HP WOLF PRO SECURITY EDITION

ADVANCED ENDPOINT SECURITY

TECHNICAL WHITEPAPER

HP WOLF PRO SECURITY EDITION PROVIDES ENTERPRISE LEVEL SECURITY,

REQUIRING LOW-TOUCH IT, SUPPORTING SEAMLESS DEPLOYMENT AND MANAGEMENT.

TABLE OF CONTENTS

INTRODUCTION

The evolution of employee workplace and workstyle continues to fuel the quantity and complexity of malware and cyberthreats. This threat landscape has grown intelligent and persistent in the ability to bypass traditional PC security. One successful attack can bring business operations to a halt, resulting in financial impacts that could cripple or destroy a business.

Small and Medium sized companies require the same advanced PC security as larger organizations that have robust IT departments, to protect against today's threat landscape.

HP Wolf Pro Security Edition provides enterprise level security, requiring low-touch IT, supporting seamless deployment and management. Leveraging HP Sure Click Pro and HP Sure Sense Pro in a single console offering, it is optimized for Small and Medium companies.

HP WOLF PRO SECURITY EDITION – DEFINED

HP Wolf Pro Security Edition[2] is a comprehensive security solution designed to protect small to medium businesses against malware and browser-based attacks—without the need of IT or Policy management. HP Wolf Pro Security Edition will detect, halt, and quarantine harmful files on your PC without user intervention.

HP Wolf Pro Security Edition uses a unique multi-technology approach by interlacing *Virtualization, Anti-Phishing, Artificial Intelligence,* and *Machine Learning* to complement one another in a unified user console via a group Security policy. Softwareupdates and new policies are deployed via HP-Cloud, delivered behind the scenes—no user actions are required.

HP Wolf Pro Security Edition can be purchased, preinstalled on select HP Notebooks. A 1-year or 3-year license includes the software, HP-Cloud delivered updates and support from the HP Support Desk[1,2].

HOW HP WOLF PRO SECURITY EDITION WORKS

There are three types of protection provided by HP Wolf Pro Security Edition:

Protection #1: Threat Containment
HP Wolf Pro Security Edition includes HP Sure Click Pro. During your PC's most vulnerable tasks (web browsing and opening email attachments), HP Wolf Pro Security Edition leverages the core capabilities of HP Sure Click, using Application Isolation, to strengthen security. Rather than trying to recognize malware, HP Sure Click opens untrusted websites and files in isolated virtual containers—called micro-virtual machines (micro-VMs). If there is malicious code present, these micro-VMs trick the malware into thinking it's running inside your computer, when in fact, it's trapped.

Inside the hardware-enforced micro-VM, malware is unable to affect your PC, access your files, or even get into other browser tabs. When the browser tab or Microsoft Office file is closed, the entire micro-VM is automatically discarded—and the malware trapped within is deleted. No special training or additional quarantine procedures are needed; just close the browser tab or file and the malware is gone.

The confidence to browse securely

Included in HP Wolf Pro Security Edition, as a feature of HP Sure Click Pro, is the Chromium-based HP Sure Click Secure Browser. The secure browser will always open websites in their own isolated micro-VMs, allowing you to explore the Internet safely without having to learn a new browser or deal with restrictive whitelisting. Any malware you may encounter is isolated from the rest of the system and destroyed when the browser tab is closed.

Protection for common files

Malware can also be hidden in seemingly innocent files, downloaded from the web or sent as email attachments. That's why HP Wolf Pro Security Edition is extending protection beyond the browser, offering protected viewing for PDFs and full editing for Microsoft Word documents within a micro-VM.

Unfamiliar files can be opened and are protected with the same hardware-enforced isolation that quarantines suspect websites. If the file is compromised, the malware is contained and prevented from infecting the PC.

Protection #2: Malware Prevention

HP Wolf Pro Security Edition utilizes the core capabilities of HP Sure Sense to provide real-time detection and prevention of zero-day threats (threats that exploit unknown computer security vulnerabilities) and advanced persistent threat (APT) attacks. The proactive protection provides accuracy in detection and real-time prevention, protecting your PC from any threat (known and unknown).

