HP Proactive Security

WHITEPAPER

Contents

Executive Summary

Cyberattacks against user endpoints continue to increase in sophistication. Most companies rely on traditional, signature-based antivirus solutions. However, it is difficult to ensure that signature lists are kept current across all of an organization's client devices. At the same time, hundreds of thousands of new malware variants are released every day, many leveraging evasion techniques designed to bypass even the most recently updated antivirus software.

More advanced anti-malware technologies are available but are often inaccessible to small and medium businesses due to their complex and labor-intensive management process. As a result, it has become very hard for companies without internal cybersecurity expertise to ensure that all end-user devices are protected, particularly while balancing employee needs to work offline, remotely, and across different devices and platforms.

This document details the security capabilities of HP Proactive Security and how it was specifically developed to empower medium-sized organizations that want the benefits of artificial intelligence-based protection, without impacting the user experience or overloading IT operations. These organizations want to improve their endpoint protection position but lack sufficient in-house security expertise and/or available administrative bandwidth to manage such solutions. HP Proactive Security provides this opportunity.

The HP Proactive Security service delivers a combination of artificial intelligence (AI) and endpoint virtualization technology to defend against risky inbound content from email or web downloads. In addition to protection against known endpoint malware threats, the solution is also designed to protect against previously unknown, undetectable threats, or "zero-day" malware.

In addition to powerful AI-based protection, HP Proactive Security adds an additional layer of government-grade application isolation protection. By isolating applications for email attachments, downloads from non-whitelisted websites, file and executable downloads, in separate hardware-enforced micro-virtual machines (micro-VMs) on the user's PC, HP Proactive Security not only prevents the devastating effects of a cyberattack, but isolates high-risk activity without impacting the end-user experience, or the way users access their data. The isolated application is monitored during operation to ensure latent threat behaviors are identified, recorded and shared back to a central cloud-based security controller before being deleted from the system when the micro-VM is closed.

Additionally, HP Proactive Security protects employees from the most common type of breaches: phishing attacks. HP Proactive Security's Identity Protection technology blocks the ability to enter passwords on credential harvesting websites after a user has clicked on a phishing link in an email, chat client, PDF or other file.

Based on telemetry data collected from attempted attacks, HP Proactive Security provides actionable insights to customers. These insights enable IT teams to monitor the protection state of their devices from a unified dashboard, view reports, and receive alerts of blocked or isolated threat activity through the powerful HP TechPulse analytics platform.

Most importantly, unlike pure software solutions, HP Proactive Security is a managed service that can help customers address the administrative and management challenges presented by advanced protection solutions. HP Security Experts work on the customer's behalf to implement and manage configuration and security policies, including management of the cloud security controller and protection policies as well as whitelists, trusted sites and quarantine settings. Once onboarded, HP Security Experts monitor device security status and notify the customer whenever threat activity has been blocked.

---

1 HP Proactive Security requires Windows 10 Pro or Enterprise version 1909 or later and Microsoft Internet Explorer, Google Chrome, or Chromium are supported. HP services are governed by the applicable HP terms and conditions of service provided or indicated to Customer at the time of purchase. Customer may have additional statutory rights according to applicable local laws, and such rights are not in any way affected by the HP terms and conditions of service or the HP Limited Warranty provided with your HP Product. For full system requirements, please visit www.hpdaas.com/requirements.

Threat Landscape

Organizations face a wide range of challenges with the continually evolving security threat landscape. With an estimated 350,000 new malware variants released every day,[2] protecting against these threats is increasingly challenging. Endpoint security is critical, but current approaches are falling short.

Traditional, signature-based AV solutions help protect against known threats but tend to be ineffective against unknown, zero-day threats and modern evasion techniques. Today, over 60 percent of new malware infections bypass, disable or are ignored by traditional anti-virus.[2] Zero-day threats are four times more likely to compromise organizations and the count of new ones is expected to double in the coming year.

Even when organizations have the advanced security tools they need, they do not always have the expertise or capacity to deploy and manage them effectively. One recent report indicates an estimated shortage of 3.5 million cybersecurity experts worldwide with 53 percent of companies[3] reporting a shortage of cybersecurity skills. Many medium-sized organizations lack not just the expertise, but the budget to staff, train and deploy advanced protection solutions. Addressing the needs for endpoint security is now a major focus for IT.

