

# HP Sure Run

Protecting what's critical, continuously



Malware poses an advanced, persistent threat, hiding itself in applications such as Windows Registry, temporary folders, ink files, and Word files. Even more insidious is the threat posed by malware to IT infrastructure security defenses. This creates the quandary of protecting the systems they are designed to protect. HP Sure Run, a hardware-enforced application persistence solution, keeps critical systems running.

## Table of Contents

Stop malware's advance on your critical OS services and settings .....	2
Hardware-enforced security protection from within.....	2
HP Sure Run shields critical processes .....	2
How HP Sure Run works in platform hardware.....	3
How HP Sure Run is enabled and managed.....	6
Conclusion.....	7

## Stop malware's advance on your critical OS services and settings

Malware targets key software security applications, attempting to disable them, making IT infrastructure vulnerable to attack.

The disruptive and damaging effects of malware include:

- Interrupted operations
- Stolen sensitive information
- Exposed access to system resources
- Decelerated computer or web browser speeds
- Disrupted network connections



IT organizations mitigate threats by deploying software security processes to help keep PCs safe and stable. For example, antivirus software helps protect against known malware. The Windows® OS possesses cryptographic services that help secure sensitive data. When these critical services or applications are disabled, malware can remain hidden and proceed deeper into the network. One example is the H1N1 malware family, which attempts to disable four different Microsoft® Windows security services (Windows Firewall, Windows Security Center, Windows Defender, and Windows Update services).

To protect against these types of attacks, organizations must ensure that critical services, applications, and settings within the OS remain operational and configured properly. Many businesses rely on processes within an OS or third-party software solution to protect PC applications. However, software-only solutions can also be targeted for removal by malware. As a result, the ideal solution must monitor and enforce the desired policies from inside the operating system domain in order to prevent malware disruptions.

## Hardware-enforced security protection from within

HP Sure Run is hardware enforced by the HP Endpoint Security Controller, making it more secure than software alone. Operating continuously, monitoring critical services, processes, and settings, HP Sure Run detects attacks or removal attempts and works to restore applications to their original state. HP Endpoint Security Controller maintains a cryptographically secure link with HP Sure Run. If malware interferes with HP Sure Run, the hardware recognizes it and can respond in a way that ensures HP Sure Run remains running.

Businesses seek to implement company policies and directives to work more effectively. It's especially important to put the correct IT security solution in place that can ensure that your company's policies remain in place.

Over time, a persistent threat can repeatedly attempt to disable protections and stop critical services without a user/admin. noticing. Sure Run is designed to continually monitor for these occurrences and restore compliance.

## HP Sure Run shields critical processes

HP business PCs equipped with HP Sure Run offer hardware-enforced application persistence with the capability both to install the agent directly into Windows in each boot and to maintain communications with the policy enforcement hardware while the OS is running. HP Sure Run builds upon the existing HP Endpoint Security Controller hardware foundation to continually maintain an operating system in a desired state. This can include applications that should always be running, policy settings that should remain in a specific state, or specific functionality that must always be present.

The HP Endpoint Security Controller, the hardware component on the circuit board on which HP Sure Start is built, protects the PC firmware at startup and during run time. HP Sure Run extends that protection into the OS, where it guards critical processes and applications, and automatically restarts them if malware tries to shut them down. If the HP Sure Run agent in the OS itself is attacked, the HP Endpoint Security Controller detects this condition and takes the configured policy action.

When HP Sure Run detects a threat or responds to an attack, it alerts the system user-administrator through the Windows Action Center. Alerts cover issues such as processes being paused or terminated; a process file that's been deleted on the storage drive; or critical registry setting changes. This ensures that system administrators are continuously aware of the state of critical services and applications.

## How HP Sure Run works in platform hardware

HP Sure Run includes an OS agent that enforces policies stored in the HP Endpoint Security Controller. The HP Sure Run agent has a secure communications link with the HP Endpoint Security Controller hardware. The link then both retrieves the policy package and communicates the status to the HP Endpoint Security Controller. This means that the HP Sure Run agent can then begin monitoring your applications, processes, policy settings, and OS functionality.

***Many threat actors have shifted focus to development of malware families and campaigns aimed at organizations where they could profit from larger payouts.***

(Source: 2020 State of Malware Report,

[https://resources.malwarebytes.com/files/2020/02/2020\\_State-of-Malware-Report.pdf](https://resources.malwarebytes.com/files/2020/02/2020_State-of-Malware-Report.pdf))

How does HP Sure Run's item categorization work? Protected items fall into four major categories:

- HP security products
- Third-party processes
- User actions, and
- Windows OS processes

To illustrate, Volume Shadow Service is one of the critical Windows services protected by HP Sure Run. Also, HP Sure Run Gen 3 made custom processes available as a protected item within the HP Sure Run platform.

