

Modern threats and leveraging Zero Trust principles in the World of Hybrid Work – Work Happy!

Riku Reimaa
Technical Pre-sales and Technology Evangelism
Northern Europe | Finland and the Baltics
riku@hp.com



HP WOLF SECURITY





**The way we work and learn
has changed permanently**

ECOSYSTEM INFRASTRUCTURE

FROM OFFICE BY DEFAULT TO HYBRID BY DESIGN

AT HOME

Our home is
A BIGGER PART OF OUR STORY

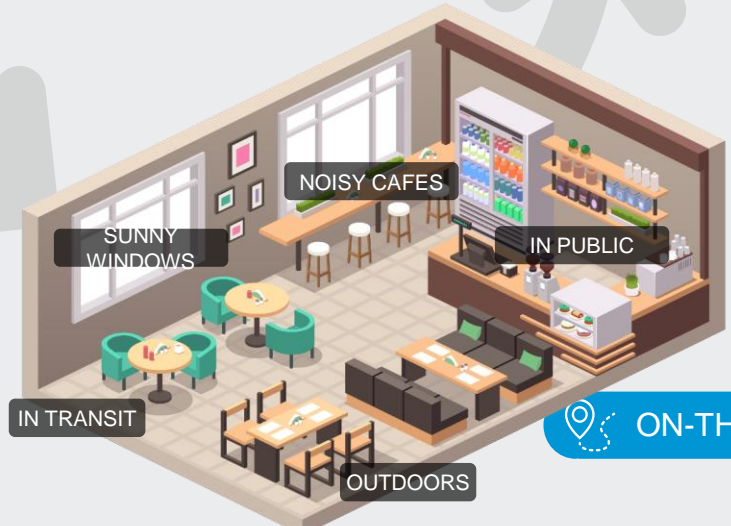


AROUND THE OFFICE

The Office shifts to a HUB for
COLLABORATION AND COMMUNITY



ON-THE-GO



HP Inc. recorded the highest average score of 29 companies measured by IDC's sustainability framework. The vendor outperformed the industry average on all three pillars. The achievement reflects HP Inc.'s commitment to the environment, employees, and social responsibility. This commitment is built into the company's business strategy.
Source: IDC Sustainability Index 2021



HP WOLF SECURITY²⁰

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

91%

of IT decision makers (ITDMs) believe endpoint security has become as important as network security, while the same say they spend more time on endpoint security now than they did two years ago.

76%

of office workers say that working from home during COVID-19 has blurred the lines between their personal and professional lives, with half saying they now see their work device as their own personal device and 46% admitting to using their work laptop for 'life admin'.

30%

of employees have let someone else use their work device, despite 85% of ITDMs saying they worry such behavior increases their company's risk of a security breach.

54%

of ITDMs say they have seen evidence of a higher number of phishing attacks in the last year, while 45% say they have seen evidence of compromised printers being used as an attack point in the past year.

HP Wolf Security Rebellions and Rejections Report Uncovers Remote Workforce Security Trends

<https://threatresearch.ext.hp.com/hp-wolf-security-rebellions-and-rejections-report/>

- 80% of IT teams experienced objections from users who do not like controls being put on them at home; 67% of IT teams said they experience complaints about this weekly.
- 83% of IT teams said trying to set and enforce corporate policies around cybersecurity is impossible now because the lines between personal and professional lives are so blurred.
- 80% of IT teams said IT security was becoming a “thankless task” because nobody listens to them.
- 69% of IT teams said they are made to feel like the “bad guys” for imposing restrictions.

Advanced security
isolation and AI Deep
technology

54%

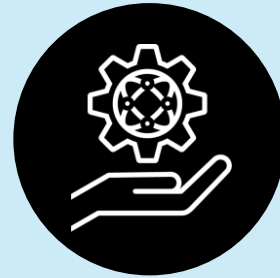
seen evidence of compromised printers being used as an attack point in the past year.

Cyber threats continue to evolve as attacks are...



More
frequent

Ransomware volume has increased
232% from 2019 to 2021¹



More
sophisticated

'Double-extortion' ransomware
damage has skyrocketed 935%²

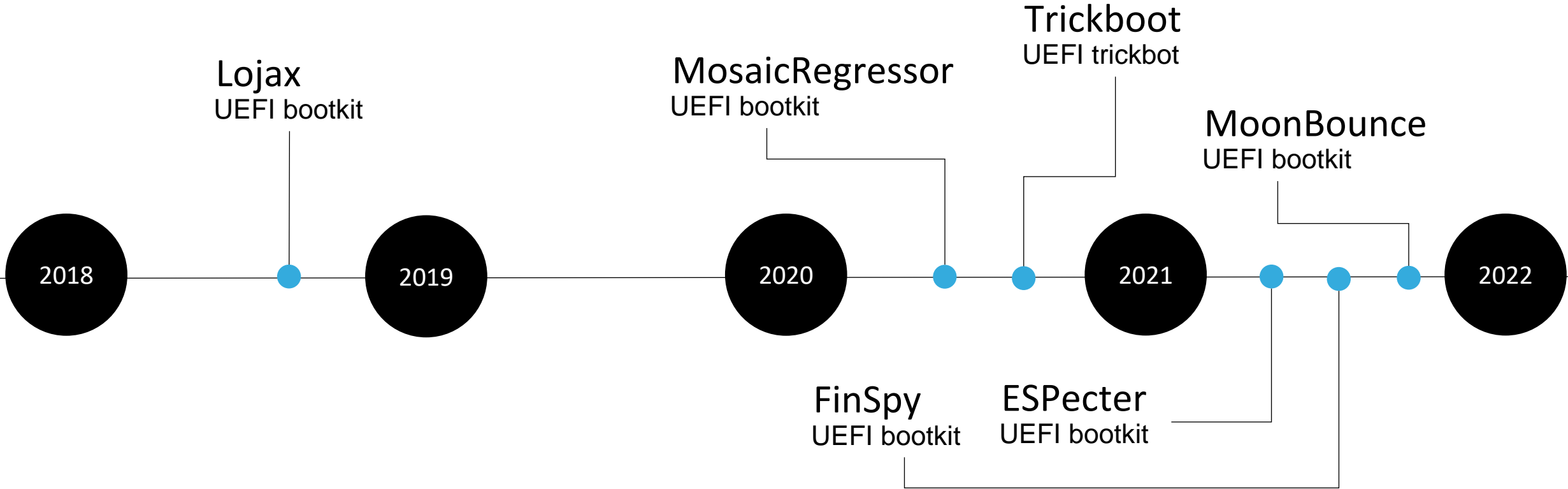


More
diverse

Supply chain, PCs, firmware, servers,
cloud, networks and identity



Attacks below the OS are on the rise



83%

Security Decision Makers experienced at least one firmware attack from 2019 to 2021³

Gas shortages worsen as fuel prices spike after Colonial Pipeline ransomware attack

BY KATE GIBSON, MEGAN CERULLO
UPDATED ON: MAY 13, 2021 / 3:17 PM / MONEYWATCH



SolarWinds Orion Security Breach: Cyberattack Timeline and Hacking Incident Details

How the SolarWinds Orion security breach occurred: A timeline involving CrowdStrike, FireEye, Microsoft, FBI, CISA & allegations vs. Russia.

by Joe Panettieri • Sep 10, 2021

The [SolarWinds Orion security breach](#), a.k.a. SUNBURST, impacted numerous U.S. government agencies, business customers and consulting firms. Here's a timeline of the SolarWinds SUNBURST hack, featuring ongoing updates from a range of security and media sources.