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

- Endpoint layers: Extensive array of protection layers, including heuristic analysis, signature-based detection, emulation, generic detection, and signatures-leveraging machine learning models.
- File Reputation Cloud Services: The File Reputation services provide a fast and scalable infrastructure in the cloud that adds a second layer of classification. Using these services, files can be re-classified in a second layer of validation using the database of intellectual information on known files and the right verdict is updated in real-time.

Protection #3: Identity Protection

Identity Protection aims to protect users from submitting credentials to credential harvesting attempts hidden in a phishing link in an email, chat client, PDF, etc.

Identity Protection is independent of the Threat Containment (Isolation) feature in HP Wolf Pro Security Edition. Its sole function is to protect users when using a web browser. Currently, the browsers supported by HP Wolf Pro Security Edition's Identity Protection feature are:

- Google Chrome
- Edge Chromium
- HP Secure Browser

How it protects the user

When a user clicks a link in email, webmail, chat client, PDF, etc., it will open as normal in a browser. Behind the scenes, an HP extension is examining the Document Object Model (DOM), contents of the web page and its structure, to determine if the web page contains a login form/page/option. In a parallel process to the page loading, the full URL is queried against the HP Cloud Service to determine if it is a known bad, known good, or an unknown site.

- If HP Cloud encounters a known bad reputation score, a status icon for the browser extension will turn red:
- If HP Cloud encounters a positive reputation score, the status icon for the browser extension will turn green:
- If HP Cloud encounters an unknown rating, the status icon for the browser extension will turn gray:

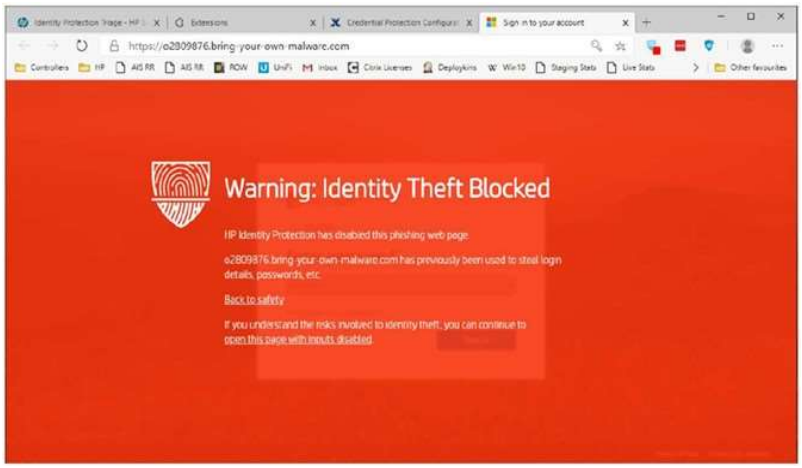
This icon serves as a status notification in the Browser and does not require user action.

As a web page may take some time to finish loading (accessing offsite assets such as tracking cookies, advertisements, etc.), the parallel background check does not interfere with the page load and has time to complete.

When a user begins entering credentials in a dialog box on a web page, HP Wolf Pro Security Edition will act upon entry of the first character of the password or credential data. If a user does not try to enter credentials on a known bad website, the blocking technology will not activate.

