HP Sure Sense

Technical Whitepaper

How long would it take to recover half of the PCs in your organization after a malware attack? At one time, a question like that may have sounded like a mythical doomsday scenario. But, in an age where a business can come to a grinding halt for days after a malware attack, and municipal governments are asked to pay exorbitant sums after a ransomware attack, today's smart IT decision makers are wise to consider scenarios like these and have a proactive plan in place. Malware is rapidly evolving with artificial intelligence to become more evasive and destructive. HP focuses on security innovation solutions to deliver freedom for users and protection for businesses. HP Sure Sense utilizes a leading form of artificial intelligence technology called Deep Learning Neural Networks. The HP Sure Sense proprietary deep learning algorithm instinctively recognizes malware and protects against never-before-seen attacks.

Table of contents

4AA7-6875ENW, September 2020

List of figures

Problem—New trends in endpoint security breaches and the risk of business losses

As malware strategies and methods evolve, the IT Security defense strategies that worked before won't work today. Every company should prepare a strategy to address these new trends.

Securing endpoint devices is key

Every PC purchase is a security decision. Designing devices with a hardware root of trust is a key factor toward security and resilience. Because traditional network security is not enough, enhanced protection must start from the hardware up.

The HP Essential Security on endpoint devices is the first step towards resilience. HP offers PCs that are built to security standards and offer the state-of-the-art deep learning HP Sure Sense device security. Recognizing a problem before it becomes a problem makes all the difference. Securing endpoint devices offers users and administrators the resilience to get back to business after an attack. Who needs resilience? Everyone.

Shifting focus to endpoints

Many organizations are counting on their firewalls to protect data and devices within the network, but the firewall alone isn't enough. It's becoming much easier for hackers to break into networks through under-secured endpoints like IoT devices, PCs, and printers. In a typical organization, the number of endpoints is much greater than the number of servers, sometimes as many as two devices per employee. Consider all the computers and printers employees use throughout the day—including laptops and other portable devices taken home for use after hours. The sheer volume of endpoints increases the risk. Just one stolen or vulnerable device can provide entry to the network, expose sensitive data, and put the entire infrastructure at risk. That's why it's so important to deploy devices with built-in security protections that can detect and automatically recover from attacks.

An increase in firmware attacks

There was a 50% growth in fileless attacks in 2017, with 30% of organizations suffering a fileless attack in 2017.[1],[2] What the security industry refers to as fileless attacks does not mean the attack is without files. It means the attack may be script-based instead of using an executable, such as Cobalt Malware; or Dual-Use abuse of admin, system, or forensic tools such as Windows Sysinternals; or Living Off The Land abuse of native Windows tools such as Power Shell. Another type of fileless attack is Code Injection. In most cases, files inject code into a process, such as Poweliks Trojan.

The rapid evolution of malware

Rapid evolution of malware carries risk because traditional list-based antivirus tools can't catch novel first-time cyberattacks. There was a 92% increase in new downloader variants in 2017. [3] New malware emerges every 4.2 seconds.[4] About 69% of organizations do not believe the threats they are seeing can be blocked by antivirus software.[5] To defend against modern and never-before-seen threats, PCs must recognize malware instinctively.

Traditional network security is not enough. Detecting malware is not enough. To defend against modern threats, we must be able to identify malware instantly and stop it in its tracks.

Increasingly destructive attacks

A new trend towards increasingly destructive attacks brings an elevated financial risk. Instead of an attack only impairing functionality, modern cyberattacks could mean hundreds of PCs are suddenly bricked, which may or may not be recoverable with traditional tools, especially if BIOS is involved.

Business impact from a security breach

Downtime from a cyberattack harms more than the IT department. It harms the entire organization, and the brand. Consider the ripple effect of these business losses resulting from a security breach:

- Loss of critical operation data
- Customer data breach resulting in fines and litigation
- Loss of productive business operation time that should be spent serving customers
- Loss of sales and operations revenue
- Loss of brand equity and customer trust

Cybercrime is a disruptive force. The average cost of a cyber security breach now reaches $3.6M[6]. It is not a matter of *if* but *when* an attack will be successful.

It's more than just a hassle. Downtime from attacks can destroy your bottom line.

Increasing risk of never-before-seen attacks

If a particular malware has been used in a previous attack, that malware will be on the list of known predators. When other security tools scan for malware, those tools are looking for known predators. First-time attacks of a malware that has never been seen before do not appear on the list of known predators, so they can slip under the radar of other security tools.

Use of AI in malware means attacks are more difficult to detect

The concept of "fight fire with fire" is certainly true in the realm of cyber security. If malware attacks use artificial intelligence (AI) to become smarter, then security tools must use AI to become even smarter. The use of AI in malware can create attacks that are more adaptive and more evasive of some security tools. This is creating a need for more highly evolved, increasingly agile and responsive security tools.

Deep learning theory

In the 1950s, artificial intelligence was introduced. In the 1980s, machine learning was introduced. In the 2010s, AI took an enormous leap forward with deep learning. Deep learning is the most advanced subset of AI, taking inspiration from how the human brain works.

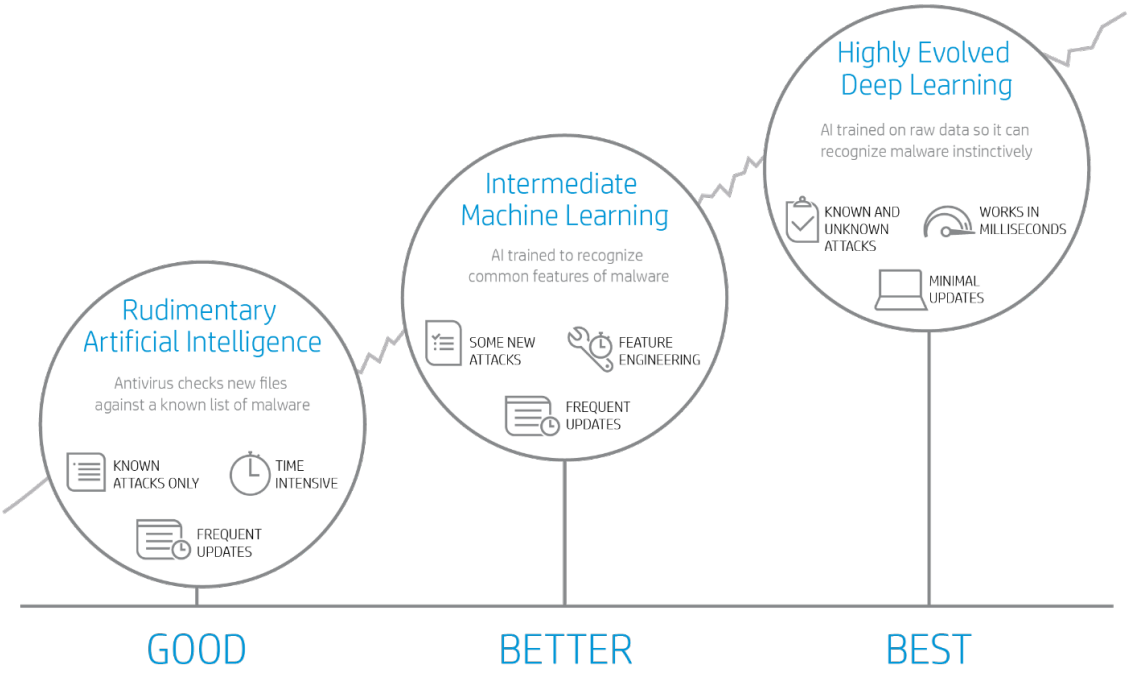

Figure 1: Comparing rudimentary artificial intelligence, intermediate machine learning, and highly evolved deep learning

During the past few years, deep learning has achieved 20% to 30% improvement in most benchmarks of computer vision, speech recognition, and text understanding, delivering the most significant leaps for performance in the history of AI and computer science.

What is deep learning?

Deep learning is the most advanced subset of AI, inspired by the brain's ability to learn. Once a human brain learns to identify an object, its identification becomes second nature. Today, the HP Sure Sense deep learning brain, consisting of complex neural networks, can process high amounts of data to get a profound and highly accurate understanding of the data analyzed. For this reason, deep learning is the preferred method in such applications as voice and image recognition, autonomous cars, and even diagnosing health care tests.

How does deep learning differ from other AI solutions?

Deep learning is light years ahead of standard machine learning solutions. Classical machine learning delivers breakthrough outcomes, but has limitations for malware prevention due to its reliance on feature extraction. In this process, human experts determine the critical features for the model to identify.

Machine learning and face recognition

To explain the methods a malware detection software uses to determine if a file is beneficial or malicious, it's helpful to consider using the same process to determine whether an animal is a cat or a dog.

