HP WOLF SECURITY

HP SURE SENSE

TECHNICAL WHITEPAPER

TODAY'S SMART IT DECISION MAKERS ARE WISE TO 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.

TABLE OF CONTENTS

INTRODUCTION

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. The HP Sure Sense proprietary deep learning algorithm instinctively recognizes malware and protects against never-before-seen attacks.

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.

HP Wolf Security for Business 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

Fileless attacks are expected to grow to 41% in 2021, that's a 24% growth since 2020,[1] and 68% of IT professionals expect their organization will be impacted by a fileless attack in 2020.[1] 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. In 2020, 80% of successful breaches are new or unknown attacks.[3] New malware emerges every 4.2 seconds.[4] Attacks are becoming more targeted, there was a 91% increase in cyber-attacks with more employees working from home.[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.

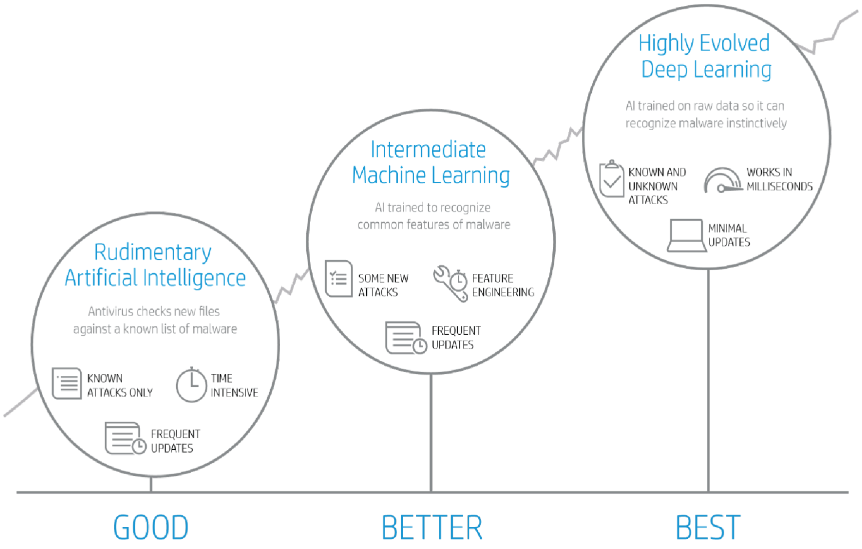
Rudimentary Artificial Intelligence
Antivirus checks new files against a known list of malware
KNOWN ATTACKS ONLY
TIME INTENSIVE
FREQUENT UPDATES
Intermediate Machine Learning
AI trained to recognize common features of malware
SOME NEW ATTACKS
FEATURE ENGINEERING
FREQUENT UPDATES
Highly Evolved Deep Learning
AI trained on raw data so it can recognize malware instinctively
KNOWN AND UNKNOWN ATTACKS
WORKS IN MILLISECONDS
MINIMAL UPDATES
GOOD
BETTER
BEST

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.

Machine learning—Certain features and criteria may be misleading

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 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.

HP Sure Sense is trained with hundreds of millions of malicious and legit files using deep learning. The outcome of the training is the HP Sure Sense lightweight module that is distributed in select HP PCs. The module is also available as a Softpaq download.

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.

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 to create a security tool that instinctively recognizes a never-before-seen threat.
- 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: HP Sure Sense users can add to the trusted file list using the HP Wolf Security 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 Wolf Security Console Quarantine tab.

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

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.

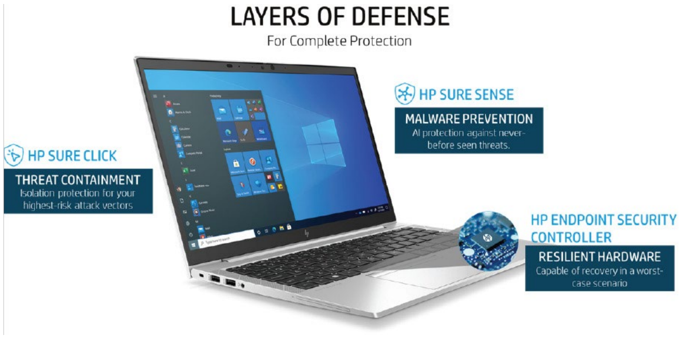
LAYERS OF DEFENSE
For Complete Protection
HP SURE SENSE
MALWARE PREVENTION
AI protection against never-before seen threats.
HP SURE CLICK
THREAT CONTAINMENT
Isolation protection for your highest-risk attack vectors
HP ENDPOINT SECURITY CONTROLLER
RESILIENT HARDWARE
Capable of recovery in a worst-case scenario

Figure 2: 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

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–Acronyms.

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 at: http://www.hp.com/wolfsecurityforbusiness

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

APPENDIX A—ACRONYMS

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 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 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 Third Annual Study on the State of Endpoint Security Risk from Ponemon Institute, January 2020.

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

[3] https://www.globaldots.com/blog/80-of-successful-breaches-are-from-zero-day-exploits.

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

[5] https://www.zdnet.com/article/covid-19-fuels-cyber-attacks-exposes-gaps-in-disaster-recovery/
N/A. Remote work changing landscape, IT Leader View, May 2020.

[6] HP Sure Start Gen3 is available on HP Elite products equipped with Intel 7th generation processors.

[7] HP Sure Start Gen4 is available on HP Elite and HP Pro 600 products equipped with 8th generation Intel or AMD processors.

Learn more at: http://www.hp.com/wolfsecurityforbusiness

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

HP WOLF SECURITY