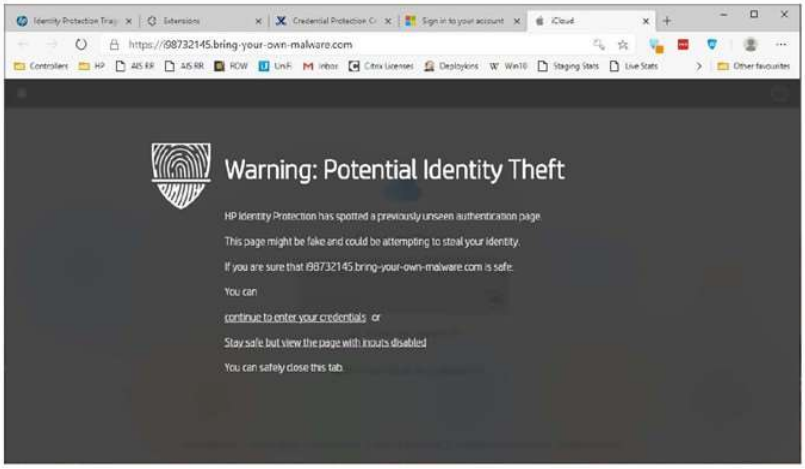
Known bad page

If the web page is known as bad, the HP Wolf Pro Security Edition (extension) status icon will appear RED. On entry of the first character of a password or credential data, a RED transparent overlay will launch over the top of the web page. The accompanying dialogue explains that this is a known bad website and HP Wolf Pro Security Edition is blocking the user from entering credentials on this site. The user can continue to view the page with all inputs blocked or they can exit to safety (by closing the tab).



Unknown page

If the web page is unknown or potentially malicious, the HP Wolf Pro Security Edition (extension) status icon will appear GRAY. On entry of the first character of the password or credential data, a gray overlay will cover the web page and explain that this site COULD be a phishing site and the user should proceed with caution.



The user can continue to view the web page with inputs disabled or can opt to continue to enter their credentials. In this case, the site is added to a local whitelist (site has been "whitelisted") stored in the user's browser extension store.

HP WOLF PRO SECURITY EDITION ACTIVATION

When HP Wolf Pro Security Edition is purchased and preinstalled at the HP factory, the following process is used to activate the software:

- The user will power-on the new HP PC preinstalled with HP Wolf Pro Security Edition.
- The new PC steps through HP's automated setup ('Out of Box Experience' or OOBE) and software license acceptance.
- When OOBE is completed, depending on user choices during OOBE, the PC may need a reboot.
- When the user opens the HP Secure Browser, HP Wolf Pro Security Desktop Console, or initiates a reboot.
- A one-time banner will appear (e.g., text may vary depending on version): "Thank you for using HP Wolf Pro Security Edition. Your PC is now protected." (prompting the user to Click 'Accept').
- Activation is complete.

UPDATING HP WOLF PRO SECURITY EDITION

HP Wolf Pro Security Edition will be delivered as a preinstalled software application on select HP computers (Notebooks, Desktops and Workstations)2. As a cloud-based security solution, updates are delivered by HP's Cloud. These updates will include new security policies, updated threat profiles and any enhancements HP chooses to apply. No user-action is required to receive updates, other than a restart to activate the new code.

THE DASHBOARD

Unified Security Console

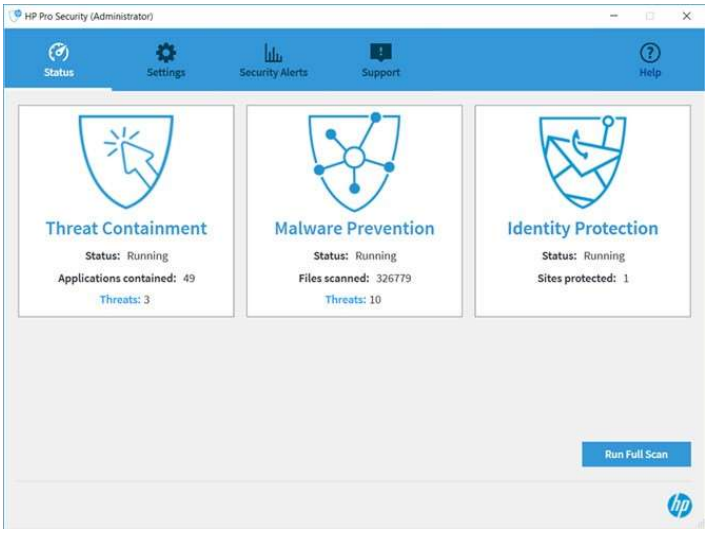
HP Wolf Pro Security Edition offers a simple dashboard from which the user can access Status,Settings, Security Alerts, and HP Support. The dashboard is designed to combine all the Security protections into four easy-to-use selectable pages.

Note for non-technical users: If a user never opens or accesses the HP Wolf Pro Security Edition dashboard, the protection and settings are installed and configured at the HP factory during the production process—the user is protected regardless if they access the dashboard or not. This ensures the small business user will be protected regardless of their Security or Software knowledge.

