Technical white paper

HP Sure Run

Hardware-enforced application persistence for HP PCs

HP Sure Run is a hardware-enforced application persistence solution that has the capability to maintain communications with the policy enforcement hardware while the OS is running. Continually monitor the presence of critical services and applications, even if the HP Sure Run agent in the OS is attacked or removed. HP Sure Run interfaces with the HP Endpoint Security Controller at the hardware level (below the OS) to ensure OS integrity. It is included at no additional charge in select HP products.[1]

Table of contents

Malware's effect on critical OS services and settings

Organizations deploy software security processes to help keep PCs safe and stable. For example, anti-virus software stays on the lookout to protect against known malware. HP Device Access Manager helps protect USB ports so only authorized users can copy data to an external device, minimizing the threat of copying a file with malware. In the Windows® OS, cryptographic services help secure sensitive data.

Killing these critical services or applications is one way that malware can remain hidden and proceed deeper into the enterprise. One example is the H1N1 malware family, which attempts to kill four different Microsoft® Windows security services (Windows Firewall, Windows Security Center, Windows Defender, and Windows Update services).

To foil 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 modern OS's or third-party software solutions to protect PC applications. However, since these are software-only solutions, they also can be targeted for removal by the malware. The ideal solution must monitor and enforce the desired policies from outside the operating system domain, so it cannot be removed or disabled by malware.

HP Sure Run protects 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 a desired state of the operating system. This can include applications that should always be running, policy settings that should remain in a specific state, or specific functionality that must be present at all times.

The HP Endpoint Security Controller is the hardware component on the circuit board upon which HP Sure Start is built to protect the PC firmware at startup and during run time. HP Sure Run extends that protection into the OS, where it guards your most critical processes and applications—Windows Security Center, for example—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 repairs settings or applications, it alerts the user and admin in the Windows Action Center. These alerts cover things like processes being paused or terminated, a process file being deleted on the storage drive, and critical registry setting changes.

HP Sure Run is available at no additional charge on HP Elite products equipped with 8th generation Intel® or AMD® processors.

How it works

HP Sure Run includes an OS agent[2] that enforces policies which are stored in platform hardware by the HP Endpoint Security Controller. A copy of the HP Sure Run agent itself is also stored in the platform hardware by the HP Endpoint Security Controller and can be injected by the firmware directly into the operating system with no user interaction required.

The HP Sure Run agent has a secure communications link with the HP Endpoint Security Controller hardware. This link is used both to retrieve the policy package, and to communicate status to the HP Endpoint Security Controller.

The HP Sure Run agent monitors the applications, processes, policy settings, and OS functionality that it has been configured to watch. Protected items fall into four major categories: HP security products, HP processes, third-party processes, and Windows OS processes. Windows Security Center is an excellent example of a critical application protected by HP Sure Run.

The HP Sure Run agent can also take action to restart critical services and applications, or restore policy settings for any of those items that it finds to be out of compliance. HP Sure Run does this based on its policies that are stored in the isolated HP Endpoint Security Controller memory, which provides protection against modification by malware.

On each boot (when configured)

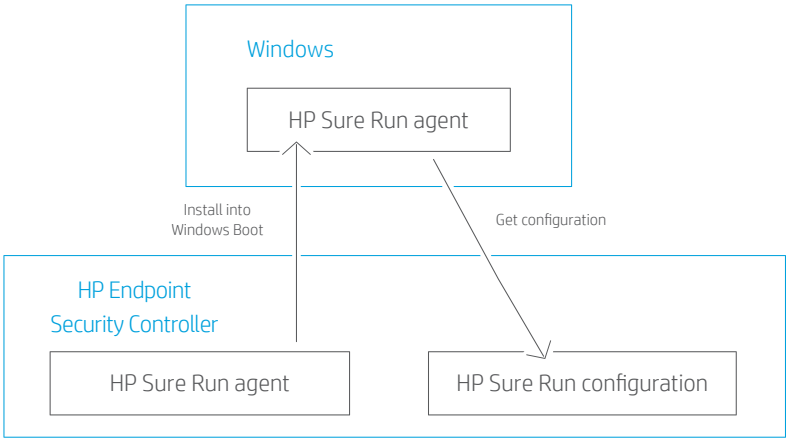

Figure 1. When configured to do so, HP Sure Run is loaded from hardware into Windows on each boot.