The weakest link in an organizations' security has often been the endpoint. In the past year alone, an estimated 68 percent[2] of companies experienced a significant security breach that was initiated from an end-user endpoint device. Phishing attacks – when users are tricked into providing their network or PC credentials or passwords to cybercriminals – are the top threat action taken against small and mid-sized businesses today, making up over a third of attempted cyberattacks.[4] Sixty seven percent of breaches are caused stolen credentials,[4] costing global businesses an average of $3.86M per attack, and up to $8.36M in the US.[5]

Most organizations already have multiple layers of security:

- Cloud Access Security Broker and Cloud Antivirus: solutions that help identify known malware that affects cloud application and help enforce security policies which are outside of your network.
- Site Categorization SSL inspection and content analysis: proxy and firewall controls that help identify known malware that is attempting to enter your network.
- Network AV, Sandboxing, and Security analytics: network controls to identify known and potentially unknown malware that has penetrated your perimeter and is on your network.
- Endpoint antivirus and application whitelisting: host controls for your endpoint devices that will stop known malware.

These layers are needed to protect your enterprise, but many of them focus on minimizing the impact of an infection rather than prevention.

Traditional Antivirus (AV) solutions

Traditional AV protection solutions depend on a continuously updated signature database to identify all known malware programs. The limitation of traditional antivirus solution architecture is that if a threat has not been seen previously, or if it has been disguised using common evasion techniques, then malware can easily slip past undetected. This is becoming increasingly challenging, as the rate of new malware creation has rapidly grown to hundreds of thousands of new malicious software "products" per day.

Typical AV solutions (e.g., legacy McAfee and Symantec and the free alternative, Microsoft Defender) are based on maintaining a database of known bad or malicious software and constantly updating that database as a new virus or malware is discovered. This approach means there must be a "patient zero" that falls victim to the attack before an identification and response can be made available.

---

[2] Ponemon Institute 2020 State of Endpoint Security Risk sponsored by Morphisec, January 2020
[3] ESG Global IT Survey 2018-2019 https://www.esg-global.com/blog/the-cybersecurity-skills-shortage-is-getting-worse
[4] Verizon's 2020 Data Breach Investigations Report (DBIR)
[5] IBM Cost of a Data Breach Report 2020

To be truly effective for known bad or malicious software:

- The AV solution provider must update their databases daily, at a minimum, and
- Companies deploying the AV solution must also update or refresh their solution continuously

This ensures that the software is accessing the latest database of known/bad software for detection.

Although many traditional AV solutions now incorporate some machine learning capabilities, they tend to be more error prone, and customers must choose between high-sensitivity and high false positive rates, or low-sensitivity and higher rate of missed threats.

Next-Generation AV solutions

Next-generation AV solutions are a category of products that rely almost entirely on machine learning. Examples include Cylance and CrowdStrike Falcon Pro. Their detection technology is not tied to a known malware database. Instead, these solutions use machine learning and other software algorithms to identify unknown malware and other malicious actors.

Although these solutions provide a solid alternative to traditional premium endpoint antimalware suites and better zero-day protection a common disadvantage of such products is they tend to require periodic tuning to reduce the number of false positive events from common IT solutions and other harmless business applications.

HP Proactive Security's Sure Sense Advanced[6] feature implements similar capabilities but also incorporates a highly sophisticated deep learning neural network engine. The advantage of solutions such as Sure Sense Advanced is that the deep learning engine does not require continuous updates to be effective.

In fact, the device does not have to be connected to the Internet to be protected. For example, if a user plugs in a USB key containing a zero-day threat, even if having been offline on vacation for weeks in a remote location, the user device will still be protected.

The deep learning engine is designed to detect and classify the malicious threat, even if it has not previously been cataloged, using a process called deep classification. Deep classification works across file-based threats, fileless threat vectors such as code injection, and also ransomware, which frequently exploits weaknesses in traditional antivirus solutions. In addition, this automatic analysis is further enhanced by a cloud-based reputation service, which allows customers to gain access to additional details on known threats blocked by the product.

Some less-advanced solutions also run the risk of incorrectly categorizing large numbers of harmless applications as malicious, known as "false positives." False positives can negatively impact company operations and performance by erroneously blocking good software and flooding IT teams with false alarms, to which they must respond. As these solutions have matured and been refined, the risks have been reduced, but they persist.

Because the response to false positive events can be labor-intensive, and because solution tuning can be a very difficult process, it is important to consider manageability and administrative costs when selecting an endpoint protection solution. Because HP Proactive Security delivers Sure Sense Advanced as a managed service, customers can take advantage of the back-end policy and controller management capabilities, which also includes built-in reporting and management by industry-certified HP Security Experts.