Generation	Major new features/capabilities
Gen 1	<ul style="list-style-type: none"> <li>• Monitor critical platform services, registry keys, and processes remediating, if necessary</li> <li>• Fully Manageable via MIK or Client Security Manager</li> <li>• Windows event logging</li> </ul>
Gen 2	<ul style="list-style-type: none"> <li>• Network Isolation</li> <li>• User Action monitoring</li> <li>• HP Sure Sense</li> </ul>
Gen 3	<ul style="list-style-type: none"> <li>• Enhanced Sure Run Agent Persistence</li> <li>• Custom Manifest Support in MIK</li> <li>• Block requests for kill permission on monitored processes</li> <li>• Expand support to 600 series Notebooks and Desktops (G7)</li> </ul>

Table 1. HP Sure Run features by generations

HP Sure Run can also take action to restart or restore policy settings of the critical services and applications that are out of compliance. HP Sure Run does this based on its policies stored in the isolated HP Endpoint Security Controller memory, which protects against modifications by malware. If HP Sure Run is removed in Gen 1 and Gen 2, you'll need a user reboot of the system to get the firmware to reinject HP Sure Run. If HP Sure Run is removed in a Gen 3 solution, dynamic mechanisms will enable the BIOS to reinject it without requiring a user reboot. Immediately reinstalling HP Sure Run without having to reboot is a beneficial capability, as it minimizes the time in which Sure Run is not running and avoids disrupting the user.

## On each boot (when configured)

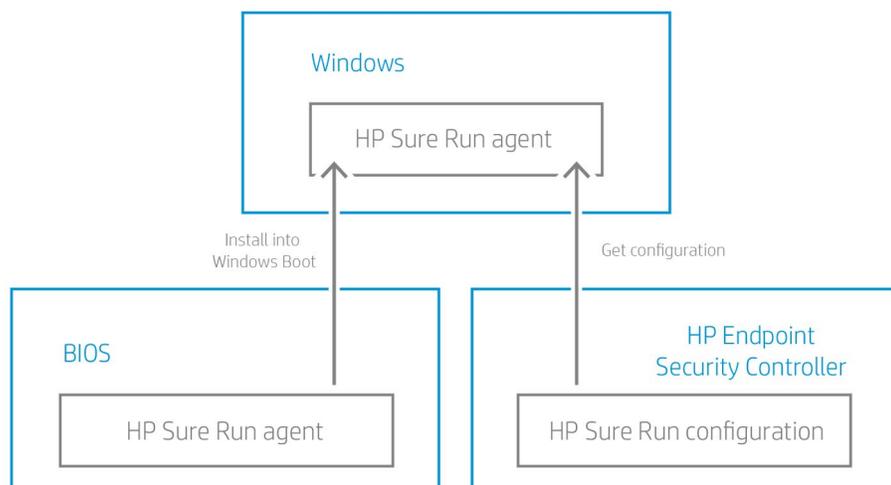


Figure 1. HP Sure Run loading from hardware to Windows on each boot, per configuration