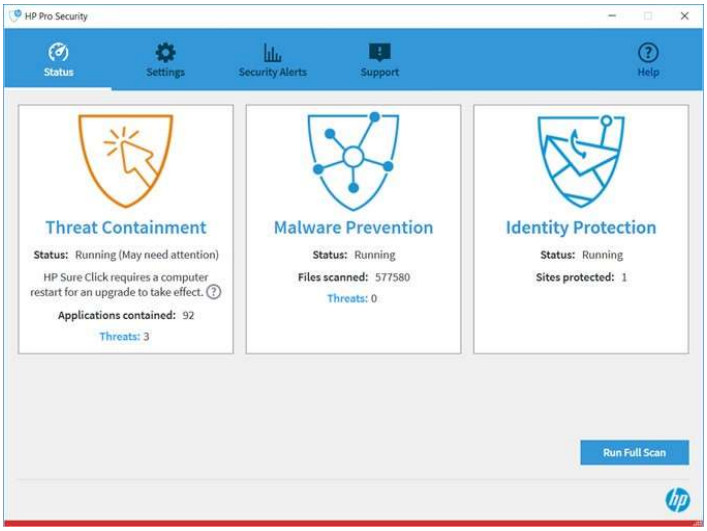
Status

The HP Wolf Pro Security Edition dashboard can be accessed via the Windows Start menu (icon). By default, it will display a status page, presenting four icon categories available for selection by the user. Additionally, the large icons of the three protection mechanisms are displayed: Threat Containment, Malware Prevention, and Identity Protection. Additionally, there is an icon to 'Run Full Scan' and restart and rescan the entire PC. (Note: HP Wolf Pro Security Edition contains an 'agent' that constantly scans and monitors pre- existing and new files. The user can reset and initiate a new scan in the event they wish torestart and rescan all files on the PC.)

The icons for Threat containment can change color to indicate if a new security policy or update has been added to the software. In most cases all the updates for HP Wolf Pro Security Edition are automatically deployed from the HP Cloud and no user intervention is required, other than an occasional restart.



Yellow icon, indicating a feature or policy has been updated—informing the user a PC restart is required.



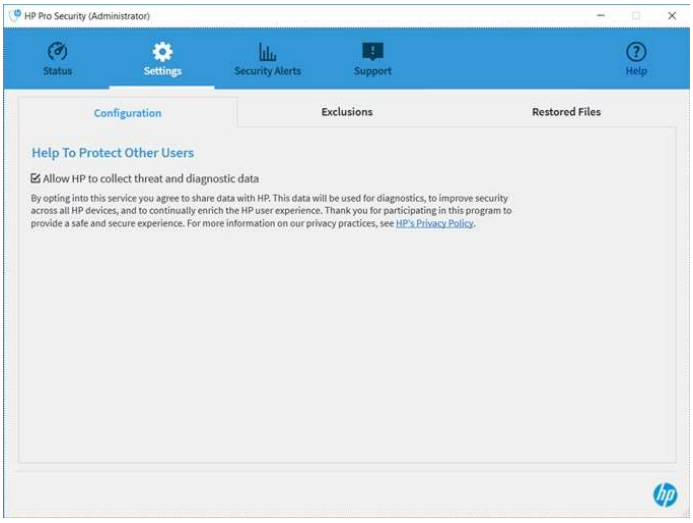
Settings

Upon selecting the Settings icon, HP Wolf Pro Security Edition reveals three tab pages of features within.

Configuration

Tab #1, or the Configuration tab, enables HP Wolf Pro Security Edition to help protect your PC, along with other users. HP recommends that users 'opt in' or check this box to enable thefeature. When malicious events are encountered by a HP Wolf Pro Security Edition user, the data is shared with the HP Cloud. By sharing this threat data, HP can record the data and prevent other users from experiencing the same attacks.