Consider the challenge of face recognition. You can't just feed the raw pixels of an image into a machine learning module. Instead, a human must first convert those pixels into specific features that the machine learning module will be on the lookout for, such as the distance between pupils, proportions of the face, and color. Focusing on aspects defined by human experts through feature extraction works to a degree, but misses the rich, intricate patterns in the raw data. When applied to malware detection, traditional machine learning is a huge step forward over legacy signature-based methods. However, this type of machine learning exhibits limitations in both the ability to detect novel malware, as well as frequent false positives, which IT must then investigate.

Traditional machine learning—Shallow learning

Using the traditional machine learning method or shallow learning, beginning with raw data, manual features are extracted to create a vector of handcrafted features, then the machine scans for these features in order to recognize what the machine is looking for.

Machine learning—General approach and feature extraction

The human brain understands and recognizes objects (even when they are obscured)—a cat partially hidden behind another object, for example. However, traditional machine learning is not good at recognizing such things due to what is called feature extraction—partial information extracted from data and used for recognition.

Machine learning—Certain features and criteria may be misleading

Sometimes dogs and cats may have similar features, so relying on features alone can be misleading. So, if you identify a cat with its face, and if the cat's face is partially or fully hidden, machine learning would not be able to understand that the object being watched might be a cat or is a cat. This is an example of the limitations of machine learning.

You don't need computer software to recognize a dog or a cat because you have instinctively learned to recognize them. Telling the difference between a dog and a cat is not the million-dollar question. Telling the difference between malware and a beneficial file is the critical need. So, let's consider what we've learned from the dog and cat discernment process and apply it to malware.

When applied to malware detection, traditional machine learning is a huge step forward over legacy signature-based methods. However, this type of machine learning exhibits limitations in both the ability to detect novel malware, as well as frequent false positives that IT must then investigate. HP Sure Sense is built on deep learning technology that is capable of training directly on raw data. In this instance, when we say raw data, we mean supervised learning using benign files and malware files.

In a data center, the raw data of hundreds of millions of files, both good and bad, are used in training HP Sure Sense's AI prediction model. During this process, algorithms define the minute characteristics between good and bad files to build an AI prediction model in a fashion similar to the way a human brain works.

This model is then distilled into a very small automated software agent that is installed on the PC. This powerful software agent can identify most never-before-seen malware with greater than 99% efficacy while consuming less than 1% CPU while idle.

HP Sure Sense software is so effective in malware identification that the model typically only requires an update four times per year. HP Sure Sense deep learning technology brings a completely new approach to cybersecurity. It's where the cyber intelligence deep learning neural net brain can learn to identify any type of cyber threat, then detect and prevent zero-day and advanced persistent threat (APT) attacks in real-time with unmatched accuracy.

How HP Sure Sense Deep Learning Starts

The HP Sure Sense deep learning startup process begins with training the Brain, then creating the HP Sure Sense software agent, and adding HP Sure Sense to HP PCs during the manufacturing process. HP Sure Sense protection is active right out of the box.

Train the Brain

The process starts with a patented Deep Learning Neural Network Brain.

Preparation: Data scientists prepare data samples that are used for training the Deep Learning Neural Network Brain. Those data samples contain over a billion samples of code, malicious and benign, to train the Brain to tell the difference.

Training: The Self-Learning Loop is a process during which the Brain is exposed to raw data of the files, learning to instinctively identify malicious code.

Detection: As the training phase continues, the Brain begins to instinctively detect and identify malware by scanning their "DNA" (raw data).

Prediction: The Brain reaches the prediction level. From now on it can predict whether or not the file is a threat.

Agent creation

This phase compresses the Brain with all of its abilities into a lightweight but powerful agent, turning terabytes of insights into megabytes of instinct.

Protection

Agent insertion: This lightweight agent is inserted into select HP PCs, where it is included and enabled right out of the box.

Agent protection: From this point on, the agent checks every file, such as PE, PDF, Office, or Fonts before it executes. The process is fast, and with a light usage of system resources, the agent doesn't slow down the user experience.

Prevention: The agent knows how to detect and prevent any type of malware, allowing the benign files to run and the malicious ones to be stopped.

The HP Sure Sense Neural Network Brain is trained with hundreds of millions of malicious and legit files using the proprietary Deep Neural Network (DNN) algorithm, also known as deep learning. The outcome of the training is the HP Sure Sense lightweight module that is distributed in select HP Elite endpoint computers. The module is also available as a Softpaq download.

Once distributed, any new file that tries to access the device is scanned by HP Sure Sense and given a score, all within milliseconds. The score represents the maliciousness level of the file. Then, according to a predefined policy threshold, the software agent decides whether to block and prevent the file, or to allow it to run.

Not only can deep learning be used to prevent malicious files from running, it can also provide threat intelligence by classifying in real time what type of malware is targeting the organization.

With HP Sure Sense Deep Learning Neural Network, the output layer may have multiple outputs, while typical standard networks have only one output. Therefore, HP Sure Sense Deep Learning can also be used to classify malware types, where each output represents a malware family type. Each output is displayed with a percentage representing the family characteristics; all outputs' sum is a weight of 100.

Solution overview—HP security with HP Sure Sense–Empowering capabilities for positive results

What product capabilities are included in HP Sure Sense?

- **Instinctive recognition:** To defend against modern and never-before-seen threats, PCs must recognize malware instinctively. HP Sure Sense applies a new evolution of artificial intelligence called Deep Learning Neural Network to create a security tool that instinctively recognizes a never-before-seen threat without waiting for an antivirus update.
- **Passive threat prevention powered by deep learning:** HP Sure Sense can identify whether a file is a malware threat before it is opened or run. HP Sure Sense provides a lightweight endpoint protection software installed on HP Windows PCs. It encompasses prediction model enabling on-device, lightweight, autonomous, and real-time cyber threat prevention. When HP Sure Sense is installed, a full file scan is performed on the PC's local drives and a file-hash is sent to a file reputation service. For each new file added to the PC hard drive after the scan, HP Sure Sense will perform a file scan. The file does not need to be opened or executed before the protective scan, meaning HP Sure Sense detects potential attacks before the file is opened or executed.
- **Active threat prevention powered by behavioral detection:** HP Sure Sense detects PC behavior associated with ransomware threats. When a file on the PC hard drive is identified as malicious, HP Sure Sense blocks and quarantines that file.
- **Protection for a broad array of file-based threats including, but not limited to:** Portable executables (such as .exe, .dll, etc.) or Microsoft Office (Excel, Word, PowerPoint) and PDF files (when Microsoft Office or Adobe Acrobat are installed).
- **Protection against fileless threats:** Protects against malware that stays memory resident, such as Macro or Dual-use that do not write to the hard drive, making it very difficult for these threats to be detected by legacy solutions.
- **Cloud support:** To protect the PC at all times, HP Sure Sense can perform protection functions with or without a cloud connection. When connected to a live Internet connection, HP Sure Sense leverages a Reputation Cloud service to scan for potentially unwanted applications (PUAs) or potentially unwanted programs (PUPs). Many commercially available anti-malware applications use this type of Reputation Cloud service. HP Sure Sense user files and user privacy remain secure using a hash-based cloud interaction of anonymous aggregated data. To ensure user data is protected, HP Sure Sense performs a scan of files saved locally to the PC searching for malicious content. If the file is suspect, a hash of the file is sent to the reputation-based cloud. The hash is encrypted via SHA-512 in transit. If the file's hash-file is evaluated as high-risk after being analyzed, the original file is quarantined on the local PC. Confidential data within the file or document never leaves the local PC.
- **Trusted file list:** The trusted file list lives in the HP Sure Sense software agent on the user's local hard drive. The trusted file list does not live in the cloud. HP Sure Sense users can add to the trusted file list using the HP Sure Sense console.
- **Zero-day threat protection and full-drive scanning:** HP Sure Sense inspects new files on writes and alerts and quarantines malware. The quarantine process copies the file to the quarantine folder, deletes the file from its original location, and provides notification in the HP Sure Sense Console Quarantine tab.
- **Hardware-enforced protection:** When enabled by an administrator, HP Sure Run prevents/protects against malware disabling HP Sure Sense.

HP Sure Sense delivers features and benefits

- On-device protection that provides real-time prevention, both online and offline
- Time to prevent, 20 milliseconds[7]
- Time to investigate, 50 milliseconds[7]
- Time to remediate and contain, less than one minute[7]
- Harness the power of deep learning
- Scans every file before execution to protect against zero-day unknown and known attacks
- Autonomous agent on each device works online or offline, with minimal updates every three months

- Real-time protection with lightweight usage of system resources—less than 30MB and less than 1% of CPU
- Enhanced threat protection identifies ransomware behavior even before the file executes, and even before an attack starts running
- Quarantines potential ransomware before it can do any damage

Solution Details—How It Works

The Deep Learning Neural Network—also called the Brain—learns in a similar manner as the human brain. This proprietary deep learning framework is autonomous; no human intervention is required. Using a non-linear model, the Brain discerns correlation and context within the data, allowing it to recognize a threat instinctively.