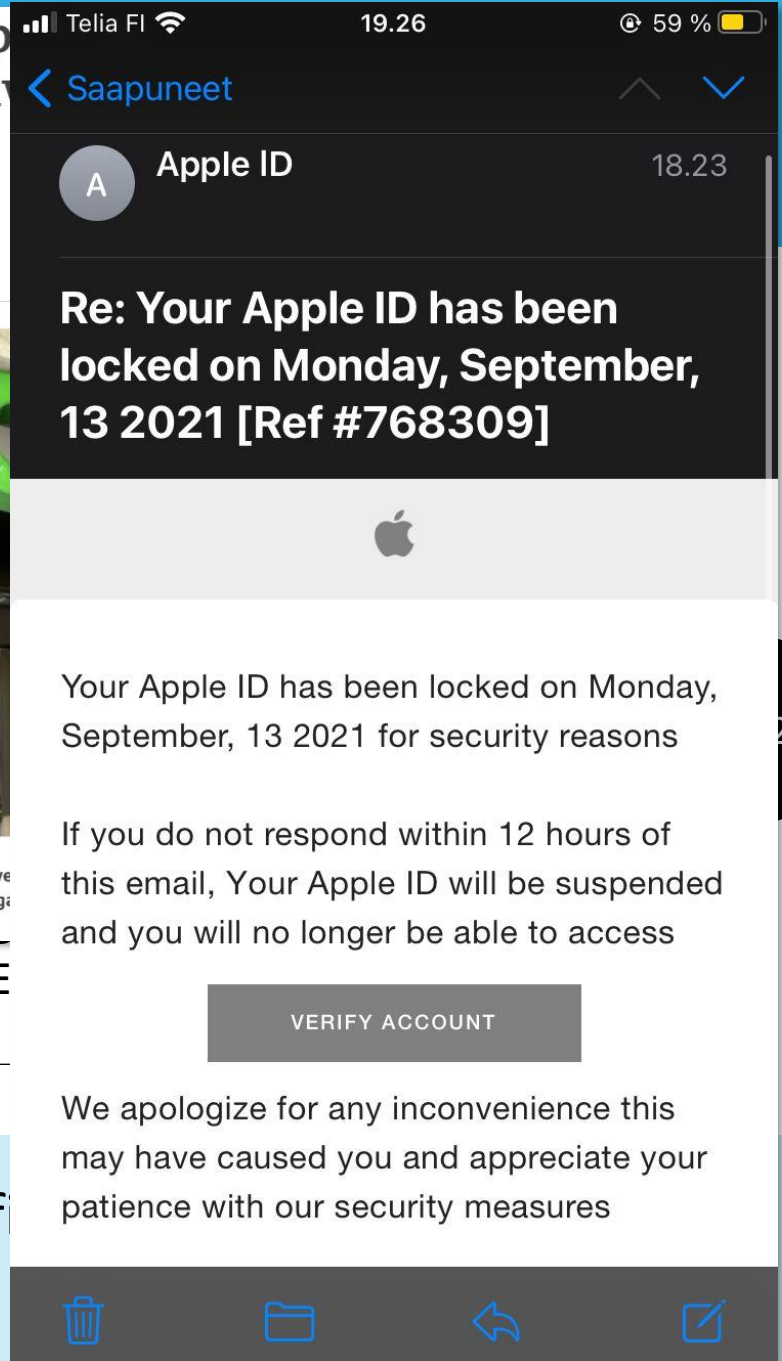
Swedish Coop supermarkets hit by ransomware due to US attack

By Joe Tidy
Cyber security reporter, BBC News

3 July



Some 500 Coop supermarket stores in Sweden have been hit by an ongoing "colossal" cyber-attack affecting organisations worldwide.





HP's CORE PRIORITIES

LEADERSHIP IN ENDPOINT SECURITY

Protecting endpoints from
DANGEROUS content **INSIDE**
the box



Protecting endpoints from
DANGEROUS content **OUTSIDE**
the box



HP WOLF SECURITY

Counteract threats with PC resilience

Why? Consider the following



Can you defend against malware unknown to the industry?



Are you able to detect attacks at every level of the stack?



What level of effort and cost will it take you to recover thousands of PCs?



Built on 20+ years of endpoint security innovation

Setting endpoint security industry standards

Established standards for TPM, BIOS, Firmware Resilience



Pioneering hardware-enforced security



Close security partnerships to drive industry state of the art (Intel®, AMD® and Microsoft®)

Strengthened security advancements with Bromium



Security is in our DNA



HP WOLF SECURITY

Advancing security beyond the industry

HP supports and extends Intel's, AMD's and Microsoft's security features to provide **differentiated, industry-leading protection**

AMD

- AMD Memory Guard
- AMD Secure Processor

intel

- Intel Hardware Shield⁹
- Intel BIOS Guard

- Microsoft Secured Core¹⁰
 - Secure Launch
 - Virtualization-Based Security for OS
 - Cloud-based recovery

- HP Sure Admin¹¹
- HP Sure Click¹²
- HP Sure Sense¹³
- HP Sure Run¹⁴
- HP Sure Start¹⁵
- HP Sure Recover¹⁶
- HP Tamper Lock¹⁷