HP Proactive Security's Multilayered Solution

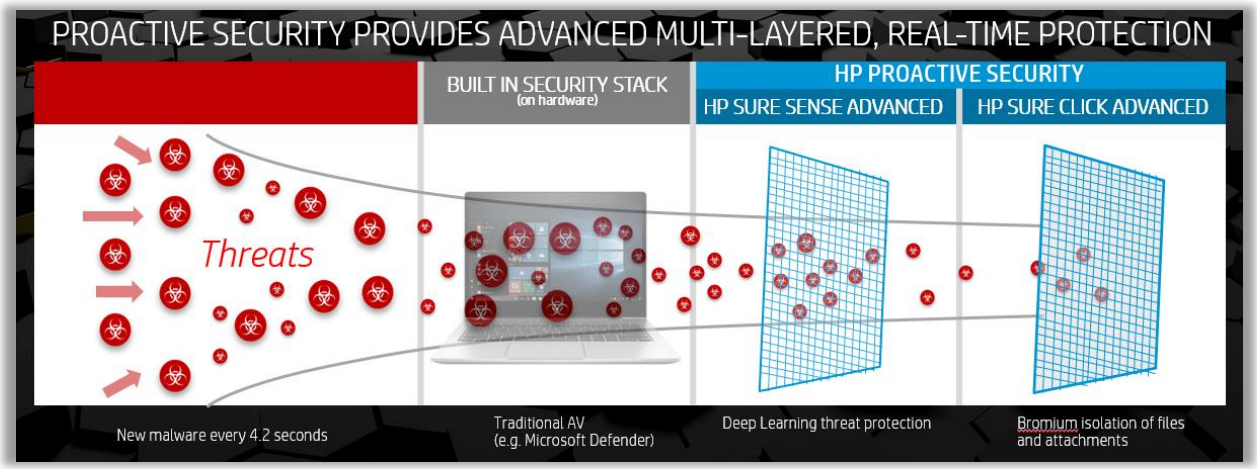
While AI-based solutions are a step forward when compared with traditional AV solutions, no solution can guarantee it will capture 100 percent of the malware it encounters. This is why many organizations continue to adopt integrated, multi-level security solutions.

---

[6] HP Sure Sense Advanced is included with HP Proactive Security. For system requirements, please visit www.hpdaas.com/requirements.

HP Proactive Security supplements deep learning AI with automatic isolation of untrusted documents downloaded from email attachments or websites on Windows 10. All untrusted downloaded attachments and documents are opened automatically in isolation, so even very well-hidden zero-day threats which have evaded the customer's other protective solutions can be contained without harm to the device or its data.

The isolation enables users to read, edit and save the content using native Word, Excel and other applications, and at the same time ensures that threats executed in isolation are protected down to the hardware level and will not be able to infect the endpoint or spread across the network.



Thus, users can safely work with content from customers, suppliers and business partners, without changing how they access the documents or concern about their security. Detailed in the following sections are the primary components of HP Sure Sense Advanced, HP Sure Click Pro,[7] the HP TechPulse[8] analytics portal, all supported by security policy management and infrastructure control from HP's industry-certified Security Experts.

HP Sure Sense Advanced

HP Sure Sense Advanced harnesses a deep learning AI engine to enable real-time malware protection for Windows 10 devices. The deep learning engine of the HP Sure Sense Advanced AI system was trained to recognize and distinguish malware from harmless files with an advanced neural network trained against malware samples. Similar to the way a human can easily identify the difference between a cat and a dog, just as a human who has not seen every breed of cat or dog can tell the difference between the two, the Sure Sense Advanced deep learning engine can readily recognize even very-carefully disguised malware files and detect file-less threats.