Understanding HP Sure Sense Software

HP Sure Sense is a lightweight endpoint protection software that is preinstalled on select HP Elite, Pro 400 series, Pro 600 series PCs, workstations, and retail point of sale PCs. It encompasses the essence of deep learning prediction model enabling on-device, lightweight, autonomous, and real-time cyber threat prevention. HP Sure Sense provides real-time detection and prevention of zero-day threats and APT attacks for Windows applications. This proactive protection provides unprecedented accuracy in detection and real-time prevention, protecting Windows applications from any threat (known and unknown).

HP Sure Sense uses the following key components to implement its security solution:

- **Prediction model:** A lightweight prediction model, the output of the training phase that detects cyber threats. It is placed on the content delivery network (CDN) for distribution and installed together with HP Sure Sense software. Once installed, the prediction model is used to autonomously detect cyber threats, enabling on-device zero-day and APT protection.
- **Content delivery network (CDN):** Distributes the latest prediction model and minor software updates (hotfixes) to all Windows devices running HP Sure Sense software.
- **File reputation cloud services:** The services provide a fast and scalable infrastructure in the cloud (Amazon Web Services (AWS)) that adds a second layer of classification. When using these services, files can be reclassified in a second layer of validation using the database of intellectual information on known files, and the right verdict is updated in real time. The following are benefits of these services:
  - No user files are shared with the cloud.
  - Assists in faster evaluation and classification of malware.
  - This is an optional service that the user can select in the control panel.

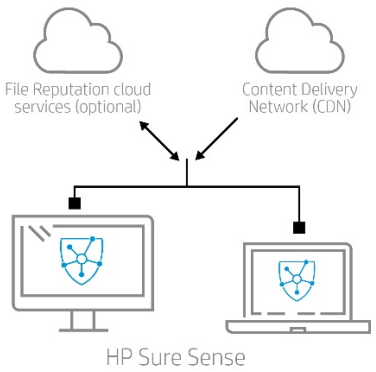

Figure 2: HP Sure Sense architecture

Static vs. dynamic protection

Static protection is scanning a file to see if it LOOKS like malware before it runs.

Dynamic protection is watching the behaviors of a particular element AFTER it has been allowed to run.

Here's one way to think of it: When airport security checks a person before that person gets into the airport, that is an example of static protection. Security is checking to see if there is anything suspicious about that person before they get into the airport. But if a person were to start acting suspiciously after they get in the airport, and security stopped the person, that is an example of dynamic protection. Even though that person may have seemed okay at first, their behaviors show they might be a threat. That is dynamic protection, based on behavior being monitored even after entering the airport.

HP Sure Sense provides static protection for all files before they execute. HP Sure Sense also provides dynamic protection against ransomware, so no matter how innocent a file looks when it enters your PC, if it starts behaving like ransomware—attempting to encrypt your files, for example—HP Sure Sense will quarantine it.

HP Sure Sense static and dynamic protection features are provided with no perceptible impact to system performance.

Layers of defense: How HP Sure Sense works with existing security tools

How does HP create the world's most secure and manageable PCs?

There are three core components:

First, we start with resilient hardware, based on a hardware root of trust. This is hardware that can self-monitor and self-heal in case of an attack—it's able to protect, detect, and recover.

This resiliency on select HP Business PCs is provided by three solutions (HP Sure Start, HP Sure Run, and HP Sure Recover), which are all enabled by HPs unique security hardware—the Endpoint Security Controller.

Second, ideally, we want to keep malware from entering in the first place. That's why HP wraps every endpoint in multiple layers of protection against malware and other attacks to proactively prevent threats—below, in, and above the OS. These are solutions you may already be familiar with, such as HP Sure Click and HP Sure Sense.

And third, HP Sure Sense can augment your current security deployment. It is intended to operate with traditional security tools such as Windows Defender, wrapping endpoints in layers of defense for synergistic protection.

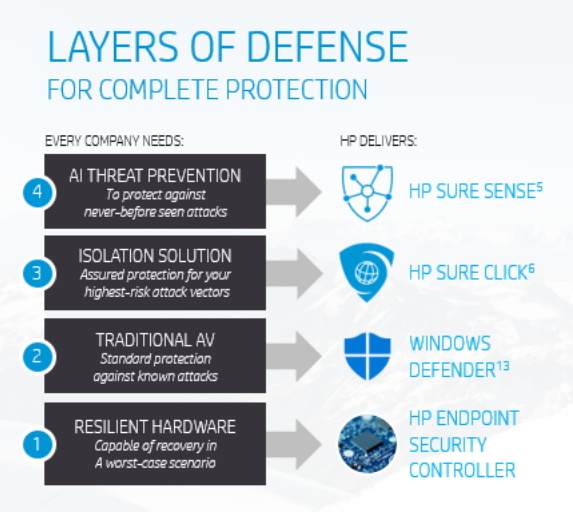

Figure 3: Layers of defense

By offering users and administrators the great advantage of identifying never-before-seen malware and immediately responding with real-time protection, HP Sure Sense fills the gap in the traditional security model, while allowing administrators to continue to leverage existing tools.

HP is revolutionizing security with a whole new approach: help protect the network and reduce risk by building layers of security into endpoint hardware. HP printers and PCs are designed to protect the device, identity, data, and documents. A comprehensive mix of built-in features and add-on solutions helps protect each of these from below (hardware enforced), within, and above the operating system.

And, of course, any protection needs to be manageable, because security without manageability is unsustainable. HP's unique management solutions help organizations improve endpoint device security without over-burdening their IT staff. Many monitoring and management tasks can be handled automatically, without IT intervention. HP devices are also designed to seamlessly connect to Security Information and Event Monitoring (SIEM) tools to provide real-time security-event analysis.

Conclusion

Securing endpoint devices is key

Every PC purchase is a security decision. Designing device resilience with a hardware root of trust is key. Traditional network security is not enough. Enhanced protection must start from the hardware up. Endpoint devices are the first line of defense. Endpoints that are built to security standards and offer the state-of-the-art in device security can make all the difference.

Hardware-based security

HP Sure Run can ensure that HP Sure Sense is not paused or prevented from running. All of the HP security solutions come factory shipped on the product to ensure the hardware you receive from the factory offers you the most protected platform—the world's most secure, manageable, and resilient PC.

Implementation

For guidance on implementing HP Sure Sense, see Appendix A–HP Sure Sense function operations console.

HP Sure Sense benefits

HP Sure Sense delivers these key benefits:

- Provides protection from zero-day never-before-seen threats
- Runs in the background with low usage of endpoint system resources
- Protects automatically without requiring end-user intervention
- Teaches itself to instinctively recognize threats
- Gives quarterly updates
- Works in concert with HP hardware root of trust with self-healing BIOS and HP Sure Run to ensure malware cannot disable HP Sure Sense
- Is available on select HP Business PCs, factory installed, or available to include with an Enterprise custom image
- Supplies peace of mind to both Small and Medium Business (SMB) and Enterprise customers—who know the deep learning algorithm evolves faster than malware, giving them automated, ongoing protection

Learn more: hp.com/go/computersecurity

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

Appendix A–HP Sure Sense function operations console

Customer Experience Improvement message

The Customer Experience Improvement message is only displayed the first time the HP Sure Sense console is opened. If you click **Join**, the related checkbox on the Settings page is selected. This message does not appear again, even if **Not Now** is clicked.

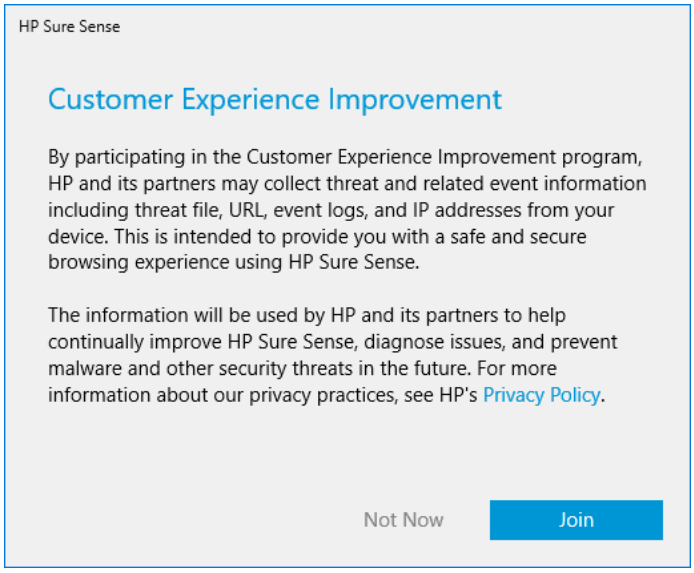

Figure 4: Customer Experience Improvement message

Status page

The Status page displays the protection status, scanning information, and other information on HP Sure Sense. The following illustrates the Status page in the HP Sure Sense console.