# During runtime

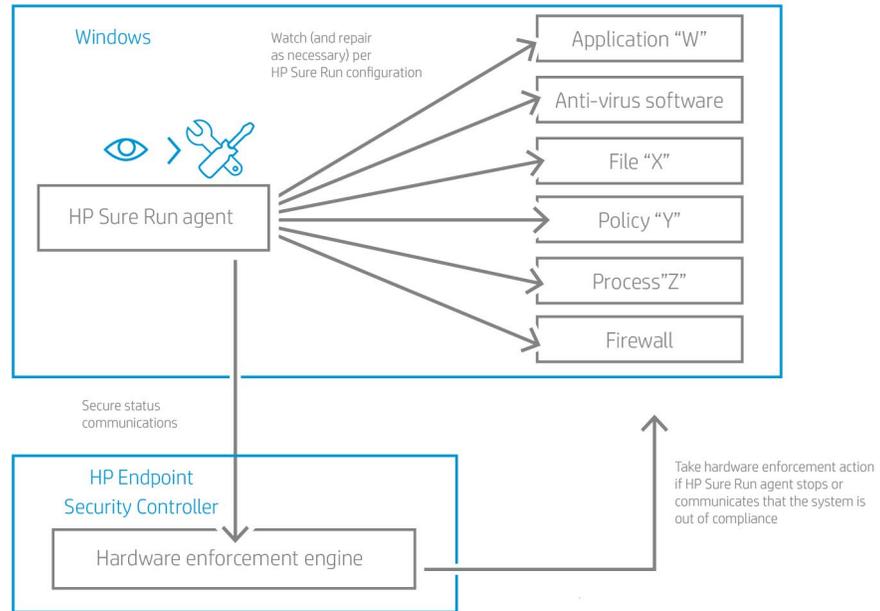


Figure 2. Runtime monitoring, per configuration, and out-of-compliance repairs

During runtime, HP Sure Run continually monitors the applications, settings, and processes according to configuration. It automatically repairs anything that is out of compliance.

## How HP Sure Run is enabled and managed

HP Sure Run is not enabled by default. Enablement and configuration of the specific applications, policy, and functionality monitored by HP Sure Run can be configured locally by the user or IT managers via the HP Client Security Manager software that is pre-installed in the HP image.

Alternatively, HP Sure Run can be securely enabled and configured remotely via the HP Management Integration Kit (MIK) plugin for Microsoft System Center Configuration Manager (SCCM).

In Gen 3, as an IT administrator on the MIK backend console, you can add up to 10 processes of your choice for HP Sure Run to monitor.

### Remote configuration

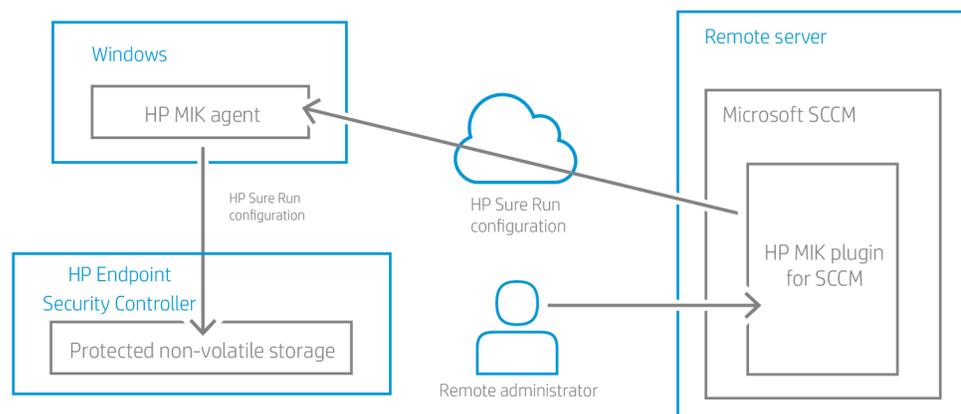


Figure 3. HP Sure Run can be configured remotely using the HP MIK plugin for Microsoft SCCM

# Local configuration

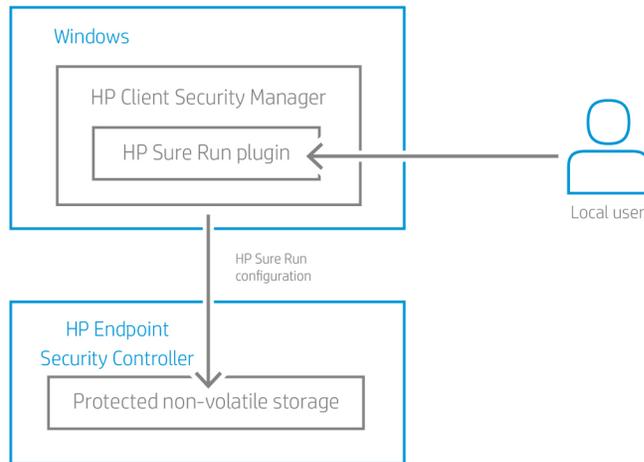


Figure 4. Alternatively, the local user or system administrator can configure HP Sure Run locally

HP Sure Run is available on HP Elite and Pro notebooks and HP Workstations with Windows 10 (Pro or Enterprise) and 8th Gen and higher Intel® processors or AMD Ryzen™ 4000 processors and higher.

## Conclusion

Advanced persistent threats are multistage attacks that can seriously disrupt your business. Protect critical services and applications with the hardware-enforced application persistence offered by HP Sure Run, exclusively available on select HP Elite and Pro PCs and select HP Workstations.

Sign up for updates: [hp.com/go/getupdated](https://hp.com/go/getupdated)

© Copyright 2020 HP Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Wi-Fi® is a registered trademark of the Wi-Fi Alliance.

4AA7-2200ENW, August 2020