The deep neural network enables the engine to automatically recognize both known and previously unseen malware types, and is designed to continuously adapt to new threats without signature updates – and with a low rate of false positives

HP Sure Click Pro

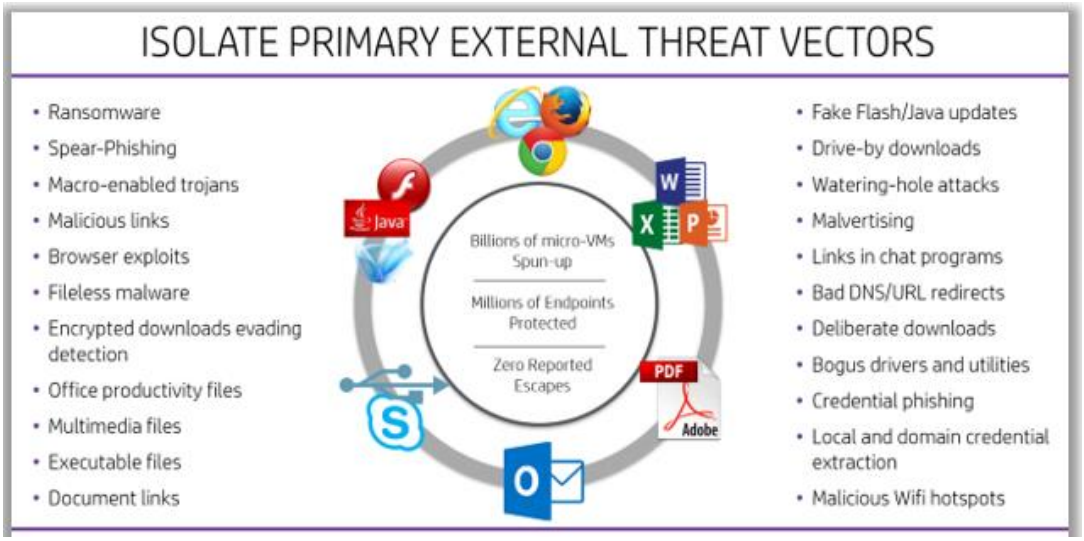
HP Sure Click Pro, also included with the HP Proactive Security Service, is a threat isolation and analytics solution powered by HP Bromium technology. HP Sure Click Pro uses hardware-enforced virtualization technology as a last line of defense to isolate threats that may have bypassed other endpoint defenses. Since the most frequent source of attack against end-user PCs occurs through downloads from malicious websites, email attachments and infected links, HP Sure Click Pro opens untrusted files in isolated containers that allow the malware to detonate inside a hardware-enforced virtual machine at the CPU level.

[7] HP Sure Click Pro is included with HP Proactive Security and requires Windows 10 Pro or Enterprise and Microsoft Internet Explorer, Google Chrome, Chromium, Mozilla Firefox and new Edge are supported. Supported attachments include Microsoft Office (Word, Excel, PowerPoint) and PDF files, when Microsoft Office or Adobe Acrobat are installed.
[8] HP TechPulse is a telemetry and analytics platform that provides critical data around devices and applications. The reporting in HP TechPulse focuses on identifying threats and their source. HP TechPulse is GDPR and ISO 27001compliant.

Files that are opened from a trusted or 'allowed' Internet domain, as specified by the organization, open in the native application, such as Microsoft Word or Excel. If they are not from a trusted, whitelisted source, they open in isolation – running normally but prevented from causing damage.

The way Sure Click Pro isolation works is that it effectively blocks all access between the protected application and the device host operating system, eliminating the risk of damage from opening an infected file. Best of all, this happens automatically in the background, seamless to the end user, so there is no impact to user workflows and people can work the way they normally do.

For example, a resumé that comes in an HP email from another HP employee would open as a trusted source. However, a resumé that is attached in an email from an unknown sender outside of the company would open in the isolation container. With HP Sure Click Pro, the user can view, edit, print and save the file without releasing the threat onto their PC.