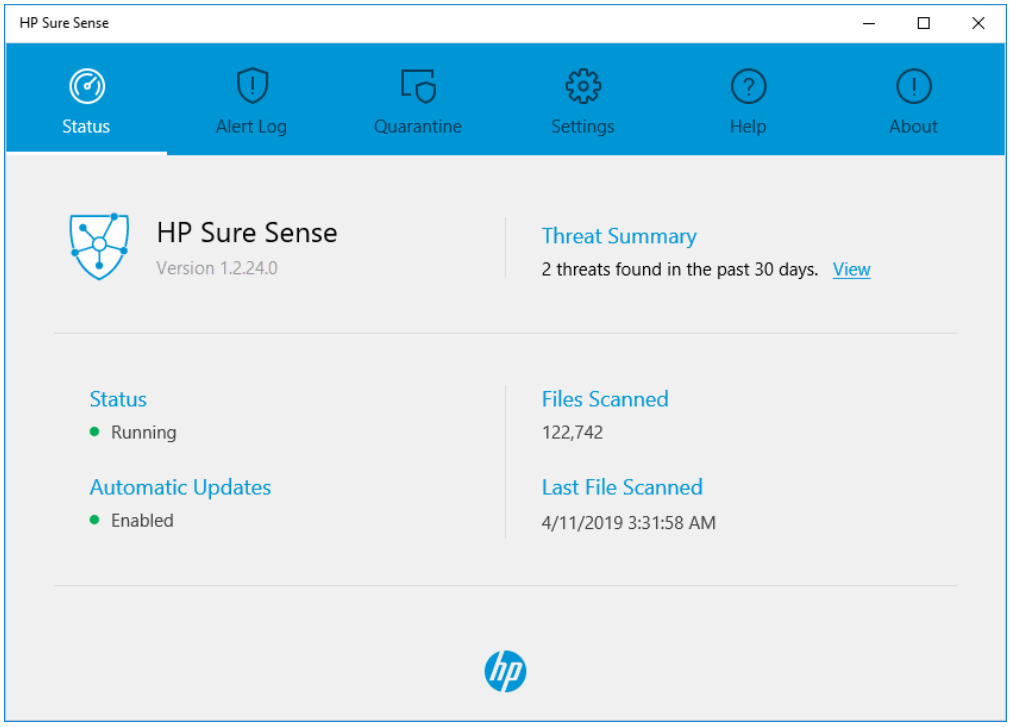

Figure 5: Status page when full scan is not running

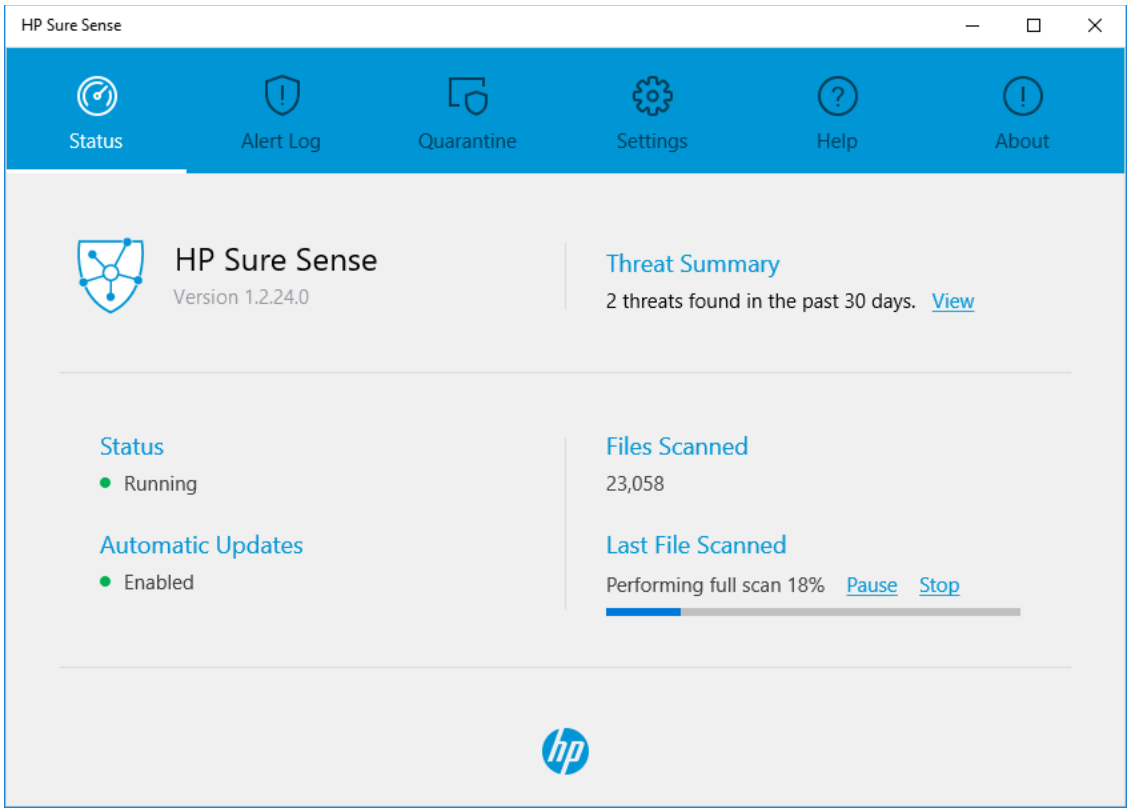

Figure 6: Status page while performing a full scan

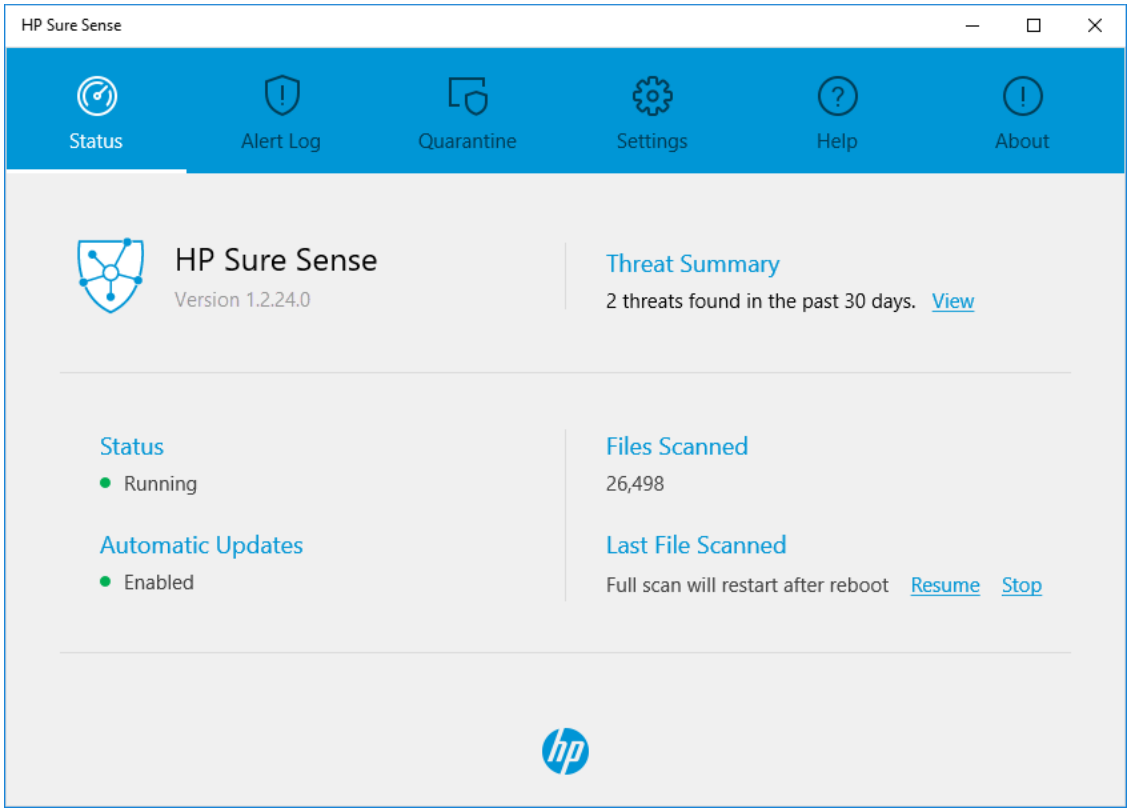

Figure 7: Status page while full scan is paused

On the Status page, the following has been implemented:

- Version – The version number of the installed HP Sure Sense.
- Click to Update – This text appears when a new update is available. Click **Click to Update** to update HP Sure Sense.
- Threat Summary – The number of threats identified within the last 30 days. Click **View** to open the Alert Log page to view information about these threats.
- Status – This indicates whether HP Sure Sense protection is enabled or disabled.
- Automatic Updates – This indicates whether HP Sure Sense is set to receive updates automatically. To change the setting, go to the Settings page.
- Files Scanned – The number of files scanned by HP Sure Sense. The counter includes all files scanned from the start of the last full scan.
- Last File Scanned – The date and time the last file was scanned. During a full scan, the following is displayed:
  - Pause – Click **Pause** to pause the full scan. Click **Resume** to continue the full scan. If the computer is restarted, the full scan will restart and scan from the beginning.
  - Stop – Click **Stop** to stop the full scan.
  - Resume – This is displayed when the full scan is paused. Click **Resume** to immediately continue the full scan.