The World's Most secure PCs⁷

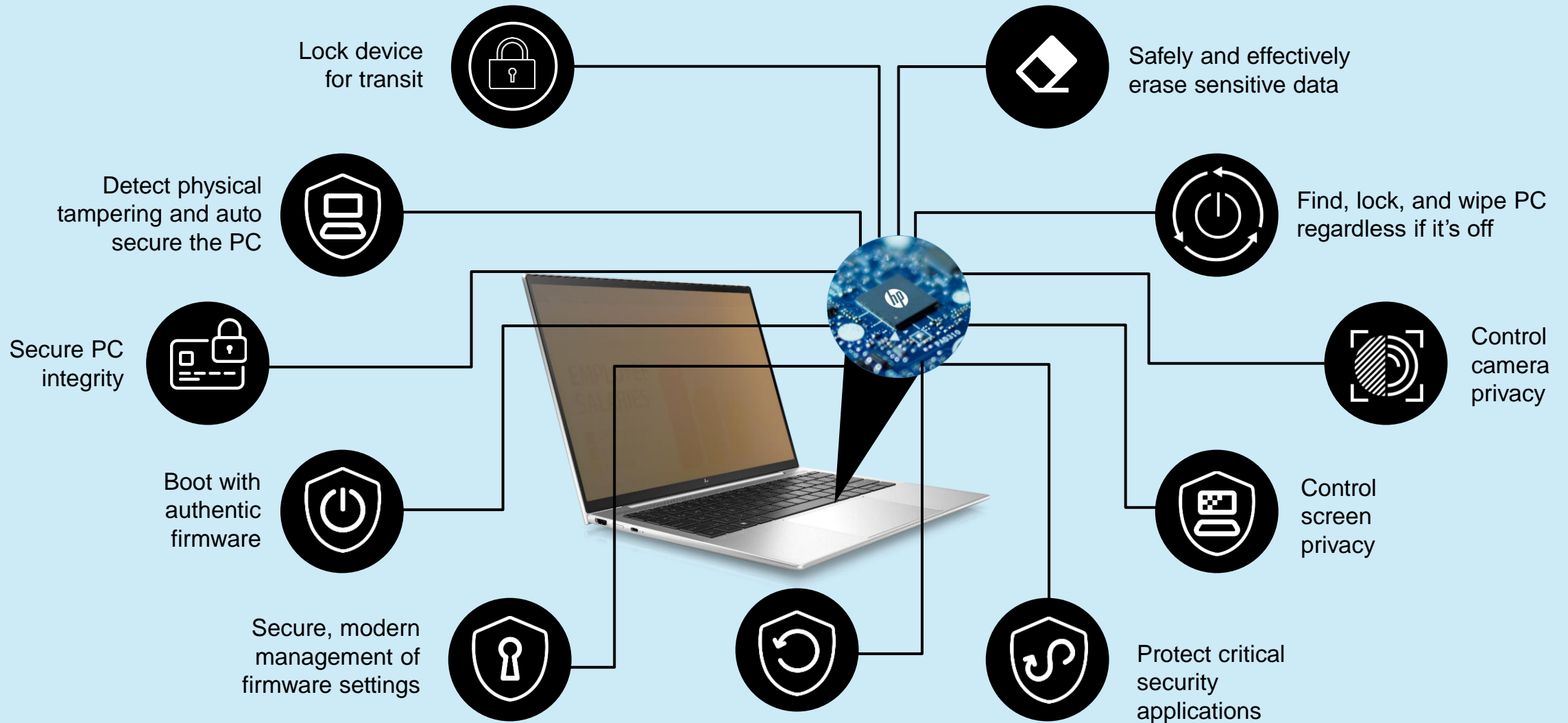


HP WOLF SECURITY



HP WOLF SECURITY

Hardening the endpoint with hardware-enforced protection

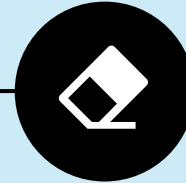


Hardening the endpoint with hardware-enforced protection

Lock device
for transit

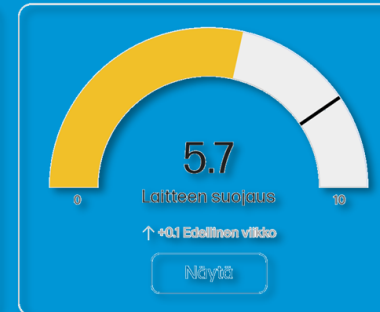
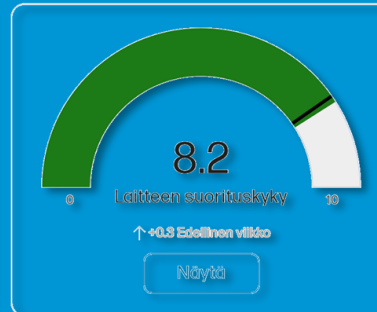
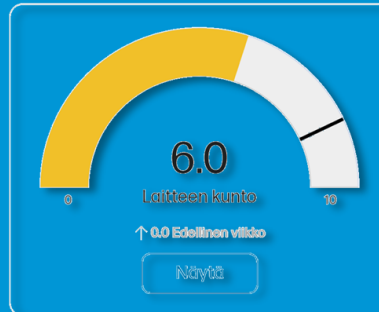


Safely and effectively
erase sensitive data



HP Proactive Insights

Proactive analytics, trend analysis, performance, health, security, digital experience and proactive warranty



Secure, modern
management of
firmware settings



Recover a secure
copy of the OS



Protect critical
security
applications





Leave nothing to chance

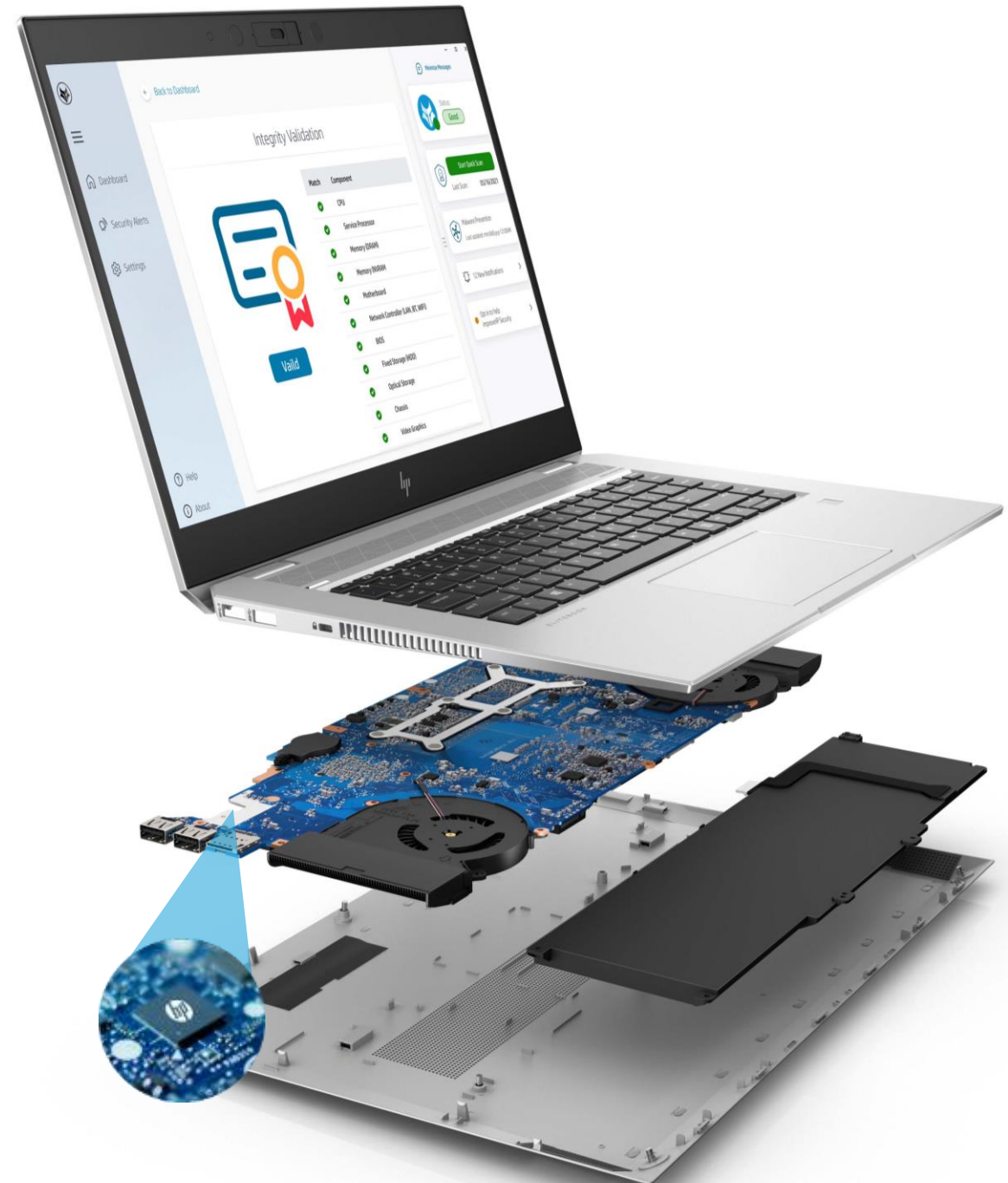
Validate the integrity of your PC with HP Platform Certificate