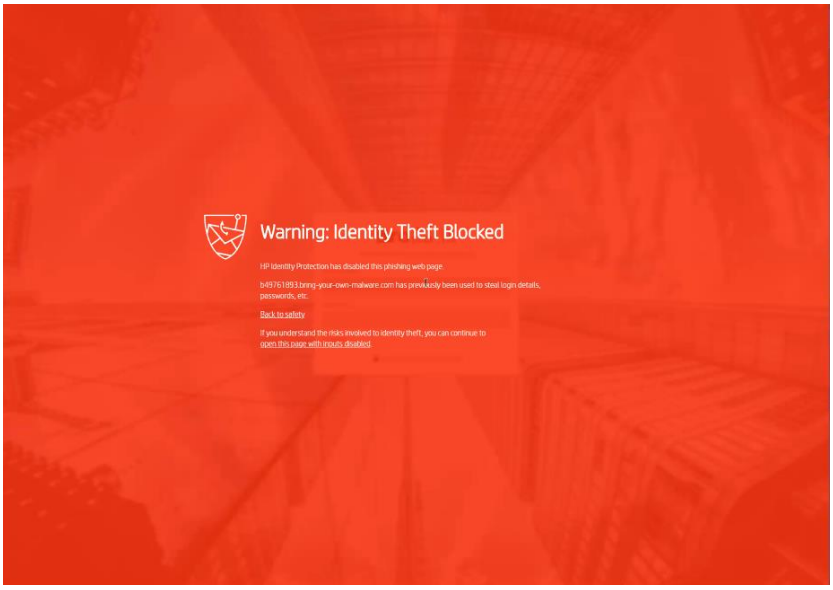


Sure Click Pro not only prevents cyberattacks but also monitors threat activity within the micro-VM, and sends a full analysis of the malware kill chain mapped to the MITRE ATT&CK™ framework[9] to the Sure Click Pro cloud-based controller so isolated threat events can be monitored in HP TechPulse.

Additionally, Sure Click Pro provides credentials theft protection, and can prevent entry of user passwords on fake logon websites (aka credential harvesting websites), after a user has clicked on a phishing link in an email, chat client, PDF or other file.

When a user visits a site and is prompted to enter login credentials, Sure Click Pro conducts a reputation and domain analysis behind the scenes to determine the safety of the site. For legitimate, known safe sites, users will be free to enter their credentials as usual with no impediments from the software.

[9] MITRE does not claim ATT&CK enumerates all possibilities for the types of actions and behaviors documented as part of its adversary model and framework of techniques. Using the information contained within ATT&CK to address or cover full categories of techniques will not guarantee full defensive coverage as there may be undisclosed techniques or variations on existing techniques not documented by ATT&CK



But if the site is a known phishing site, or is detected, based on its attributes as malicious, a red warning window will appear over the page as the user attempts to enter their password, preventing the site from capturing their credentials. The user may then either safely close the browser window or proceed to view the site with all data capture fields inactivated.

If a site has a suspicious rating, but cannot be confirmed to actually be malicious (examples might include unusual intranet sites), a gray warning window will appear with a recommendation for users check the site and avoid entering credentials. If the user knows the site is safe, they may choose to proceed, which will add the site to the whitelist stored in the user's local browser extension store, removing the impediment from future visits. HP can also adjust the policy for a customer to "trust" their internal websites, so the warning message does not appear to end users.

Security Analytics and Reports

HP TechPulse is HP's telemetry and analytics platform that provides critical data around devices and applications, putting deep learning at IT's fingertips so they can provide employees with the right PC, software and services to succeed. HP TechPulse proactively identifies issues such as unprotected devices to enable remediation and minimizes threats by actively monitoring the security posture of the organization, helping them optimize their IT spending and effort.

Through the HP TechPulse dashboard, HP Proactive Security customers have access to several security-related reports for all managed devices – including non-HP devices. These reports are designed to show the endpoint protection state for Sure Click Pro, Sure Sense Advanced, as well as reports on whether traditional endpoint antivirus and firewall protection are active on managed Windows PCs.

In addition, HP TechPulse includes reports for Sure Start and Sure Recovery activity, to give customers a more holistic view of the protection features in their HP devices, and even offers Windows Defender users a summary view of device protection states and threat events.

The reports available to HP Proactive Security customers include:

- Company Security Compliance
- Device Compromised
- Device Security Compliance
- Driver Inventory
- Hardware Inventory
- Hardware Warranty
- Incident Resolution
- Non-Reporting Devices
- Sure Click Pro Security
- Sure Recover Activity
- Sure Recover Settings
- Sure Sense Advanced Security
- Sure Start System Integrity
- Windows Defender Endpoint Protection

Management by Industry-Certified Security Experts

In addition to highly advanced protection technology, HP Proactive Security was designed to enable small- and medium-sized organizations to gain the full benefits of enterprise-grade security, but without the added staff and budget normally required to manage such solutions, and at a competitive value to software-only solutions.

HP Security Experts have been certified in a wide range of security areas, including multiple SANS Global Information Assurance Certification (GIAC) specialties, Certified Information Systems Security Professional (CISSP), IT Infrastructure Library (ITIL) certification and other areas. As part of the service, HP Security Experts configure the controller policies for customers, manage policies, whitelists, trusted site and email domain lists; they also provide security incident notifications whenever endpoint threats are detected. These make advanced security accessible even to companies with limited in-house security expertise and are a key differentiator relative to more complex, self-managed solutions.