Alert Log page

The Alert Log page displays a table that lists the security events and logs collected by HP Sure Sense. It includes information related to security, updates, and management.

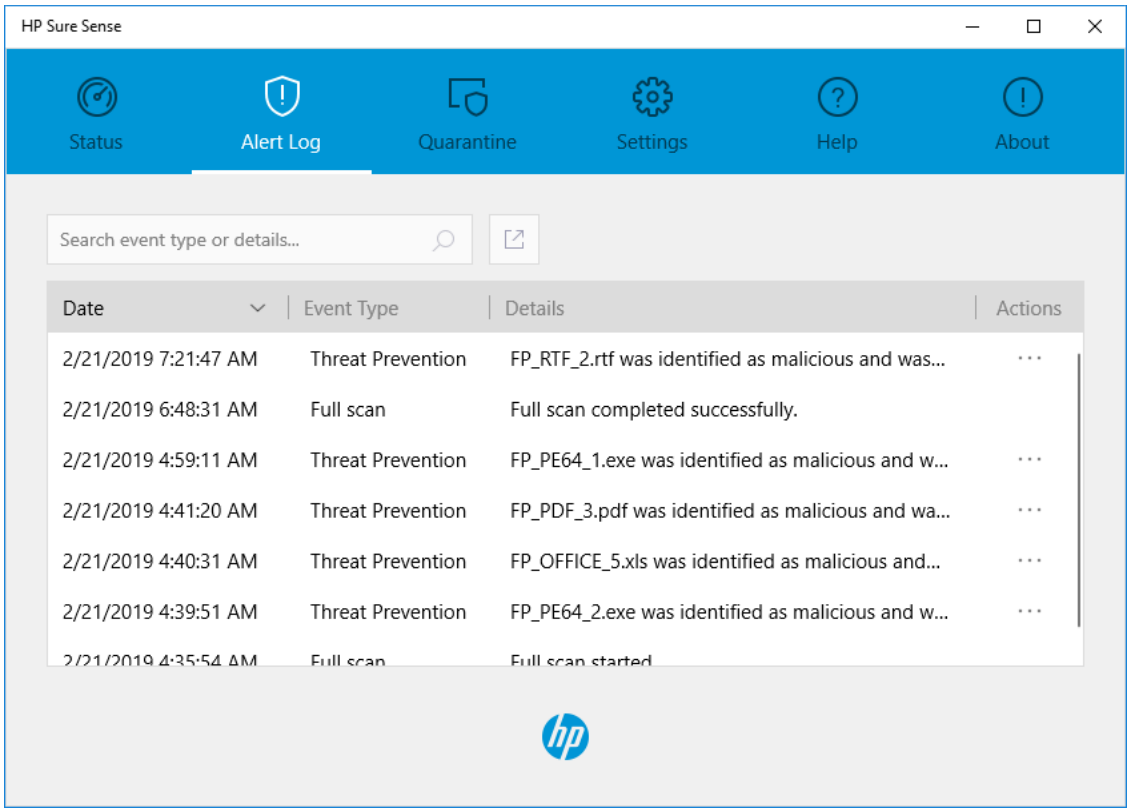

Figure 8: Alert Log page

The Alert Log table includes the following information:

- Date – The date and time the event occurred.
- Event Type – The type of event or action that occurred.
- Details – It's detailed information about the event or action. This displays the malware filename and type of attack, or type of action that occurred.

From this page, you can do the following:

- Filter the information to display only the relevant information.
- Sort the information by clicking on column headings. The information in the table is sorted based on the selected column.
- Export all the events from the table to create a CSV file.
- Access the File Details screen for a selected event, to display additional information on a quarantined file.
- Access the Process Details screen for a selected event where the process was terminated.
- Restore the quarantined file related to a selected event
- Add a process with ransomware indicators to the Trusted Files list and allow the process to run.
- For an entry with an associated quarantined file, delete the file from the quarantine folder and its associated entry on the Quarantine page.

Quarantine page

The Quarantine page displays a table that lists all quarantined files. Each entry is based on a unique hash value. Entries include information related to the files and their original locations.

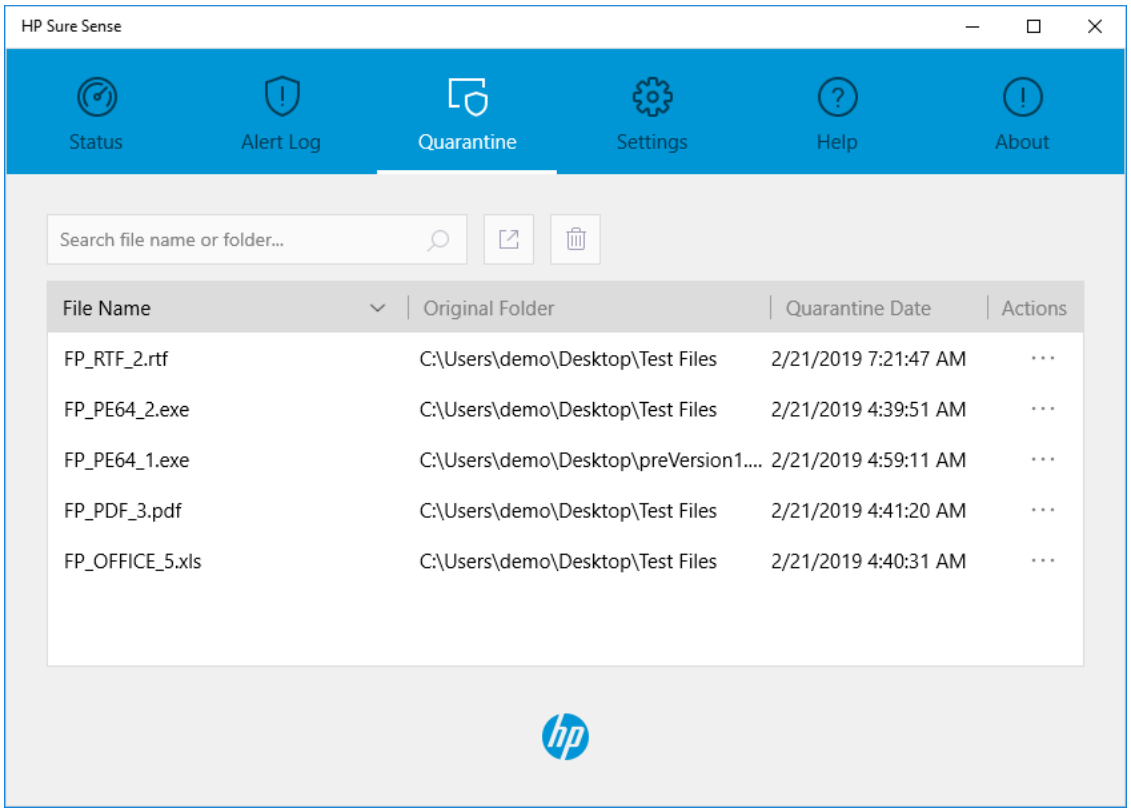

Figure 9: Quarantine page

The Quarantine table includes the following information:

- File Name – The name of the quarantined file.
- Original Folder – The path of the folder from where the file was deleted and quarantined. When the file is restored, it is restored to this folder.
- Quarantine Date – The date and time the file was quarantined.

From this page, you can do the following:

- Filter the information to display only the relevant information.
- Sort the information by clicking on column headings. The information in the table is sorted based on the selected column.
- Export all entries from the table to create a CSV file.
- Delete all quarantine entries.
- Access the File Details screen for a selected entry.
- Restore the quarantined files related to a selected entry.
- Delete a file from the quarantine folder and its associated entry on the Quarantine page.

