# HP Sure Recover

## Help ensure business continuity with secure, automated recovery

Major cyberattacks deploying destructive malware continue to increase in number and severity. These attacks can render a company's entire fleet of PCs inoperable. The escalating frequency and sophistication of these types of events has resulted in the recognition that not all cyberattacks can be stopped. Cyber resilience requires not only threat detection and defense, but response and recovery capabilities as well.

HP Sure Recover, designed to resolve these issues, can restore a software image to the system drive in as few as five minutes.[1]

# Table of Contents



4AA7-4556ENW, Nov 2020

## When disaster strikes

Cyberattacks vary in as many types and approaches as there are in number. Yet the consequences of those attacks are often all too similar, with a difficult road to recovery.

One of the first indicators of a malware attack is the computer failing to boot. As is the case in many scenarios, damage may be widespread before an organization's IT department discovers the breach, resulting in the IT helpdesk becoming quickly overwhelmed.

With PCs being the primary mode of employee communications, when they are no longer available, even activating a business continuity plan becomes significantly more challenging. Remediation processes are impacted and this likely lengthens the recovery time.

PC users are left with no ready means to recover their operating systems, applications, and data. It's a disaster. How large of a disaster could this be? An internal HP study of financial reports from four major corporations impacted by notPetya attacks revealed a loss of 4% to 7% of annual pre-tax income due to the malware attack, totaling $800M US dollars.[2]

Other software image recovery processes often depend on critical assumptions. The first of which is expecting the system drive to still have a partition with an application to assist with Windows recovery, and that the GUID Partition Table (GPT) is still intact. Victims of various wiper attacks, such as notPetya or the different versions of Shamoon, know firsthand that it's highly likely the GPT is overwritten. Additionally, these methods often do not securely validate the authenticity of the image to be recovered. They do not know if malware has tampered with this recovery image and inserted malicious code, which then comes back to the system drive through the recovery event.

Another common assumption for a legacy process is the use of recovery media, such as a USB flash memory drive, which also has uncertainty if the recovery data has become compromised, or using a DVD drive, which modern systems don't include.

Cyber events, such as the one described, reveal a pattern. A typical recovery scenario includes IT staff going to every PC and reinstalling the operating system, applications, and data. Large organizations typically have a corporate image which can automate some tasks. But this still remains a very time-consuming process. It is one thing to manually recover a handful of PCs, but for organizations with tens of thousands of PCs, this would be a daunting task, taking weeks or months to completely restore business operations.

Now, consider a scenario where the physical hardware on a PCs motherboard has the capability to automatically and securely restore the software image to the PC. A capability that exists even if a new system drive is put into the PC and it is completely blank. Consider a scenario where the software image is restored in as few as five minutes. In this scenario, the PC is attacked, wiped, and the user could be productive again in less time than a coffee break. This is the innovative technology of HP Sure Recover.

## Architectural overview

HP Sure Recover is included in many HP Business PCs (see datasheets for availability in individual models). The technology's sequence begins with the HP Endpoint Security Controller (HP ESC), which is a hardware device mounted on the PCs motherboard. The HP ESC is the foundation for several HP hardware-based, security innovations, such as HP Sure Start, HP Sure Run, HP Sure Recover, HP Sure Admin, and HP Tamper Lock. For further reading, the *HP Sure Start* whitepaper contains more details on the HP ESC.

Because HP Sure Recover is built into the PC hardware at the lowest level, it cannot be compromised by a corrupted system drive. Further, the integrity of HP Sure Recover is protected by HP Sure Start and is resilient against malware.

The basic technology begins with HP Sure Recover detecting that the system drive has been corrupted, leaving the OS unable to boot. The user is given a prompt to continue with OS recovery and a warning that the system drive will be reformatted. The user has a choice to accept and proceed or cancel and remain unbootable.

When the user chooses to proceed, HP Sure Recover loads a recovery agent, which partitions and formats the drive, securely removing any confidential information that remained. The recovery agent then downloads a system image from the network. This can be done while wired or wirelessly in HP Sure Recover Gen4.

Once downloaded, HP Sure Recover validates the authenticity of the software image to ensure that it has not been tampered with. The ESC provides a hardware root of trust for a public/private key pair used to validate the signed image. Once validated, it is then unpacked onto the system drive. After imaging has finished, the PC is rebooted, resulting in a functioning Windows environment for the user, who can proceed to restore data that has been backed up to a cloud service (e.g., Microsoft OneDrive).

HP provides a default system image accessible on the Internet for HP Sure Recover users. However, an organization may also choose to host a custom corporate image either on the Internet or a corporate intranet.