HP Security Leadership

HP has a more than 20-year track record of clear security leadership in the PC industry, investing in protecting PCs from the most damaging and least visible threats. In 1999, HP co-founded the Trusted Computing standards group, and in 2003, was first to install Trusted Platform Modules (TPM) in PCs. In 2005, HP was first to introduce cryptographic signing of BIOS firmware updates, driving the industry forward by working with the National Institute of Standards and Technology (NIST) to create BIOS security standards.

HP introduced a security-focused embedded controller to the PC platform in 2013, providing a secure computing environment separate from the main CPU that can be used to enforce critical platform security functions. The embedded controller is used to enable the platform to self-heal the firmware if it has been tampered with and to implement HP Sure Start, which enables the BIOS and other firmware to be cryptographically verified on every boot.

In 2016, HP extended its investment, leadership and focus in securing endpoint devices by entering into a formal OEM relationship with Bromium, Inc. The following year, HP successfully began shipping an OEM version of Bromium containment software on millions of enterprise-class devices branded as HP Sure Click.

HP Sure Run functionality, introduced in 2018, uses the embedded controller to create a cryptographic heartbeat between the controller and the host OS, enabling security-critical host OS processes to be monitored and corrective action taken upon failure. Sure Recover was also added to the platform in 2018 to enable systems to be able to securely re-install the host OS in the event that it is corrupted. The OS image can be downloaded from a cryptographically signed image stored on the Enterprise network or Cloud, or from a special Flash memory chip that is protected by the embedded controller. Thus, HP systems are uniquely able to reinstall the host OS in just a few minutes to facilitate recovery from destructive malware that has deleted critical on-disk information such as the Master Boot Record or Partition Table.

In 2019, HP introduced Sure Admin, an industry leading solution to enable secure management of BIOS configuration data using Public Key cryptography, enabling a much more scalable and secure solution than the traditional BIOS password, allowing for both remote administration over the network and secure local user access to BIOS configuration menus.

In addition to below-the-OS security capabilities, HP created an endpoint security stack that offers industry leading protection of the host OS that uses the hardware virtualization capabilities of modern CPUs to isolate high-risk activities such as web browsing and opening of documents from Internet sources.

Due to the success of Sure Click, HP acquired Bromium in the fall of 2019. Subsequently, HP created a new Global Business Unit, HP Security, with the legacy Bromium team leading the new unit.

ISO 27001:13 Certification

HP Proactive Security has achieved ISO27001 certification, as defined by the International Organization for Standardization (ISO) to ensure that rigorous end-to-end processes and controls are in place to protect customer data. As the security of information systems and business-critical information needs constant measurement and management, ISO is responsible for the development of several internationally recognized standards for products, services, and systems.

The ISO 27001 family of standards specify the requirements for establishing, implementing, maintaining and continually improving an Information Security Management System (ISMS) within the context of an organization. HP has achieved ISO certification across the Remote Monitoring and Management Services environment, for both Managed Print and Personal Systems Services.

The latest ISO 27001:13 certification is awarded upon the completion of an external audit by an accredited external certification body and is asset based (information, processes, people, and technology). HP's ISO 27001:13 certification by KPMG verifies its commitment to deliver operational continuity and data.

Conclusion

Securing end point devices is critical in the rapidly evolving IT landscape. Because the client endpoint is the front line of defense against cybersecurity attack, HP embarked on a mission to address these risks more than twenty years ago. Its legacy of innovation in device-threat detection and protection both in and above the hardware level has informed the design of applications such as HP Proactive Security and HP TechPulse.

By taking a protection-first approach, the HP Proactive Security managed service helps small and medium-sized businesses defend against cyberattacks without disrupting employee productivity or increasing IT workload. The service provides advanced protection that is monitored and managed by certified HP cybersecurity experts.

Company data and devices are secured with multiple layers of proactive protection applying advanced deep learning and isolation technologies to protect endpoints and reduce risk.

The administration of such solutions is commonly the highest single factor in the total cost of ownership for endpoint security. This managed service solution provides the benefits of an advanced security solution, including actionable insights, without the complexity or need to expand in-house security expertise.

Because HP manages the complex technologies on the customers' behalf, customers who would normally be unable to take advantage of the advanced endpoint protection technology can gain their full benefit without the additional cost. It also frees IT to work on strategic projects, instead of chasing false positives and security threats and empowers employees to work with their choice of common productivity applications without fear of compromising their IT networks, providing increased productivity and peace of mind for all levels of the organization.

4AA7-7561ENW – February 3, 2021