Settings page

The Settings page is used to display and configure HP Sure Sense. To view or change Advanced Settings, you must have administrator permissions. Click **Edit** to enter the administrator credentials and the Advanced Settings appear. If you logged on as an administrator, a message appears to confirm your request to open the Advanced Settings.

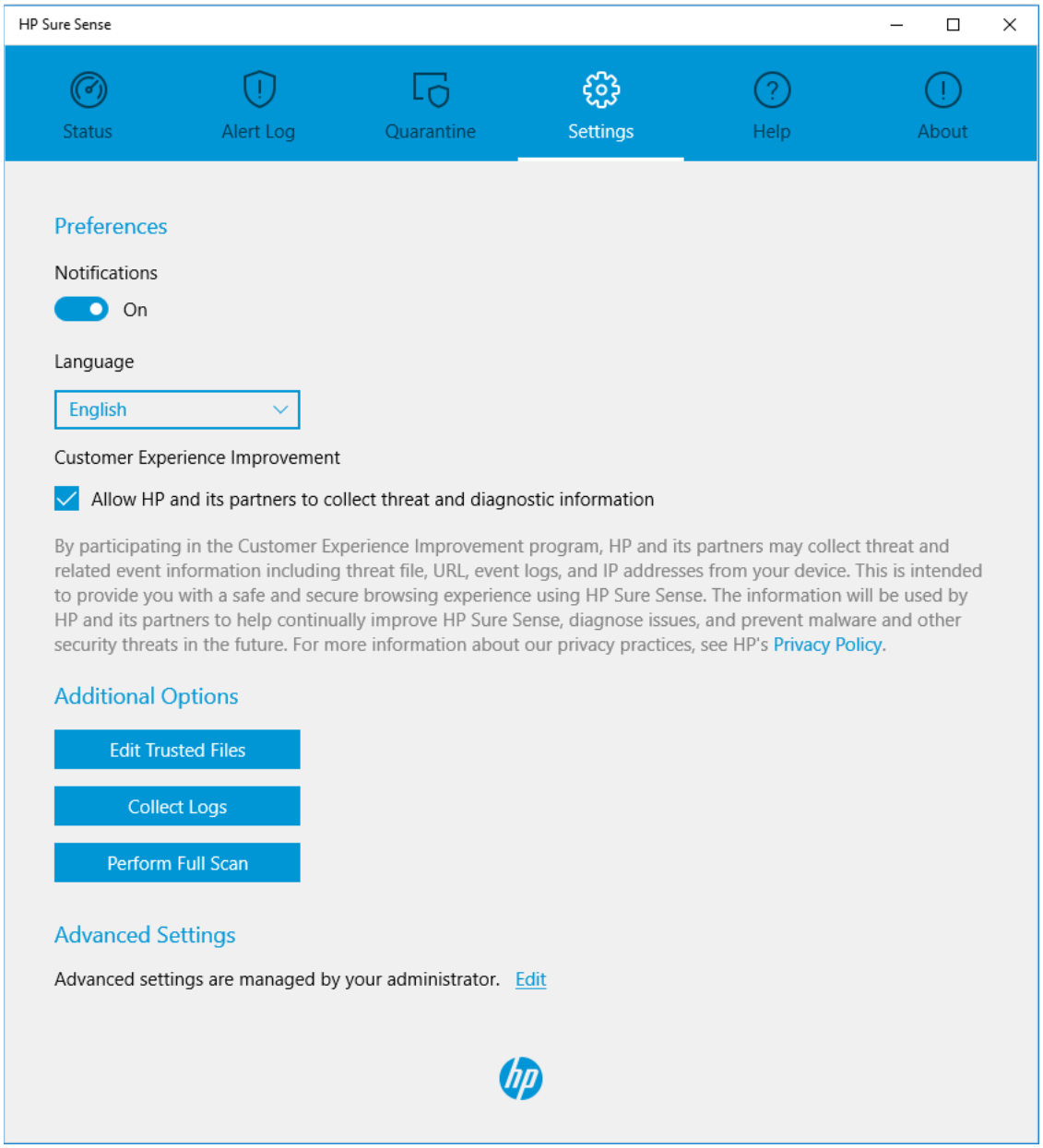

Figure 10: Settings page with basic settings

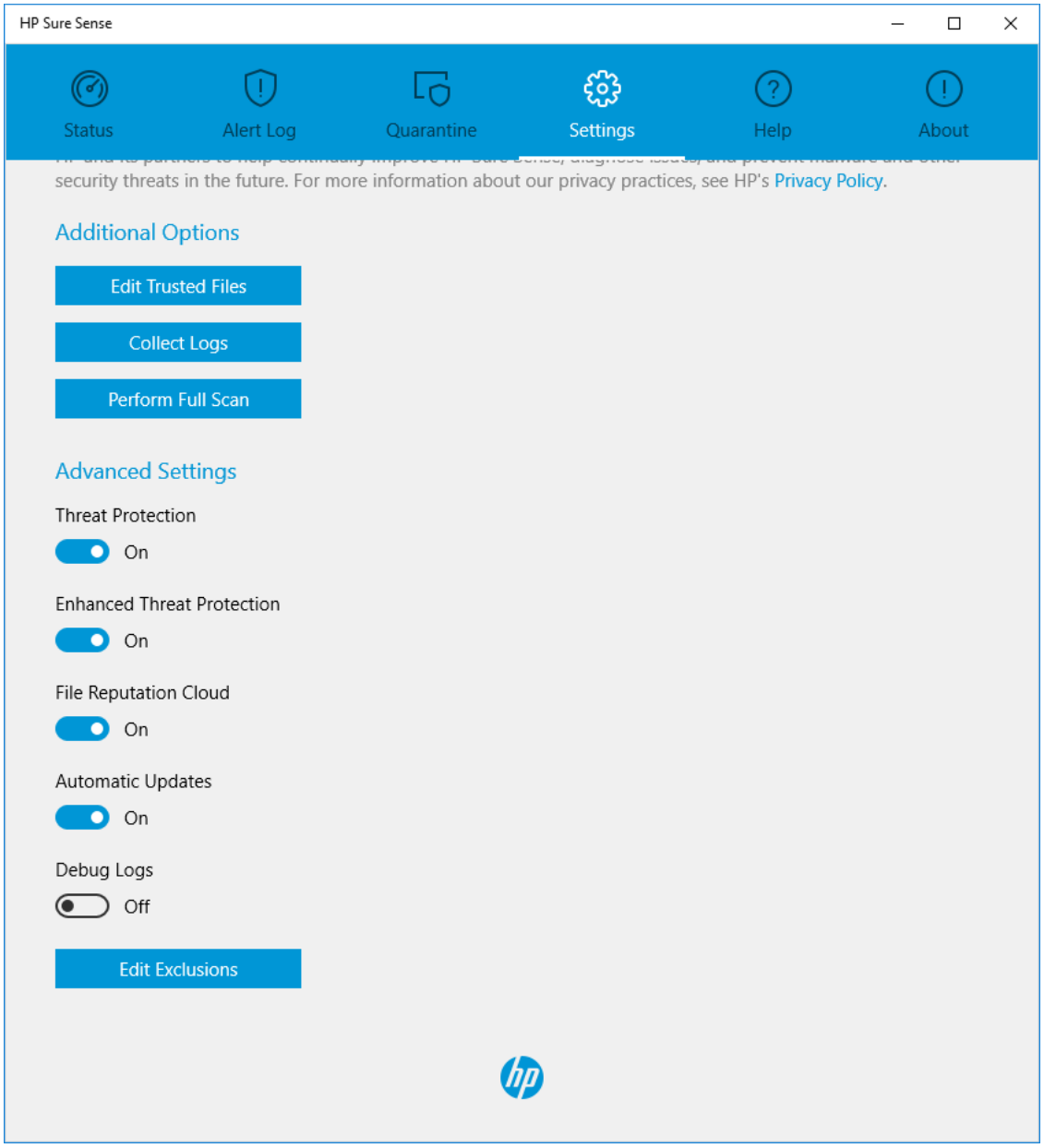

Figure 11: Settings page with Advanced Settings

The implemented settings are as follows:

- Preferences
  - Notifications – Defines whether all notifications (toasts) are displayed. This does not influence what is displayed on the Alert Log page.
  - Language – Defines the user interface language.
  - Customer Experience Improvement – Defines whether you participate in the Customer Experience Improvement program. When selected, threat and related event information is collected from your device.
- Additional Options
  - Edit Trusted Files – Click **Edit Trusted Files** to open the Trusted Files screen. From this screen, the list of files that have been selected to be trusted are displayed. These files were selected either from the Alert Log page or the Quarantine page.
  - Collect Logs – Click **Collect Logs** to collect logs and create a log file. The type of logs recorded is based on the Debug Logs setting.