Verify the PC is the same as when it left the factory



Customer validation of installed PC components



Firmware Resiliency

with HP Sure Start¹⁴

Always on, persistent protection below the OS



HP WOLF SECURITY



HP Confidential. For HP and Partner use with Customers under HP CDA only.



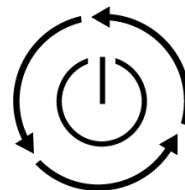
Validate

firmware before running code



Stop

corrupted code from running



Recover

a safe copy of the BIOS



Prevents

malicious peripheral attacks



HP WOLF SECURITY

Recover more than just the BIOS

HP Sure Start can recover the entire flash including the following

HP Firmware	HP Firmware Settings	Partner Firmware
HP UEFI BIOS	HP UEFI settings	Intel/AMD specific SoC boot critical content
HP Endpoint Security Controller firmware	HP Factory configuration	Intel Management Engine firmware / AMD Secure processor firmware
	Secure Boot key databases	



File Explorer window showing 'Important Documents' folder. The left sidebar includes 'Quick access' (Desktop, Downloads, Documents, Pictures, Music, Videos) and 'This PC' (master password list, stock portfolio, taxes).

Windows Firewall control panel window. Title: 'Windows Firewall'. Subtitle: 'Help protect your PC with Windows Firewall'. Text: 'Windows Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.' Network status: Private networks (Not connected), Guest or public networks (Connected). Firewall state: On. Incoming connections: Block all connections to apps that are not on the list of allowed apps. Active public networks: None.

Settings application window showing network scan options. Scan options: Quick (selected), Full, Custom. A 'Scan now' button is visible.

Outlook email client window. Title: 'My Manager - milind.thakre@hp.com - Outlook'. Shows an email from Jeff Jeansonne with subject 'Quick Feedback' and content 'Hi Milind, I am off'.

HP Sure Start warning dialog box. Text: 'HP Sure Start detected an unauthorized modification to the system firmware. Please save all data files and shut down the computer to enable HP Sure Start to repair and recover the system firmware.' Includes an 'OK' button.

Weekly Budget table:

	Income	Expenses	10% Savings	Entertainment	Daily Savings
Sunday					
Monday					
Tuesday					
Wednesday					
Thursday					
Friday					
Saturday					
Total Weekly Savings					

HP Sure Start Demo window. Text: 'Current Status = Enabled'. Buttons: 'Disable Sure Start', 'Reset Demo'. Link: 'Enable Sure Start Test Mode'.

N.I.S.T. NUMBERS YOU SHOULD KNOW

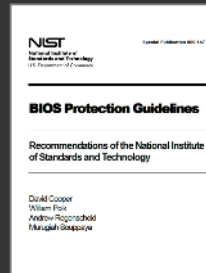
Learn more:

[HP Sure Start Whitepaper](#)



HP MEETS AND EXCEEDS

NIST SP 800-193
FOR ALL CORE EMBEDDED PLATFORM FIRMWARE

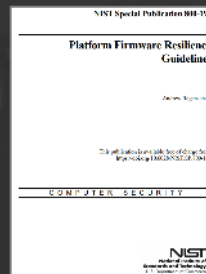


2011

BIOS PROTECTIONS

NIST SP 800-147

(2015: ISO 19678 creates an international standard)



2019

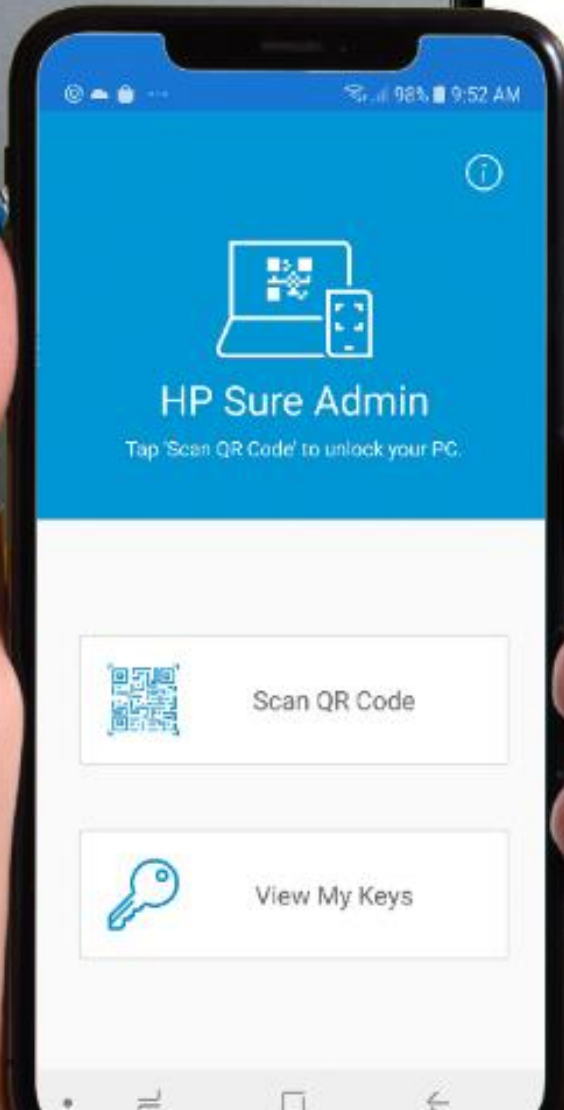
FIRMWARE RESILIENCE

NIST SP 800-193

HP Confidential. For use by HP or Partner with Customers under HP CDA only.

