



HP WOLF PRO SECURITY SERVICE



HP WOLF SECURITY



SERVICE OVERVIEW

Service Benefits

- Stop previously unknown zero-day attacks and credential theft with reinforcing layers of defence.
- Secure your endpoints with enterprise-grade isolation technology.
- Help protect employees from cyberthreats without creating barriers to their productivity.

Service Highlights

- Protection-first approach to endpoint security with real-time, multi-layered defence.
- Expertly monitored & managed by industry-certified security professionals.
- Timely and actionable analytics and insights.

HP Wolf Pro Security Service helps keep your organisation safe with a multi-layered, endpoint security service that is the right size for growing and maturing businesses.¹ With a protection-first approach to managing endpoint security, it reduces your risk of attacks and gives users the freedom to work without disrupting their productivity or increasing IT workload.

HP Wolf Pro Security Service integrates reinforcing layers of enterprise-grade anti-malware protection. It combines advanced, next-generation antivirus software based on the latest AI technology like deep learning, credential theft prevention and defence-grade isolation technologies, with real-time actionable insights and ongoing threat monitoring by cybersecurity experts.

FEATURES AND SPECIFICATIONS

Protection

HP Wolf Pro Security Service provides advanced, multi-layered protection for computing endpoints.

The artificial intelligence system used in HP Wolf Pro Security Service leverages a combination of machine learning, deep learning and other techniques, enabling it to readily recognise even very carefully disguised malware files, as well as detect fileless threats based on their characteristics, rather than relying on unique signatures. The solution can successfully detect never-before-seen, zero-day malware, in addition to stopping known threats, and it does so without any updates needed to the client.

FEATURES AND SPECIFICATIONS (CONTINUED)

Additionally, HP Wolf Pro Security Service protects employees from the most common type of breach: credential phishing attacks. HP Wolf Pro Security's Identity Protection feature blocks users from entering passwords on credential-harvesting websites which a user may have accidentally launched from a phishing link in an email, chat client, PDF or other file.

HP Wolf Pro Security's enterprise-grade isolation technology is the last line of defence, containing even invisible threats that may have evaded the customer's other endpoint defences and rendering them harmless. This hardware-enforced isolation protection allows email attachments, file downloads and even content from USB drives to be safely opened, edited, printed and saved within their own secure micro-virtual machine. While open, the applications are automatically monitored for threat activity and the HP Wolf Security Controller provides a full analysis of the attack kill chain for threat incidents to help you to better understand the nature of the threat and protect against future attacks.

By combining these complementary advanced technologies, HP Wolf Pro Security Service provides real-time, multi-layered proactive protection to your devices.

Insights

HP Wolf Pro Security Service provides actionable insights to customers through the HP Wolf Security Controller, a powerful security analytics platform.² Your IT teams can monitor the protection status of devices, view reports and receive alerts about unprotected devices and blocked threat activity – all from a unified, cloud-based dashboard.

Expert Monitoring & Management³

Unlike pure software solutions, HP Wolf Pro Security Service is delivered as a monitored service. HP Security Experts implement and manage configuration and security policies, including ongoing security policy enforcement of the threat quarantine, on your behalf. Once devices are onboarded, HP Security Experts monitor the device security protection status and conduct forensic and kill chain analyses on previously unseen, zero-day threats to help you to better protect against future attacks.

Category	Features
Protection	<ul style="list-style-type: none"> HP Sure Sense Pro AI-based threat prevention for Windows 10⁴ HP Sure Click Pro⁵ attachment and download isolation for Windows 10 HP Identity Protection blocks accidental disclosure of user passwords on credential theft websites
Security Analytics	<ul style="list-style-type: none"> Device protection dashboard HP Sure Click Pro and HP Sure Sense Pro threat data Detailed device protection state information Full threat kill chain analysis mapped to the MITRE ATT&CKTM framework⁶
Ongoing Service Management	<ul style="list-style-type: none"> Controller setup, tuning and policy enforcement Threat analysis and insights Quarantine and exclusions management Security agent health investigation Security agent update deployment
Other Features	<ul style="list-style-type: none"> SIEM integration via syslog feed

DELIVERY SPECIFICATIONS

Customers must install the security and analytics client software on managed devices. An Internet connection is required to access analytics and reporting, and to receive policy updates and software upgrades. These software agents do not need an Internet connection in order to provide protection once set-up has been completed. User-sensitive data, including credentials, files, content, and personal data, will not be captured. The data collected will be stored in a secure cloud repository.²

HP will provide HP Wolf Security Controller access to security insight information, including a dashboard, reports, incidents and more.