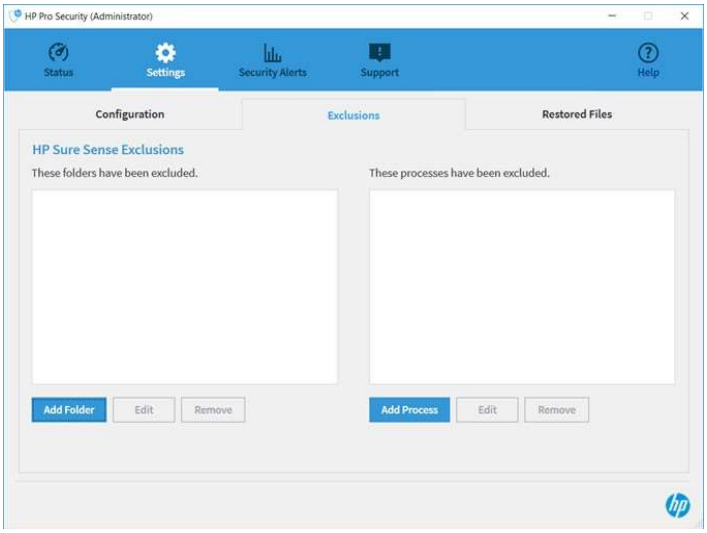
Note: No personal or user data is sent to the HP Cloud when opting into this feature—only data captured from an attack is recorded.



Exclusions

Tab #2, the Exclusions tab, enables users to select folders and processes that are known safe. Adding a folder (containing a file or multiple files) or a process name to either list on this page will be bypassed (considered 'safe') when HP Wolf Pro Security Edition performs security scans.

For example, if a work environment has created a set of custom applications, HP Wolf Pro Security Edition may view the unique files as a threat. Adding this custom application (or associated files) to the exclusions list will exclude the file from any future malware scans.



Restored Files

Tab #3, the Restored Files tab, maintains an active list of files HP Wolf Pro Security Edition initially flagged as malicious; however, the user can elect to mark the file as safe. Typically, a safe file will have come from a trusted source and/or the user took action to mark it as safe.

Note: Files that were flagged as unsafe have been captured and logged on the Security Alerts page (a description of the Security Alerts page is included in this file).

Security Alerts

Selecting the Security Alerts icon will reveal a list of file names and/or websites that were quarantined and flagged as malicious.

Information on the files, against which, HP Wolf Pro Security Edition took protective action will display with the following column headers:

- Time: Month, Day, Year, and Time the threat was detected.
- Source: An icon and file name will be presented in the Source column, indicating the file type categorized and quarantined as a potentially malicious file. Typically, the icon will inform the user if the suspicious file was a document (e.g., Word, Excel) or an encounter via web browser, flagging a website attempting to steal credentials.
- Type: Some malware types can be categorized (e.g., Ransomware) and if capable, HP Pro Security will display information in this column.
- Response: The action taken by HP Wolf Pro Security Edition when encountering a malicious file or website.
- Action: The action " ... " button provides multiple user options.

– On a Quarantined response, the user is presented four options:

  • Details of the file: The location, time, and hash value.

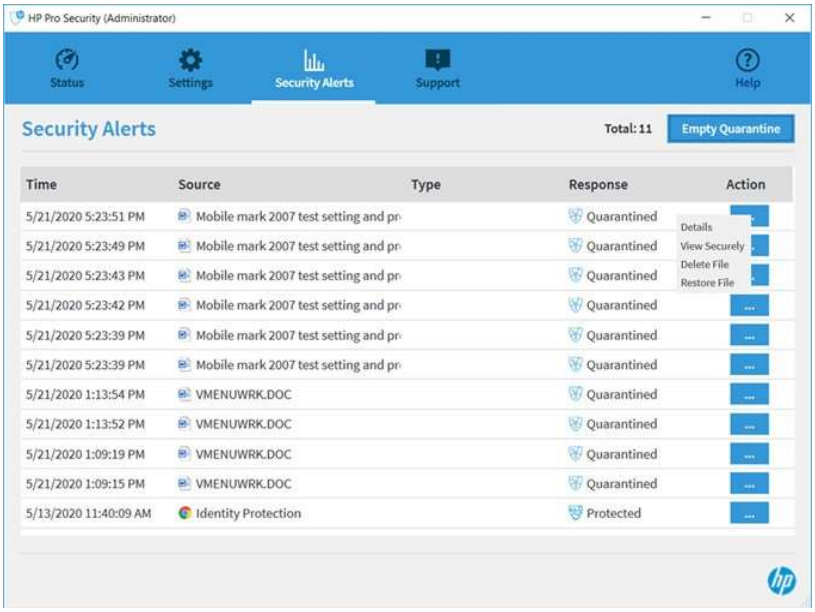
  • View Securely: To open and view the file in a protected virtual machine and determine if the file is safe or should remain quarantined.