- Perform Full Scan – Click **Perform Full Scan** to start a full scan on the computer. Once the full scan starts, the progress is indicated on the Status page. From the Status page, you can also pause, resume, or stop the full scan.

- Advanced Settings
  - Threat Protection – Defines whether HP Sure Sense is enabled or disabled. When disabled, Enhanced Threat Protection and File Reputation Cloud services are disabled and no longer displayed.
  - Enhanced Threat Protection – Defines whether behavioral analysis is performed on running processes. Threat Protection must be enabled for this setting to be displayed.
  - File Reputation Cloud – Defines whether File Reputation Cloud services are enabled. The File Reputation Cloud services includes a database of malicious and benign files. When enabled, HP Sure Sense uses the File Reputation Cloud services to add a second layer of protection. Threat Protection must be enabled for this setting to be displayed.
  - Automatic Updates – Defines whether HP Sure Sense is updated automatically.
  - Debug Logs – Defines whether extensive debug logs are recorded, in addition to the general logs.
  - Edit Exclusions – Click **Edit Exclusions** to open the Exclusions screen. This screen displays a list of folders and processes that are excluded from being scanned. From this screen, folders and processes can be added or removed from the list. For more information, see the Exclusion screen.

Trusted Files screen

The Trusted Files screen lists the files that were selected as a trusted file, where these files are excluded from being scanned. To open the Trusted Files screen, click **Settings**, and then click **Trusted Files** in the Additional Options section.

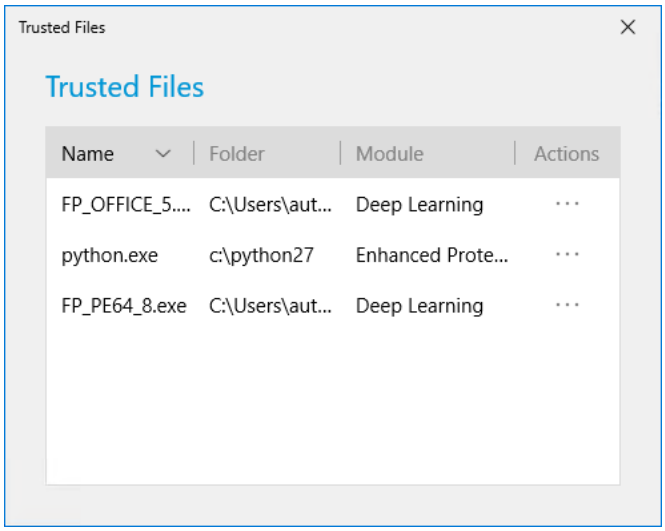

Figure 12: Trusted Files screen

The Trusted Files table includes the following information:

- Name – Names of the file.
- Folder – Path of the folder from where the file was originally scanned.
- Module – Name of the module that originally detected the file as a possible threat.

From this screen, you can do the following:

- Sort the information by clicking on column headings. The information in the table is sorted based on the selected column.
- Access the File Details screen to display additional information on a specific file (see Figures 15 and 16).
- Access the Process Details screen to display additional information on a specific process (see Figure 17).
- Remove a file from the Trusted Files table and quarantine the file.
- Remove a process from the Trusted Files table.

Help page

The Help page displays information about the HP Sure Sense product and answers questions on how to use the product.

Figure 13: Help page

About page

The About page displays additional information about your computer and the HP Sure Sense product installed.

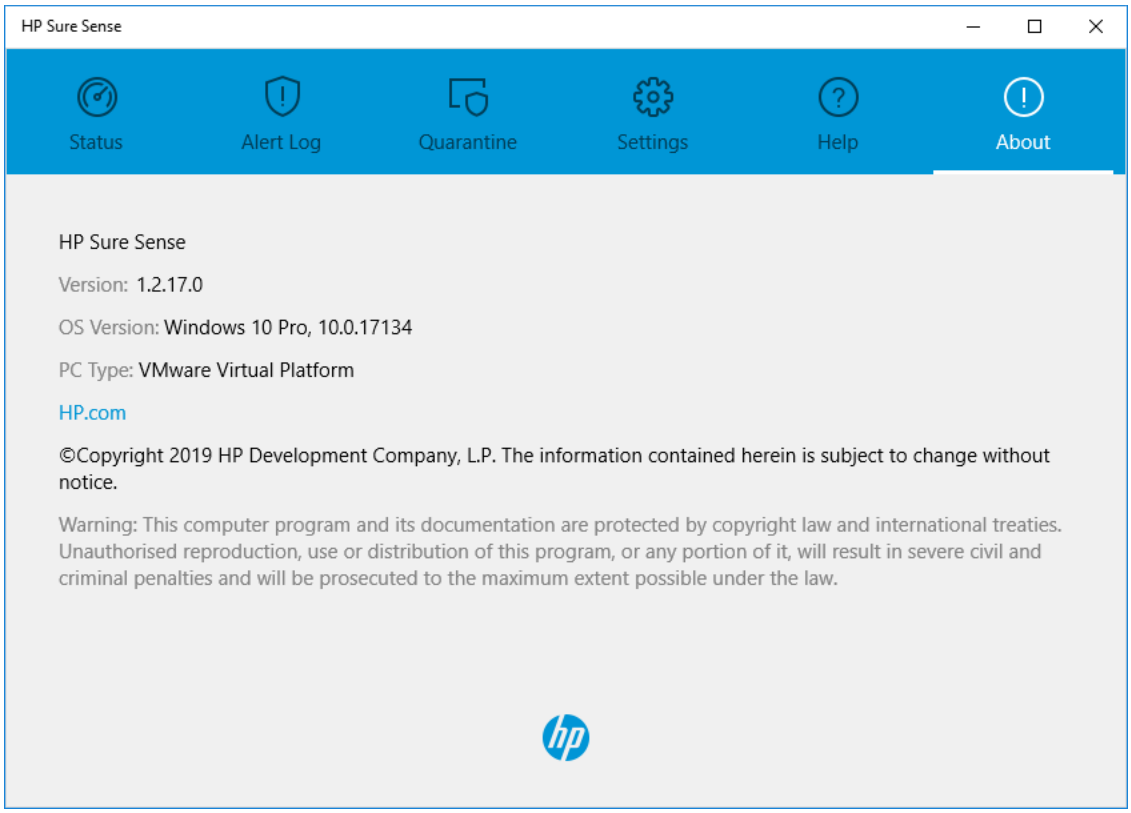

Figure 14: About page

This page includes the following information:

- Version – The version number of the installed HP Sure Sense.
- OS Version – The Windows operating system version number.
- PC Type – The PC type and model.

File Details screen

The File Details screen provides detailed information about files identified as malicious or selected as trusted. The File Details screen is displayed after selecting a file from the Quarantine page, Trusted Files table, or Alert Log page.