© 2021 HP Development Company, L.P. The information contained herein is subject to change without notice.





Never let your guard down

with HP Sure Run¹³

Protect security defenses from being disabled



Monitor

Sure Click^{12,40} & Sure Sense^{42,43}



Alert

of any changes



Auto-respond

when defenses are down

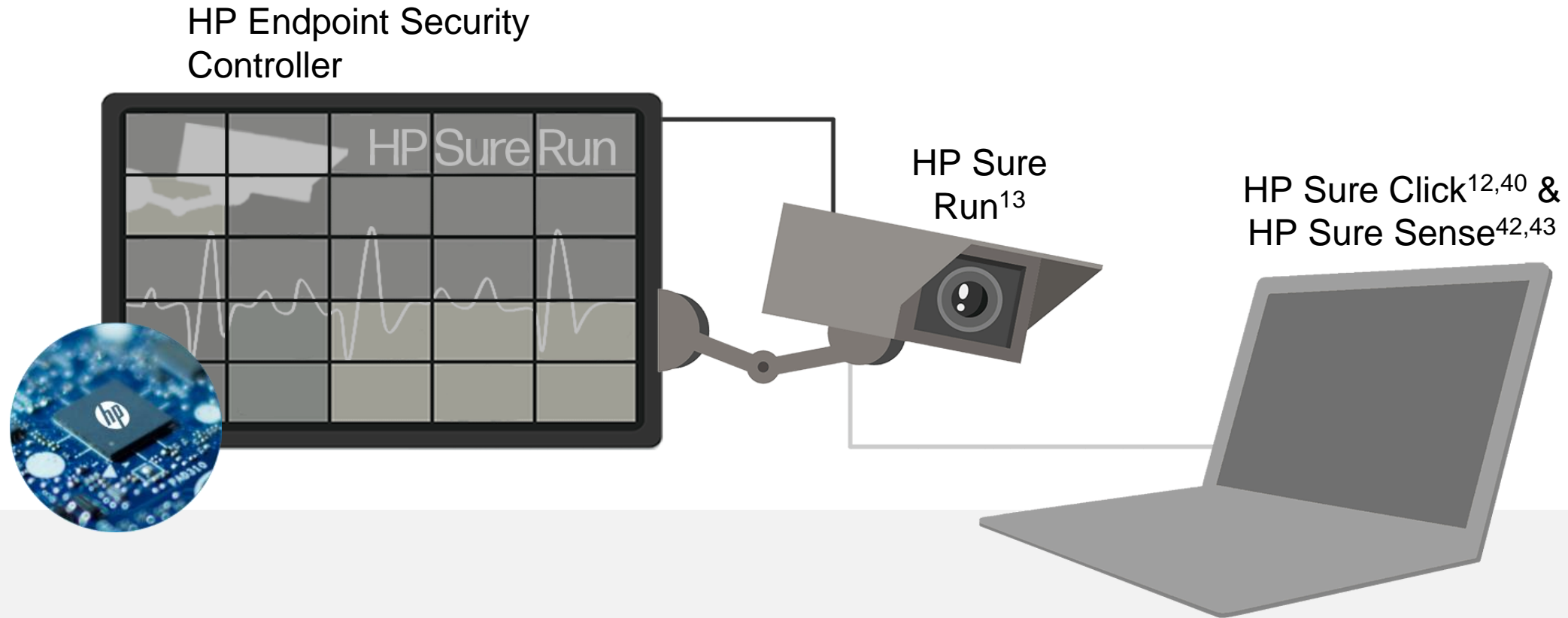


HP Sure Run¹³ leverages the power and protection of the HP Endpoint Security Controller



Resiliently stand guard

Hardware-enforced protection prevents HP Sure Run¹⁶ from being shut down



Reduce downtime. Maximize productivity. Ensure OS integrity.



Bare metal
recovery



Cloud-based
recovery²⁹



Recovery faster than a coffee break

Minutes, not hours or days

No complexity, cost effective, highly scalable

Recover one or recover all - requires no additional effort

Recover the image your way

Corporate-ready or customer image

Flexible and comprehensive

Slow or corrupted PC, destructive malware, on-demand or scheduled – pre-configure custom images and provision settings



A deeper look at HP Sure Recover¹⁵



Embedded Recovery⁴⁴

Recover image anytime, anywhere with the embedded storage option



Scheduled Recovery

Refresh PCs on your schedule to reduce potential dwell-time for malware



Modern Management

Makes it easy for users to self-recover a copy of the golden image




Designed for Deployment

Pre-configure custom images and provision settings



NOTICE Most features are disabled because your Office product is inactive. To use for free, sign in and use the Web version. [Activate](#) [Use free at Office.com](#)

HP Sure View



HP SURE VIEW INTEGRATED PRIVACY SCREEN

Helps keep data protected from visual hackers

You are opening a sensitive document.
HP Sure View will turn on automatically.

Don't show this again

OK





Dashboard



Threat Containment



Total isolations: **28**

Credential Protection



Sites protected: **0**

Sure Access



Security Management



Connected



Minimize Messages



Status:

