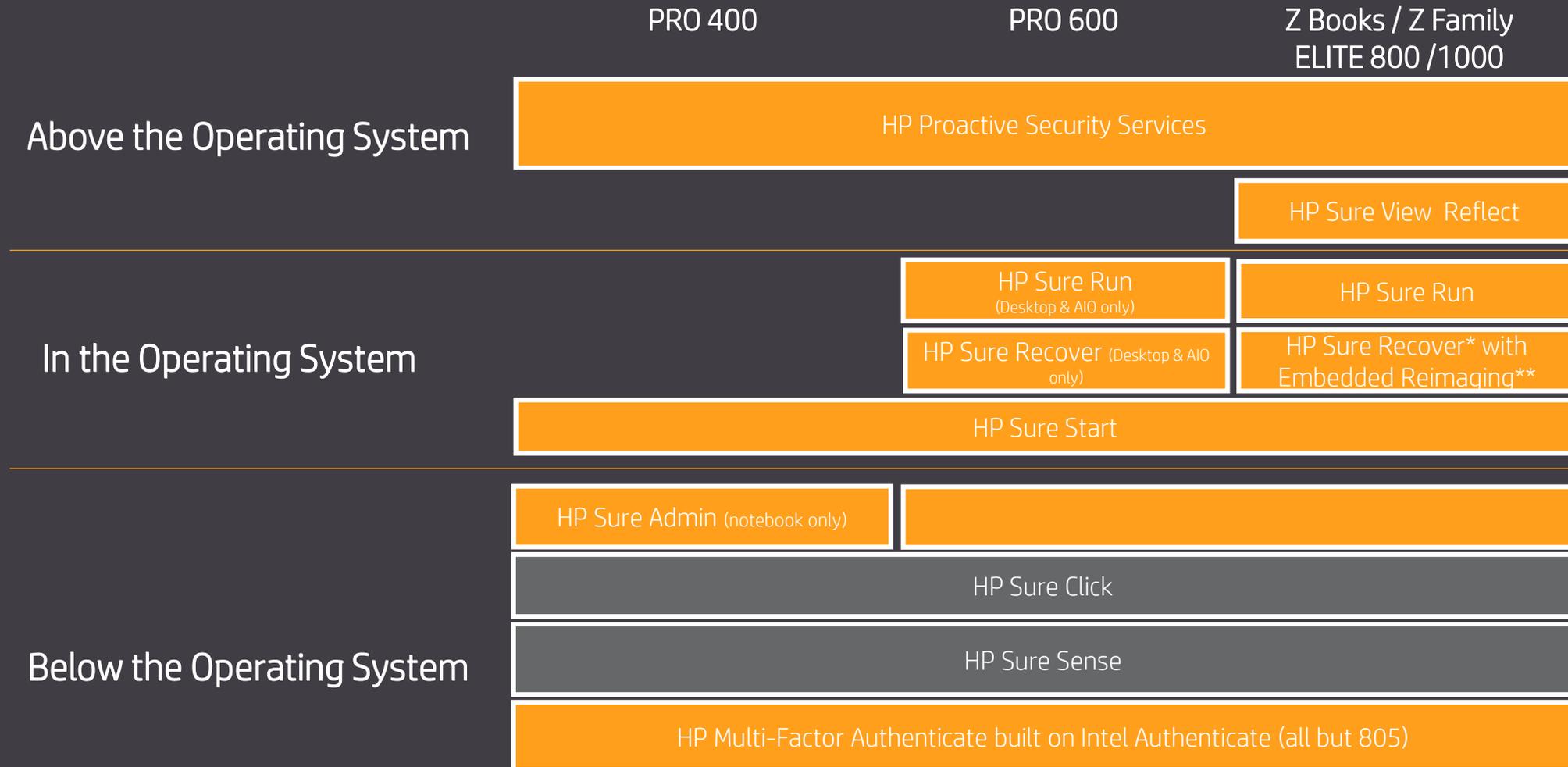
Secure – For peace of mind everywhere

Ubiquitous Security & Privacy

■ New
 ■ Updated
 ■ No update needed



HP SECURITY UPSELL PATH – 2020 Security Solutions



* HP Sure Recover Available on AMD Products

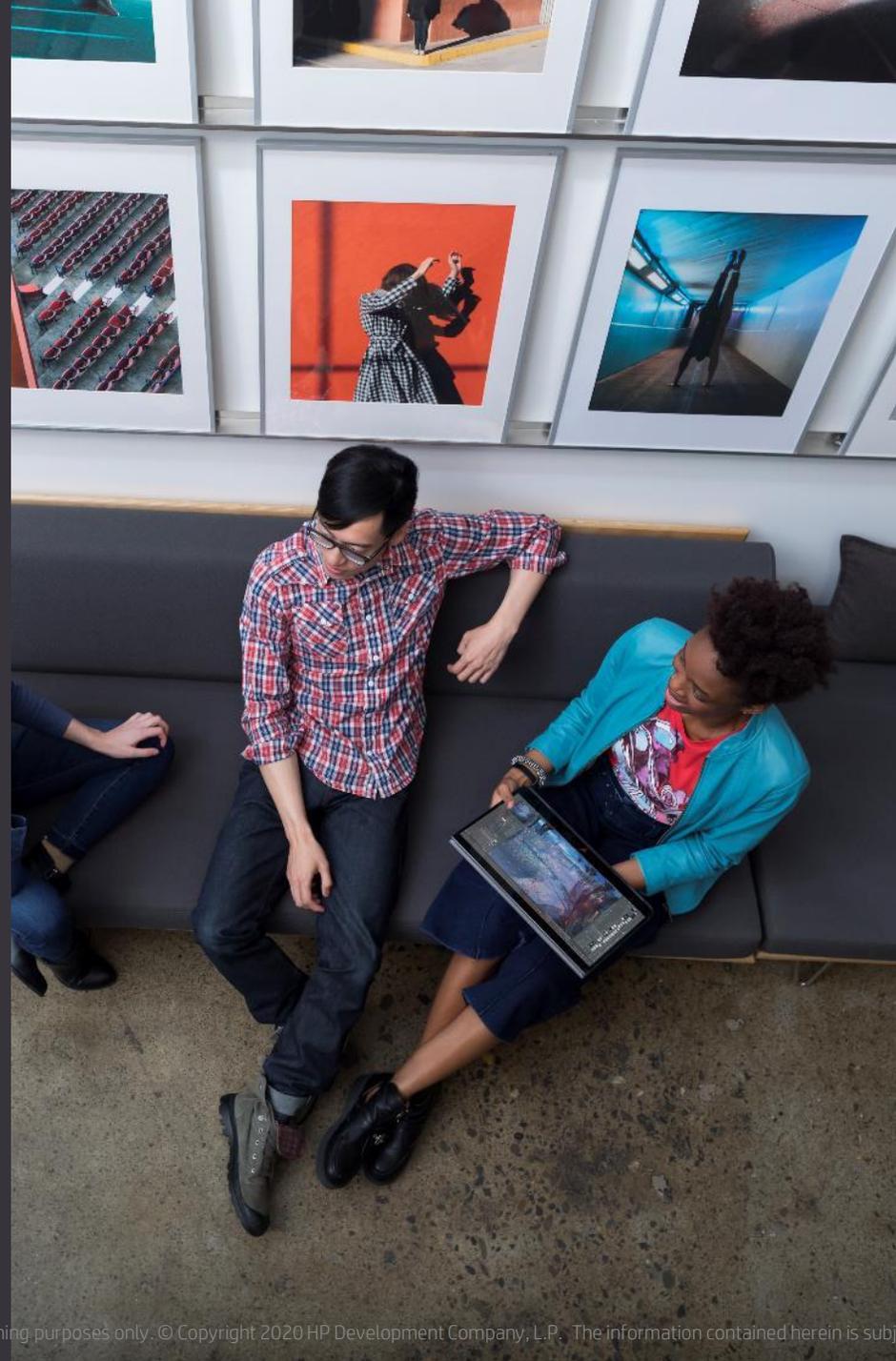
**HP Sure Recover with Embedded Reimaging only available on Intel powered products

AG EN DA



- 01 State of Cyber Security
- 02 Layers Of Protection
- 03 Resilient Hardware
- 04 Proactive Management
- 05 HP Security Stack Overview
- 06 Conclusion

AG EN DA



06 Conclusion

- Key Take-aways
- Q&A



KEY TAKE-AWAYS

1

EVERY ORGANIZATION SHOULD HAVE A PLAN FOR ENDPOINT RESILIENCY

How long would it take to recover a fleet of PCs if each BIOS is compromised and each drive wiped?

2

EVERY PC PURCHASE DECISION IS A SECURITY DECISION

Endpoints are the origins of most attacks – security must be considered for every device.

3

ENDPOINT SECURITY REQUIRES A HARDWARE ROOT OF TRUST

PCs are only as secure as their lowest level defense, which must be in hardware



EVERY PC PURCHASE IS A SECURITY DECISION





Q&A