  • Delete the file from PC.

  • Restore: Changes the file to a 'trusted' state.

– On a Protected response – Identity Protection (HP Wolf Pro Security Edition's anti-phishing protection), the user can view the following details of the website that was flagged as unsafe:

  • View Details of the file: The URL location, time, and hash value.



Support

The Support tab on the HP Wolf Pro Security Edition dashboard provides multiple information points.

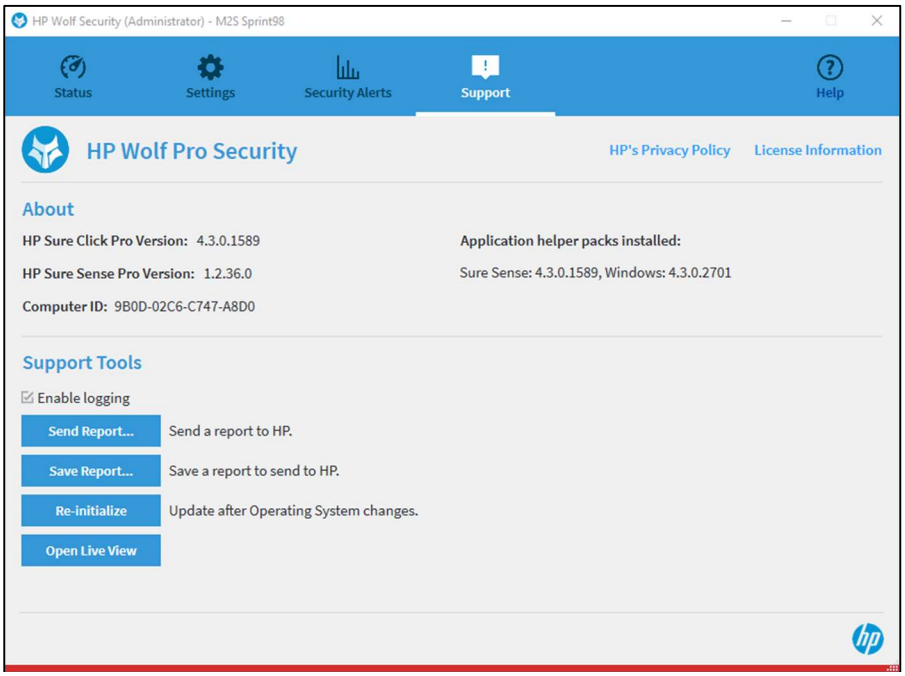
About

HP Sure Click Pro and HP Sure Sense Pro are unique applications, which have been combined and interlaced to complement one another—presented on this unified console. Each application may receive updates separately from the HP Cloud. The version numbers will not be synchronized or the same as each Security element can receive unique updates.

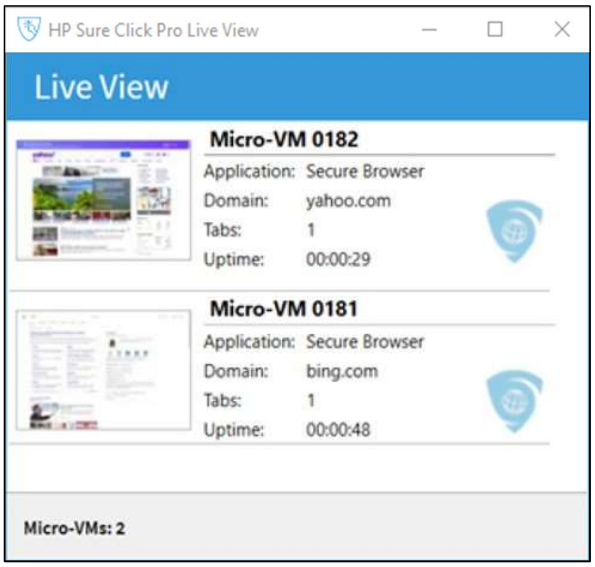
The Computer ID shown on the Support page is unique to each PC, indicating the PC contains a licensed copy of HP Wolf Pro Security Edition installed.