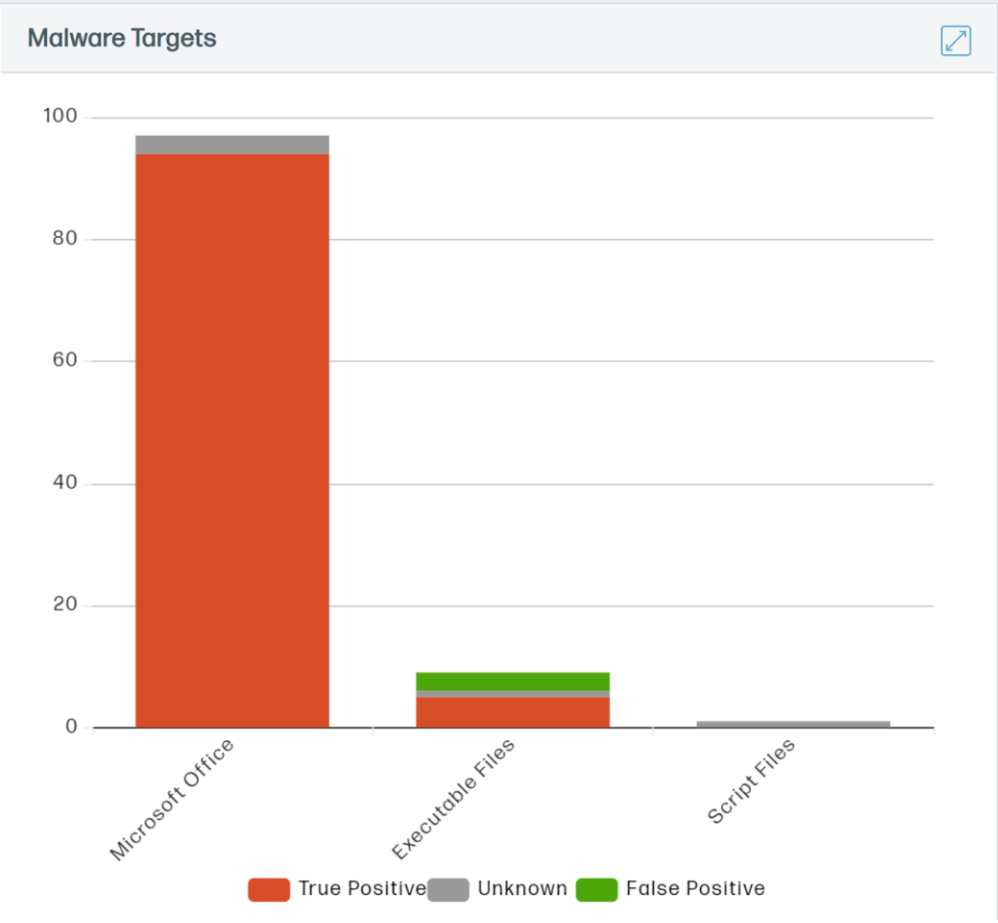
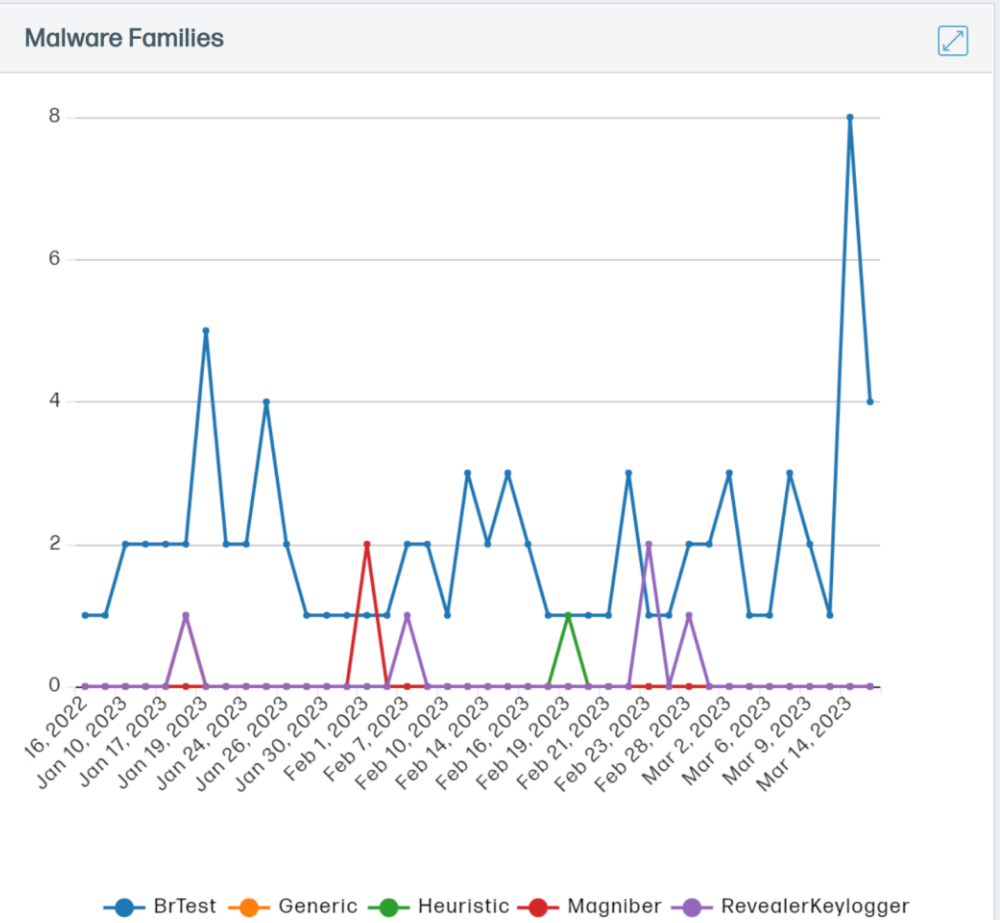
Normal

- Device Security
- Malware**
 - Dashboard
 - Threats
 - Reports
 - TAXII Consumers
- Credential Protection
- Sure Access Enterpri...
- Configuration
- Events
- Settings

Malware Dashboard

Saved Views

Status: Active Add Filter Detected: Last 90 Days



Threat UUID: 986c551f-28a9-42f6-b1e4-777374aab34e

- SUMMARY
- GRAPH
- FILES
- BEHAVIORAL
- NETWORK
- EMAIL INFO

SEVERITY **High** TOTAL EVENTS **707** HIGH SEVERITY EVENTS **23**

X360-1040-G6-SH X360-1040-G6-SH\Proactive

Threat triggered for Microsoft Word because 14 suspicious activities were detected. The triggering event was reported because of the 'cmd.exe launched' behavior. This event occurred after the micro-VM had been running for 4 seconds.

Initiated By: User Action

Threat Response: Isolated

Detected: September 22, 2021 3:49 p.m.

Received: September 22, 2021 3:53 p.m.

Updated: September 22, 2021 3:53 p.m.

Threat Ingress Details

Time: September 22, 2021 3:49 p.m.

Original File Name: CV_Edward_Teach.doc

Process: outlook.exe

TOTAL DURATION

00:00:57

ATTACK DURATION

00:00:53



After 00:00:04

Threat Indicators

HP Threat Intelligence Response

- bromium_test_malware
- edward_teach_cv

MITRE | ATT&CK™

- TA0001: Initial Access 1
- T1193 - Spearphishing Attachment
- TA0002: Execution 3
- T1106 - Execution through API
- T1129 - Execution through Module Load
- T1086 - PowerShell
- TA0003: Persistence 1
- T1215 - Kernel Modules and Extensions
- TA0004: Privilege Escalation 0
- TA0005: Defense Evasion 4
- T1107 - File Deletion
- T1112 - Modify Registry
- T1027 - Obfuscated Files or Information
- T1102 - Web Service
- TA0006: Credential Access 0
- TA0007: Discovery 1
- T1082 - System Information Discovery



- Dashboard
- Experience Mgmt
- My Organization
- Customers
- Logs
- Help & Support
- What's New

View Default

Time Duration

Add Widget

Edit

Digital Experience This Week

6.2
Device Health
↑ 0.0 Last Week
[View](#)

8.8
Device Performance
↑ +0.1 Last Week
[View](#)

5.9
Device Security
↓ -0.1 Last Week
[View](#)

Disk Capacity

1
Disk at Max Capacity

Thermal Grading

Good Thermal Grading
All PCs have good thermal grading

Network Speed (Wireless and Wired LAN)