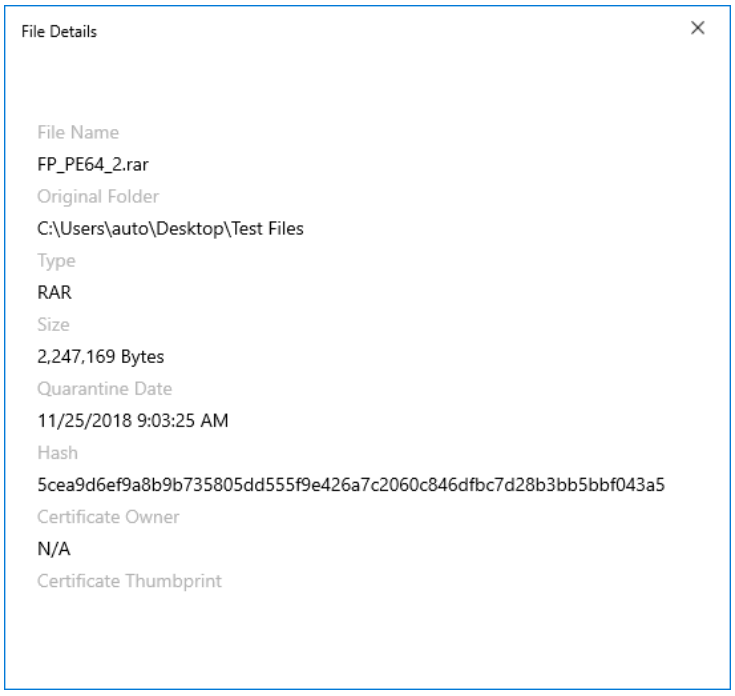

Figure 15: File Details screen for quarantined files

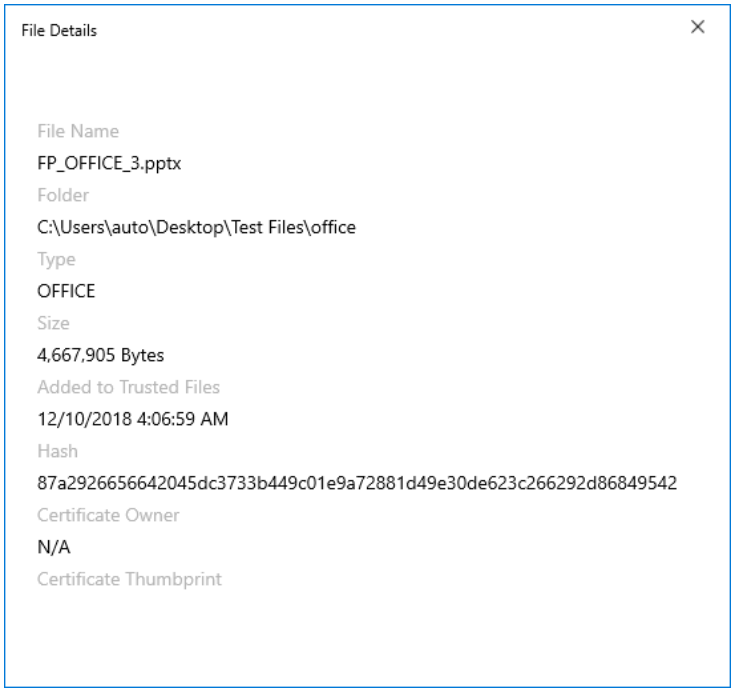

Figure 16: File Details screen for trusted files

These screens include the following information:

- File Name – Name of the file.
- Original Folder – Path of the folder from where the file was deleted and quarantined.
- Folder – Path of the folder where the trusted file is located.
- Type – The actual file type of the file. If the file name extension has been modified, the actual file type is displayed.
- Size – Size of the file.
- Quarantine Date – Date and time when the file was quarantined.
- Added to Trusted Files – Date and time when the file was added as a trusted file.
- Hash – SHA256 hash value of the file.
- Certificate Owner – For signed files, it identifies the Subject (owner) of the certificate.
- Certificate Thumbprint – For signed files, it identifies the thumbprint of the certificate.

Process Details screen

The Process Details screen provides detailed information about a process identified as malicious and the file that initiated the process. The Process Details screen is displayed after selecting a process-related entry from the Alert Log page or Trusted Files table.

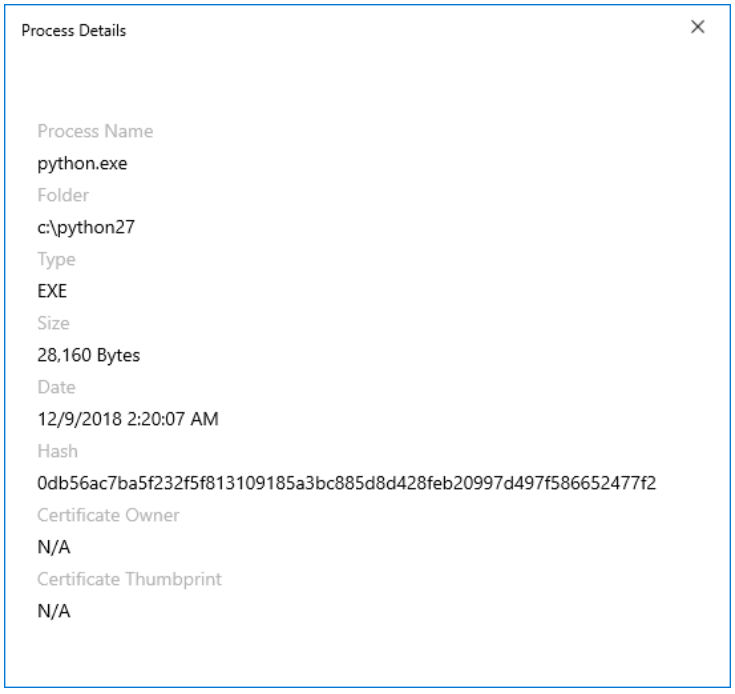

Figure 17: Process Details screen from the Alert Log page

Acronyms

- **AI** – Artificial intelligence
- **APT** – Advanced persistent threat
- **AWS** – Amazon Web Services
- **BIOS** – Basic Input/Output System (or host processor boot firmware)
- **CDN** – Content delivery network
- **CPU** – Central processing unit
- **DNN** – Deep Neural Network
- **PUA** – Potentially unwanted applications
- **PUP** – Potentially unwanted programs
- **SIEM** – Security Information and Event Monitoring
- **SMB** – Small and Medium Business

Appendix B: FAQ

What is HP Sure Sense?
HP Sure Sense harnesses the power of deep learning to deliver powerful malware protection from both known and never-before-seen malware. **HP Sure Sense can detect 99% of both known and unknown malware in as few as 20 ms.**

Legacy antivirus solutions have relied upon signature-based technologies to identify and stop malware. According to AV Test, over 350,000 new types of malware are created every day. This malware has never been more dangerous. Relying on frequent signature updates, as required by legacy malware solutions, is insufficient protection against a perpetual onslaught of novel, never-before-seen malware.

HP Sure Sense does not use signatures; instead, it uses the power of deep learning AI to provide real-time detection and prevention of malware threats and APTs. This proactive protection provides cutting-edge accuracy in real-time detection and prevention, protecting endpoints from both known and previously unknown malware.

Can SMB customers use HP Sure Sense, or is it just for enterprise?
HP Sure Sense offers tremendous value for both Small and Medium Business (SMB) customers and enterprise customers. While SMB customers may have not previously had access to advanced security tools, with HP Sure Sense, SMB customers have access to the same cutting-edge neural network protection available to enterprise customers. HP Sure Sense provides advanced protection out of the box without incremental subscriptions. Most importantly, HP Sure Sense can be a vital part of every business plan for resilience to get back to business as usual and mitigate lost revenue. HP Sure Sense is a vital part of your resilience plan.

How often does HP Sure Sense require updates?
The deep learning agent used by HP Sure Sense is so powerful that it only needs to be updated approximately once every three months, as opposed to the two to three times a day required by legacy antivirus solutions.

How do customers get HP Sure Sense?
HP Sure Sense will be available and built-in as an integral part of select HP Business PCs, without additional charge. HP Sure Sense is also available via web download for supported platforms.

In which regions and localizations will Sure Sense be available?
HP Sure Sense is expected to be available worldwide, subject to regulations, and limited by language support as follows:

- US – English
- BR – Brazilian Portuguese
- DE – German
- ES – Spanish
- FR – French
- IT – Italian
- JA – Japanese
- KO – Korean
- RU – Russian
- TW – Taiwan Chinese (Traditional)
- ZH – Chinese (PRC Simplified)

Is HP Sure Sense a hardware or a software technology?

HP Sure Sense is software. However, select HP Business PCs that feature HPs Endpoint Security Controller will enable administrators to employ HP Sure Run to add hardware enforcement to HP Sure Sense, ensuring that the software cannot be shut down by malware or users.

What is the impact of HP Sure Sense on system performance?

The HP Sure Sense agent that detects malware is lightweight, using less than 30MB of system resources and less than 1% of CPU when idle. HP Sure Sense does momentarily use higher levels of CPU during whole system scans and active file scanning, but does not meaningfully impact performance or battery life in our testing.

Does HP Sure Sense remove the need to have signature-based antivirus protection?

No – HP Sure Sense is not a replacement for conventional antivirus solutions. HP recommends running HP Sure Sense along with Windows Defender or other AV solution. Signature-based antivirus solutions are virtually 100% effective against malware for which they have signatures and provide a strong complement to HP Sure Sense, which is highly effective at protecting against never-before-seen malware.

The system performance impact of HP Sure Sense is very light, so there is little reason not to employ a strategy of layered security with both antivirus and deep learning.

Will customers be able to install HP Sure Sense on non-HP PCs?

At this time, HP Sure Sense will be exclusive to select HP Business PCs, Workstations, and Retail Point of Sale PCs.

How is HP Sure Sense managed?

HP Sure Sense will be manageable by the HP Manageability Integration Kit, as are our other HP security solutions.

---

[1] "The 2017 State of Endpoint Security Risk" from Ponemon Institute.

[2] "Playing Whack-a-Mole: Results of the 2017 SANS Threat Landscape Survey: Users and Endpoints Are Both Targets, Part of the Solution" by SANS Institute August 7, 2017.

[3] "Symantec 2018 Threat Report".

[4] "A new malware strain was discovered every 4.2 seconds in Q1 2017" G DATA Malware Trends 2017.

[5] "69% of organizations don't believe the threats they are seeing can be blocked by anti-virus software" Ponemon Institute.

[6] "Third Annual 2018 Cost of Data Breach Study: Global Overview" IBM Security and Ponemon Institute.

[7] Based on internal testing performed by HP, observing malware protection and remediation performance against a variety of malware types.