Certified HP Security Experts will proactively monitor and manage the endpoint security for you, including tuning and enforcing the security policy; analysing the incidents when a true positive threat is detected; managing the security agent's updates; investigating problems around the agent's health; and more.

An HP Service Expert will provide first-level customer support and work with HP internal teams, including Security Experts, to resolve issues you report. HP Service Expert availability is as follows:

North America: English support is available Monday to Friday (excluding HP holidays) from 6:00 a.m. to 6:00 p.m. MT.

Latin America: English and Spanish support is available Monday to Friday (excluding HP holidays) from 7:00 a.m. to 6:00 p.m. GMT - 5.

Europe, Middle East, and Africa: English, French, and German support is available Monday to Friday (excluding HP holidays) from 8:00 a.m. to 6:00 p.m. CET.

Asia Pacific and Japan: English support is available 24 hours a day across the region. English and Japanese are supported for Japan from 9:00 a.m. to 9:00 p.m. Japan Standard Time, 7 days a week (excluding HP holidays).

Customer responsibilities

- Provide the required information so that HP can set up the customer account.
- Deploy the Wolf Pro Security Service agent on your managed devices.
- Request to add or remove whitelisted website download sites, exclusions and email domain settings (for file attachment isolation, AI-based malware protection and credential theft prevention).
- Request to add or remove internal company IP address ranges not subject to isolation.
- Request or approve release or exclusion of quarantined or blocked files.
- Log on to the HP Wolf Security Controller portal to view dashboards, reports and incidents.
- Review security reports and respond as necessary.



SYSTEM REQUIREMENTS

HP Wolf Pro Security supports systems running Windows 10 operating systems that run on supported Intel® or AMD processors. For the most up-to-date system requirements, please visit <https://www.hpdaas.com/requirements>.

Network requirements

An Internet connection is required for communications between the managed device and the cloud management service.

Prerequisites

To use the service, it needs to be registered after purchase following the instructions from HP. During the onboarding process, you will be required to provide information needed to set up the accounts and security policies.

SERVICE LIMITATIONS

HP Wolf Pro Security Service is not an ongoing, real-time monitoring service. HP Sure Sense Pro and HP Sure Click Pro automatically block or isolate untrusted or malicious content, ensuring protection on your devices. HP Wolf Pro Security Service does not include remediation or mitigation services in the event of a breach. Mitigation and remediation services are available separately from HP partners.

TERMS AND CONDITIONS

[HP Care Pack terms and conditions](#) may apply if the service is purchased as a HP Care Pack. [HP TechPulse terms and conditions](#), [HP Personal Data Rights Notice](#) and [HP Privacy Statement](#) are all applicable to the service.

FOR MORE INFORMATION

Contact your local HP sales representative or channel partner for details or visit <https://www.hp.com/uk-en/services/pro-security-service.html>

- 1 HP services are governed by the applicable HP terms and conditions of service provided or indicated to the 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 a complete list of system requirements, please visit <https://www.hpdaas.com/requirements>.
- 2 HP does not track or monitor details that identify which URLs a user visited. The reporting focuses on identifying threats and their source in the HP Wolf Security Controller. The HP Wolf Security Controller is GDPR and ISO 27001 compliant. HP Wolf Security Controller is not available as a stand-alone product and requires HP Wolf Pro Security Service. For full system requirements, please visit <http://www.hpdaas.com/requirements>. HP services are governed by the applicable HP terms and conditions of service provided or indicated to the customer at the time of purchase. The 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.
- 3 The threat analysis by HP Security Experts is a forensic process that is available after a malware event has been blocked or isolated by the HP Wolf Pro Security software agent. It is not a "real-time", 24 x 7 monitoring service. For more information on this service feature, please consult the HP Wolf Pro Security Service Definition document. The HP Wolf Pro Security Service agent automatically isolates untrusted or malicious content, ensuring protection before the analysis. Also, neither plan includes remediation or mitigation services in the event of a breach.
- 4 For a complete listing of Windows 10 supported versions, please refer to <https://www.hpdaas.com/requirements>. Please note that Windows 7 and 8.1 are not supported by HP Wolf Pro Security Service.
- 5 HP Sure Click Pro technology is included with HP Wolf Pro Security Service and requires Windows 10 Pro or Enterprise. 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. For more details, please see <https://www.hpdaas.com/requirements>.
- 6 MITRE does not claim ATT&CK enumerates all possibilities for the types of actions and behaviours 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.

Sign up for updates
hp.com/go/getupdated



Share with colleagues



Rate this document



© Copyright 2021 HP Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

4AA7-4656EEE, May 2021, Rev. 5



HP WOLF SECURITY