29
Devices

■ <15 Mbps ■ >50 Mbps

Recommended Actions

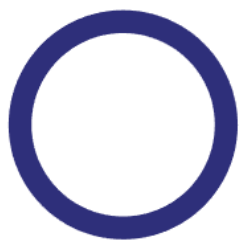
43
Devices with out of date BIOS without Policy
[View >](#)

4
Battery Replacements
[View >](#)



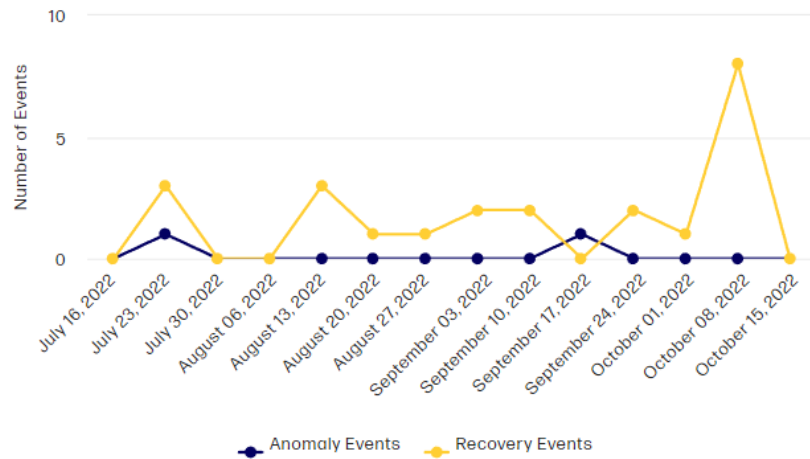
Summary Details

Unauthorized Sure Start Firmware Changes

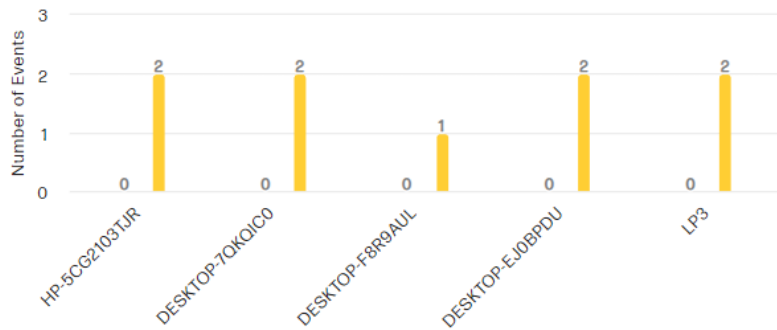


Firmware in System Flash

Activity Over Time



Most Impacted Devices



High Severity Events

No data to display

Sure Start

Shows HP Sure Start firmware anomaly and recovery activities over the past 90 days.

Company
LDK Financial
Category
Security
Subcategory
HP Sure Start System Integrity
Option
Summary
Created by
Riku HP
Created on
10/11/2022 at 05:42:34 AM (CDT)

[View Filter Criteria](#)

Detailed BIOS information of enrolled devices

Company
LDK Financial
Category
Hardware
Subcategory
BIOS Inventory

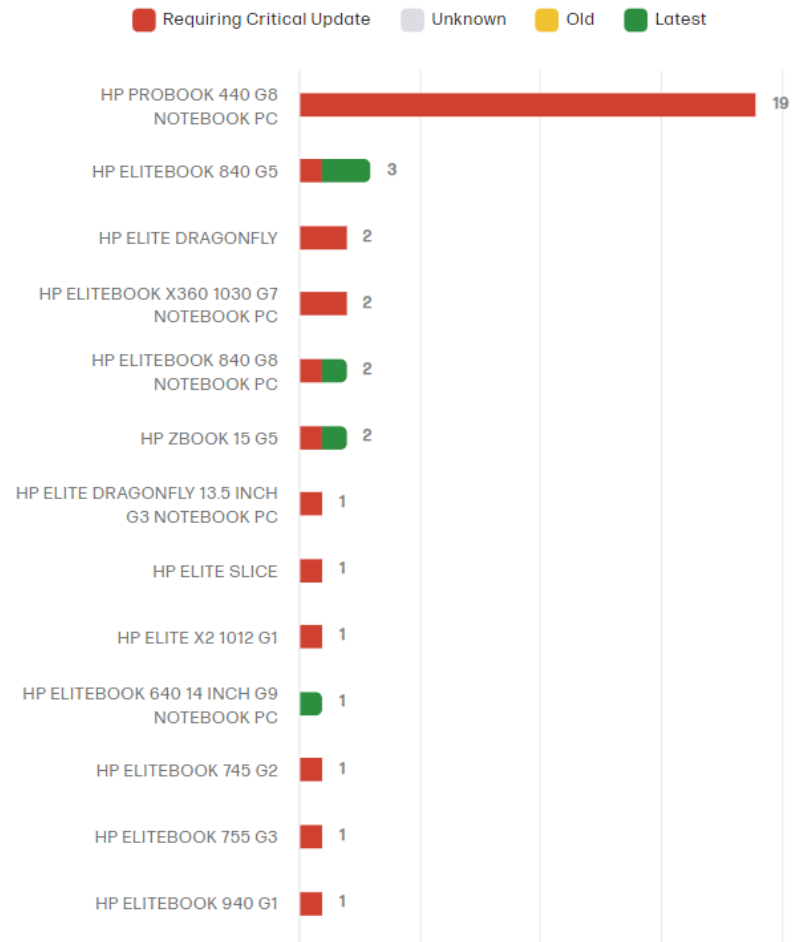
Option
Details

Created by
Riku HP

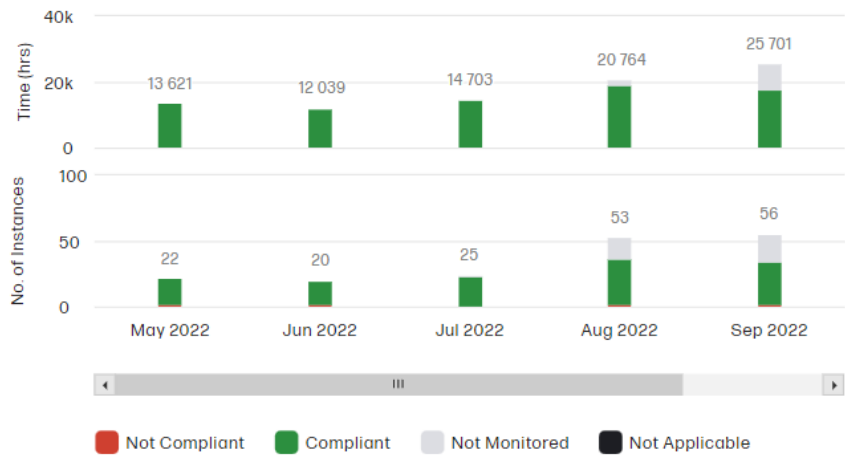
Created on
10/11/2022 at 05:44:12 AM (CDT)