HP Sure Recover Gen4 provides valuable tools to increase the efficiency of a network-based recovery. These new features allow the system image download process to retry, pause, and resume. Policies can be established to tune these features for your environment and recovery goals.

For more details, refer to the "HP Manageability Integration Kit" (HP MIK) and the "HP Client Management Script Library." Both can be found at the HP Client Management Solutions Portal.

## Recovery without a network connection

HP Sure Recover with Embedded Reimaging is an optional feature that includes additional storage mounted on the PCs motherboard. A copy of the network-based system image is stored on this onboard storage. This enables a fast recovery, in as few as five minutes, without the need for a network connection. HP Sure Recover can also be configured to periodically check for an updated system image on the network and securely copy it into this onboard memory.

This onboard memory has strong protection and may only be accessed in a pre-boot environment, protecting it from malware running on the PC in the OS. After an updated system image is downloaded, it will be validated and copied to the onboard storage during the next reboot, before the OS is started. This version of HP Sure Recover provides the most efficient and fastest recovery method for a large fleet of computers. Contrast that to downtime caused by destructive malware that can take weeks or months to resolve.

## Scheduled recovery

PCs in certain locations can benefit from regular cleaning of the primary storage drive. For example, a PC in a retail point-of-sale location or a PC located at a hotel front desk or airport lounge have increased risk of tampering and would benefit from periodic cleanings. These PCs are in heavy traffic areas 24 hours a day and are easily accessible. Public news reports have cited examples where malware has remained undetected for more than 15 months on PCs in these types of environments.

HP Sure Recover can be configured to reimage the PC on a schedule. For example, early morning hours, when the PC is not in use, would be an excellent time to wipe the system drive and reinstall the software image.

If malware managed to infect the system drive during use, it would be removed when the system drive is wiped. Wiping the system drive on a regular schedule, such as once every 24 hours, would limit the amount of time any malware could go undetected on the PC, as well as limit the amount of damage inflicted or data stolen.

## Configuration and management

HP Sure Recover is shipped from the factory in a default configuration, giving the user a recovery solution from the moment the PC is powered on.

Additionally, users and IT administrators can configure and manage HP Sure Recover. A corporate IT administrator can use HP MIK to configure and deploy policies via Microsoft SCCM. Refer to the *HP MIK* whitepaper for details.

Additional HP Sure Recover Gen4 tools are available through the HP Client Management Script Library, including a set of free PowerShell scripts to help IT administrators automate PC lifecycle management tasks.

HP MIK and HP CMSL may be downloaded from: http://www.hp.com/go/clientmanagement.

Local users can also change some settings with the HP Client Security Manager application, which is preinstalled from the factory and available via softpaq download from HP.com. HP Sure Recover can also be configured from HPs PC BIOS (UEFI) setup menu.

## Conclusion

HP Sure Recover can greatly reduce downtime when malware has left a PC system unbootable. This translates into less costs and lost business operations.

Learn more at: hp.com/go/computersecurity.

## Appendix A—HP Sure Recover generations

| Generation | Release date | Capabilities added |
|---|---|---|
| HP Sure Recover | 2018 | • Cloud-based OS recovery; meets or exceeds proposed NIST requirements for recoverable systems<br>• Scheduled reimaging; start each day malware free |
| HP Sure Recover with Embedded Reimaging | 2018 | • Embedded reimaging; fastest and most secure imaging |
| HP Sure Recover Gen2 | 2019 | • Corporate recovery agent; customized image deployment from private distribution points<br>• Split image file support with download resume; optimized network delivery<br>• Golden master imaging; speeds deployment by eliminating dependency on the Windows installer<br>• Intel Optane and multiple drive configurations; support for complex storage configurations<br>• Windows 10 Home and IoT editions; more choices for a wider range of systems |
| HP Sure Recover Gen3 | 2020 | • Cloud-based OS recovery over WiFi; recovery, untethered<br>• HP Client Management Script Library; provision and configure HP Sure Recover with PowerShell<br>• Support for HP Pro 600 PCs (*Refer to datasheet for availability*)<br>• Pause, resume, and retry; policy-based controls to minimize network utilization during at-scale attacks<br>• HP TechPulse analytics and reporting; configuration, managed status, recovery schedule, repository locations |

Table 1: HP Sure Recover generations and capabilities

1. Reimaging time estimate based on HP Internal testing of an HP EliteBook x360 1030 G3 with Core i7 vPro processor and TBD SSD (factory installed SSDs probably all have similar performance characteristics) using preinstalled image and drivers (5.9 GB total size).
2. *Analysis of Financial Impact due to 2017 notPetya Attacks*, November 2017.

Sign up for updates: hp.com/go/getupdated



4AA7-4556ENW, Nov 2020