Support Tools

Enable logging will create a .zip log file in a user-defined PC directory location (e.g., on the 'Desktop') for the purpose of providing information to HP 3LS support. The Send Report button will email the log file to HP Support agents.



Open Live View is an advanced feature when using the HP Secure Browser. Pressing the Open Live View button will create a dialog window (shown below) and display web pages that are viewed in a secure browser virtual environment on the PC. The web pages viewed in browsing mode are isolated from the PC's memory and hard drive.



Links to HP's Privacy Policy and License Information are also included on the Support page.

POLICIES AND SETTINGS

HP Wolf Pro Security Edition comes preconfigured from the factory with a cloud-based security policy configuration. In simpler terms, it is a 'headless' application that does not require IT management or back-end console controls. The software self-updates when connected to an active Internet connection. User-defined policies are not required to be created or configured, making it optimal for small to medium business environments.

As outlined in this whitepaper, there are settings for Folder and File Exclusions—that can be defined by the user—to identify files and processes determined to be safe, to prevent HP Wolf Pro Security Edition from categorizing these files as malware.

CONCLUSION

Building on more than a decade of HP's Security leadership, HP Wolf Pro Security Edition is prepared to fight complex attacks. Cyberthreats are indifferent to company size. No longer will cyber-attackers only target large enterprises. All categories of business are under attack and a growing number of attackers have set sights on small and medium businesses (SMBs).

HP research reports most small businesses are consistently under attack and may not have the resources or tools to effectively protect their PCs.[3]

HP has exhibited leadership in PC Security products for years, providing Security solutions that protect your device, data, and identity. Building on more than a decade of HP's Security leadership, HP Wolf Pro Security Edition is prepared to protect against the growing number of complex cyberattacks.

HP Wolf Pro Security Edition addresses the challenges small to medium businesses may encounter—insufficient IT personnel, budget constraints to invest in Security, and a lack of resources to understand how to best protect against cyberattacks.

HP Wolf Pro Security Edition is advanced cyberthreat protection targeting environments that do not have a budget to support a robust IT infrastructure.

Learn more hp.com/go/computer security

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

1. HP PC System Requirements
   a. Window 10 Pro 64, Windows 10 Enterprise or Windows 10 Enterprise LTSC (64-bit only)
   b. 11th Generation Intel® Core™ i7 processor (i7-8665U, i7-8565U models); 11th Generation Intel® Core™ i5 processor (i5-8365U, i5-8265U models); 11th Generation Intel® Core™ i3 processor or AMD Ryzen or newer processors
   c. Minimum 8GB memory

2. HP Wolf Pro Security Edition (including HP Sure Click Pro and HP Sure Sense Pro) is available preloaded on select SKUs and, depending on the HP product purchased, includes a paid 1-year or 3-year license. The HP Wolf Pro Security Edition software is licensed under the license terms of the HP Wolf Security Software - End-User license Agreement (EULA) that can be found at: https://support.hp.com/us-en/document/ish_3875769-3873014-16 as that EULA is modified by the following: "7. Term. Unless otherwise terminated earlier pursuant to the terms contained in this EULA, the license for the HP Wolf Pro Security Edition (HP Sure Sense Pro and HP Sure Click Pro) is effective upon activation and will continue for either a twelve (12) month or thirty-six (36) month license term ("Initial Term"). At the end of the Initial Term you may either (a) purchase a renewal license for the HP Wolf Pro Security Edition from HP.com, HP Sales or an HP Channel Partner, or (b) continue using the standard versions of HP Sure Click and HP Sure Sense at no additional cost with no future software updates or HP Support."

   The HP Wolf Pro Security Edition supports a limited tool set that can be used by the HP Manageability Integration Kit which can be downloaded from http:// www.hp.com/go/clientmanagement.

3. Source: 2019 Verizon Data Breach Investigations Report; 2018 State of Cybersecurity in Small & Medium Businesses

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

HP WOLF SECURITY

4AA7-7373ENW, May 2021