[View Filter Criteria](#)

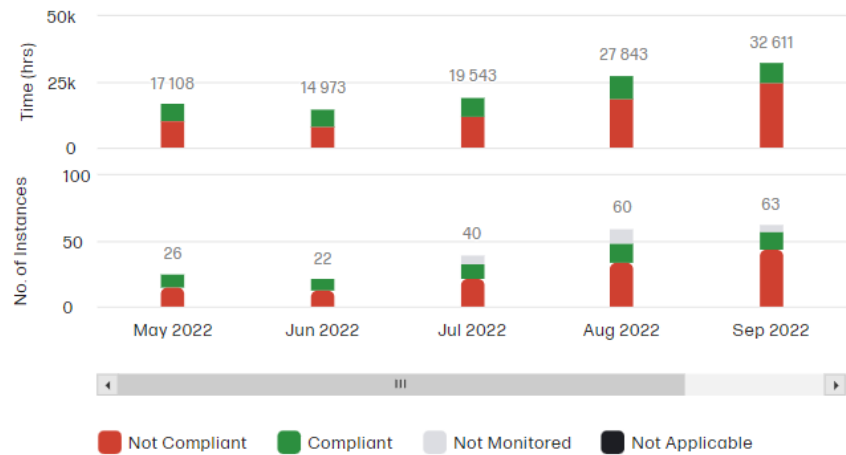
BIOS Versions by Device Model



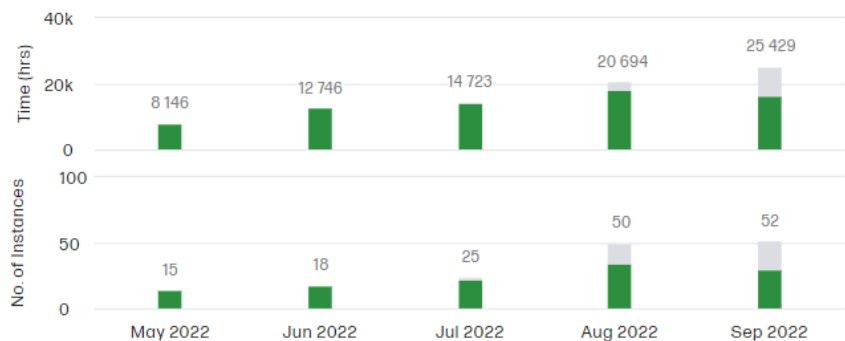
Antivirus



Encryption



Firewall



Device Security Compliance Monthly Summary

Monthly summary information of the security policy compliance of enrolled devices

Company
LDK Financial

Category
Security

Subcategory
Device Security Compliance

Option
Monthly Summary

Created by
Riku HP

Created on
10/11/2022 at 05:43:59 AM (CDT)

[View Filter Criteria](#)

Summary Details

Affected Devices

Replace Now

Replace Now (5)

Others (1)

Notebook (4)

HP Options to Consider

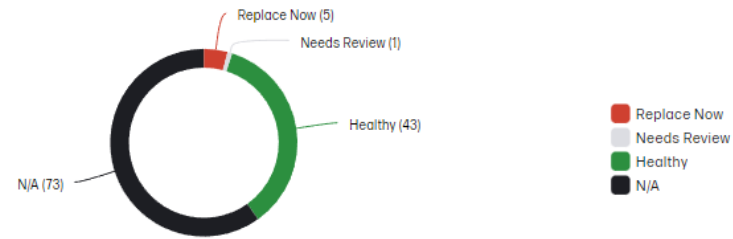
The devices below represent suitable replacements for your affected hardware

- | | | | | | |
|---------------------------------------|-------------------------------|-----------------------------------|----------------|-------------------|--|
| 1 | 1 | 2 | 1 | 1 | 1 |
| HP EliteBook x360 1040 G5 Notebook PC | HP ProBook 445 G6 Notebook PC | HP ZBook 17 G3 Mobile Workstation | HP Z-Studio G5 | OMEN Laptop - 15t | HP EliteOne 800 G4 23.8-in All-in-One PC |

1-6 of 7

< 1 2 >

Device Health Summary



Hardware Replacement

Hardware replacement recommendation of enrolled devices

Company: LDK Financial
Category: Hardware
Subcategory: Hardware Replacement

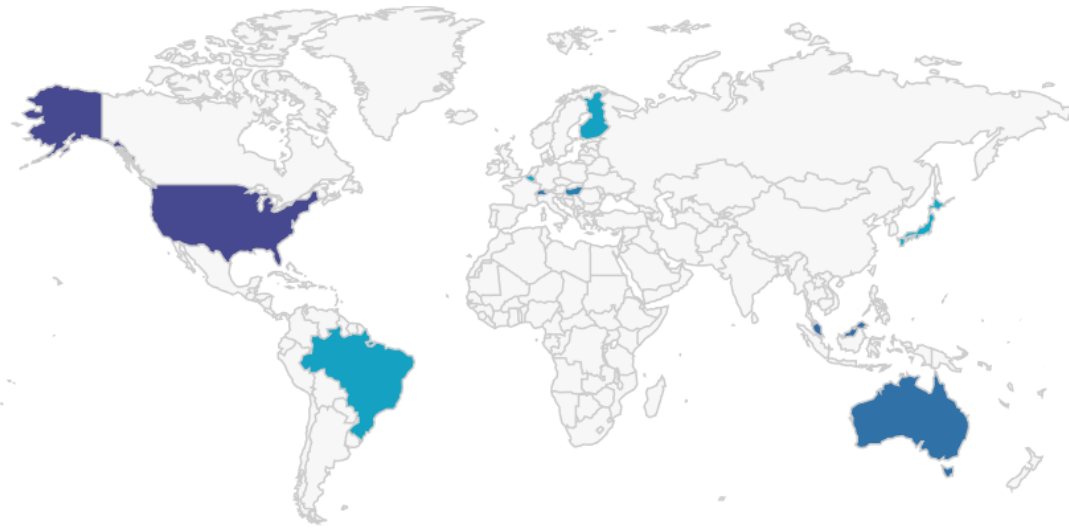
Option Details
Created by: Riku HP
Created on: 10/11/2022 at 05:49:41 AM (CDT)

[View Filter Criteria](#)

- By Location
- By Device Configuration
- By Device Model
- By Operating System
- Details

Hardware Inventory by Location

...



Hardware Inventory Details



Detailed hardware inventory of enrolled devices.

Company
LDK Financial

Category
Hardware

Subcategory
Hardware Inventory

Option
Details

Created by
Riku HP

Created on
10/11/2022 at 05:49:44 AM (CDT)

[View Filter Criteria](#)

Q & A





HP WOLF SECURITY

Дякую

AITÄH

PALDIES

KIITOS

AČIŪ