During runtime

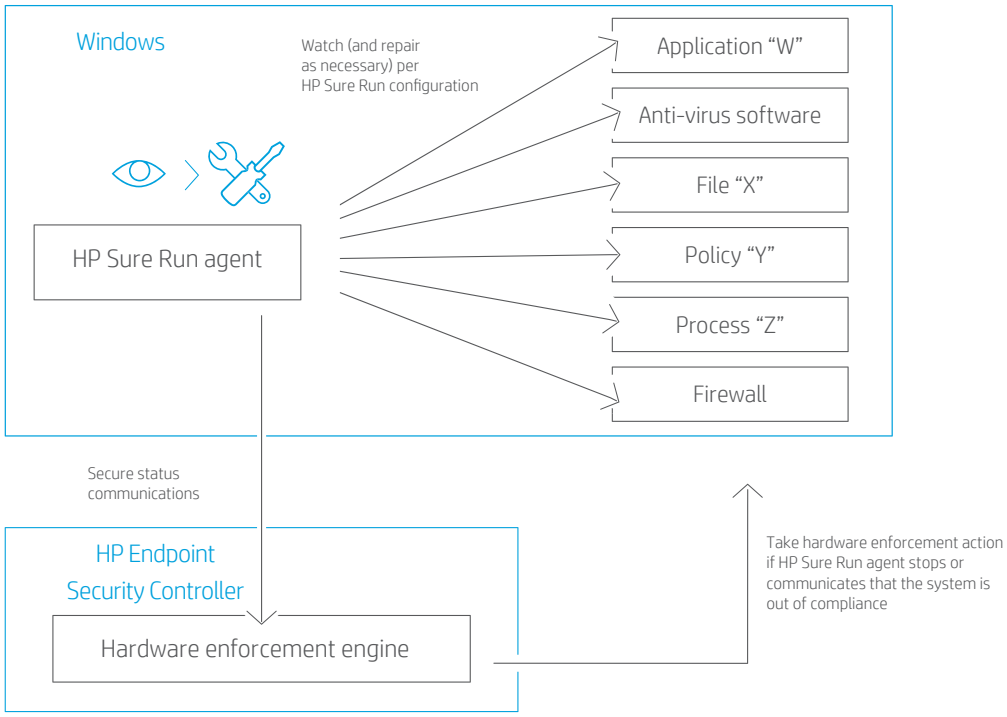

Figure 2. During runtime, HP Sure Run continually monitors the applications, settings, and processes that it has been configured to watch. It automatically repairs anything that is out of compliance.

How it's 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).

Remote configuration

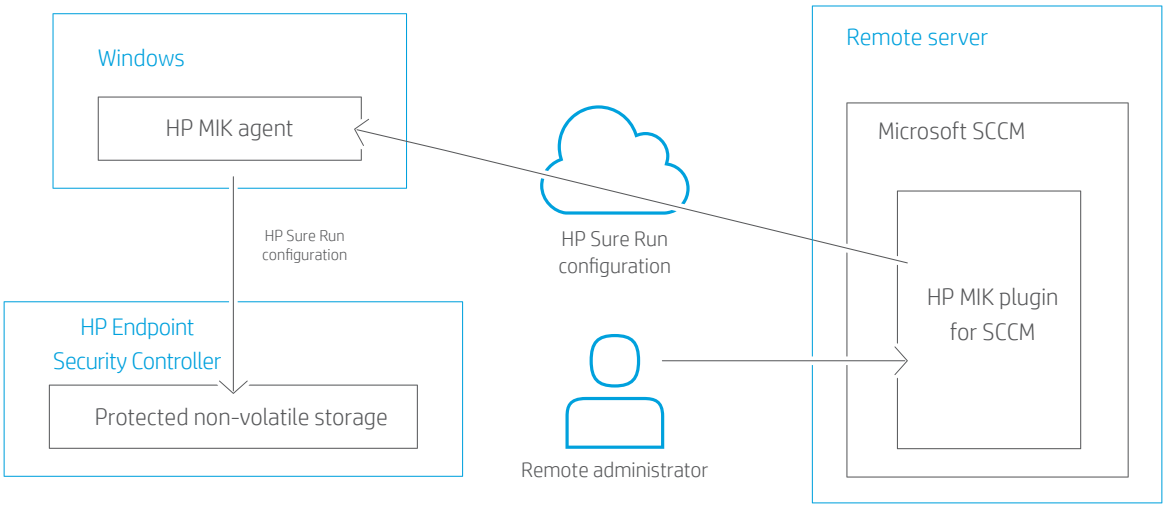

Figure 3. HP Sure Run can be configured remotely, using the HP MIK plugin for Microsoft SCCM.

Local configuration

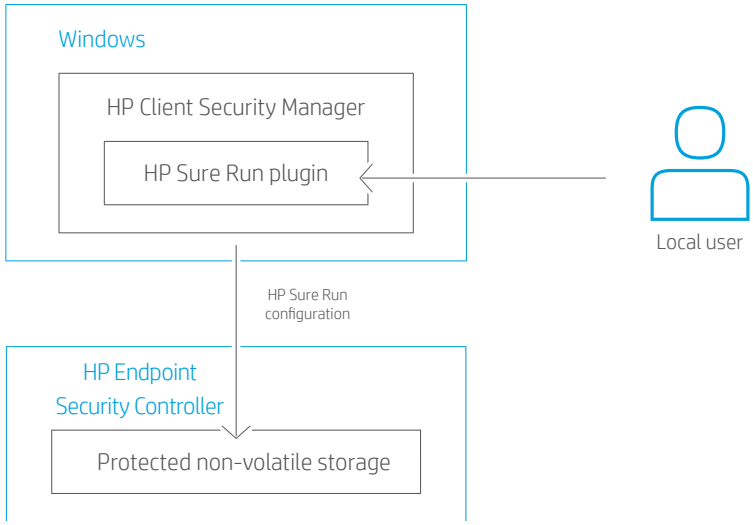

Figure 4. Alternatively, the local user or system administrator can configure HP Sure Run locally.

Conclusion

Protect critical services and applications with the hardware-enforced application persistence offered by HP Sure Run—exclusively available on select HP Elite PCs.

Learn more
hp.com/go/computersecurity

Links to technical content
support.hp.com/us-en/topic/goIT

[1] HP Sure Run is available on HP Elite products equipped with Intel or AMD 8th generation processors.
[2] Windows 10 RS2 or greater.

Sign up for updates
hp.com/go/getupdated

Share with colleagues

4AA7-2200ENW, February 2018