

HP Proactive Security



Service benefits

- Stop previously unknown, zero-day attacks and credential theft with reinforcing layers of defense.
- Secure your endpoints with government-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 defense.
- Expertly managed by industry-certified security professionals.
- Timely and actionable analytics and insights.

Service overview

HP Proactive Security helps keep your organization safe with a multi-layered, endpoint security service right-sized for medium businesses.¹ With a protection-first approach to managing endpoint security, it reduces your risk from attacks and gives users the freedom to work without disrupting their productivity or increasing IT workload.

Proactive Security integrates multi-layered, government-grade anti-malware protection that combines deep learning, credential theft prevention and government-grade isolation technologies with actionable insights and management by cybersecurity experts—delivered as a managed service.

Features and specifications

Protection

HP Proactive Security provides advanced, multi-layered protection for computing endpoints including HP Sure Sense Pro and HP Sure Click Pro.²

The deep learning-based protection technology of HP Sure Sense Advanced was trained across hundreds of millions of malware samples enabling it to readily recognize even very carefully disguised malware files, as well as detect file-less 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.

Additionally, HP Proactive Security service protects employees from the most common type of breaches: credential phishing attacks. HP Proactive Security 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 Sure Click Pro uses government-grade isolation technology as a last line of defense to stop even invisible threats that may have evaded the customer's other endpoint defenses.

HP's hardware-enforced isolation protection allows email attachments, file downloads, and even content from USB drives to be safely opened, edited, printed and saved. While open, the applications are automatically monitored for threat activity. HP's TechPulse analytics console also provides a full analysis of the attack kill chain to help you better understand the nature of the threat and protect against future attacks.

Features and specifications (continued)

By combining these complementary advanced technologies HP Proactive Security provides real-time multi-layered proactive protection to your devices

Insights

HP Proactive Security provides actionable insights to customers through HP TechPulse, a powerful AI-based analytics platform.⁴ 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 dashboard.

Management

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

Access to Aon's CyQu

With HP Proactive Security, you have access to Aon's Cyber Quotient Evaluation (CyQu), an online cyber evaluation tool that provides you with an online score of your security profile. You also have an opportunity to opt-in to pursue preferential incident response retainers (\$0, one hour of consultation included) and a streamlined application process for cyber-insurance policies.⁴

Category	Features
Protection	HP Sure Sense Pro AI-based threat prevention for Windows 10 devices
	HP Sure Click Pro attachment and download isolation for Windows 10
	HP Identity Protection blocks accidental disclosure of user passwords on credential theft websites
Security reports	Company security compliance report
	Device compromised report
	Device security compliance report
	Non-reporting devices report
	HP Sure Click Pro security report
	HP Sure Recover activity report
	HP Sure Recover settings report
	HP Sure Sense Pro security report
HP Sure Start system integrity report	
Security incidents	Incident Resolution report
	HP Sure Click unprotected device
	HP Sure Click true positive threat isolated
	HP Sure Sense unprotected device
	HP Sure Sense threat prevented
	Windows Defender Endpoint Protection report
	Driver Inventory report
Hardware Inventory report	
Hardware Warranty report	

Ongoing Service Management	Controller setup, tuning and policy enforcement
	Threat analysis and insights
	Quarantine and exclusions management
	Security agent health investigation
	Security agent update deployment
	Deep-dive Sure Click Pro threat report ⁶
Other features	SIEM integration API for security incidents
	Aon's CyQu, an online cyber evaluation tool with options to opt-in to evaluate Aon's incident response and cyber insurance services ⁴

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 setup 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.⁷

HP will provide TechPulse portal access to security insight information, including a dashboard, reports, incidents, and more.

Certified Security Experts will proactively manage the endpoint security for you, including tuning and enforcing the security policy; analyzing 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 through Friday (excluding HP holidays) from 6:00 a.m. to 6:00 p.m. MT.
- **Latin America:** English and Spanish support is available Monday through 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 through 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 required information so that HP can set up the customer account
- Deploy the Proactive Security agents onto your managed devices
- Request to add or remove managed users and 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 TechPulse portal to view dashboards, reports, and incidents
- Review security reports and respond as necessary
- Complete the CyQu survey online^{4,5}



System requirements

HP Proactive Security does not support Android, macOS, Windows OS for RPOS, thin client devices, or VDI and other desktop virtualization deployments.

For the most up-to-date system requirements visit <https://www.hpdaas.com/requirements>

Third-party software requirements

Adobe Acrobat Reader DC is required to be the default application for PDF files.

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 Proactive Security 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 Proactive Security does not include remediation or mitigation services in the event of a breach. Mitigation and remediation services are available separately from HP partners, including Aon.

Terms and conditions

[HP Care Pack terms and conditions](#) may apply if the service is purchased as 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 partner or sales representative for details, or visit hp.com/proactive-security.

Sign up for updates
hp.com/go/getupdated



Share with colleagues

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 Sure Click Advanced technology is included with HP Proactive Security and requires Windows 10 and Microsoft Internet Explorer, Google Chrome, or Chromium. Supported attachments include Microsoft Office (Word, Excel, PowerPoint) and PDF files, when Microsoft Office or Adobe Acrobat are installed. HP Sure Click Advanced cannot be installed for Simplified Chinese languages.
3. HP Sure Click Pro technology 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. For more details, please see <https://www.hpdaas.com/requirements>.
4. HP does not track or monitor details that identify which URLs a user visited. The reporting focuses on identifying threats and their source in HP TechPulse. HP TechPulse is GDPR and ISO 27001 compliant.
5. Aon services are only available in the United States. Purchasers of the HP Proactive Security service in the U.S. receive the Aon CyQu self-assessment and security score. A \$0 retainer and one-hour consultation are included, with optional incident response services available from Aon. Your HP onboarding service representatives will provide instructions.
6. The threat analysis by HP Service Experts is a forensic process which is available after a malware event has been blocked or isolated by the HP Sure Click Pro software client. It is not a "real-time," 24 x 7 monitoring service. For more information on this service feature, please consult the HP Proactive Security Definition document. The HP Sure Click Pro client 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. Mitigation and remediation services are available as separate services from HP partners, including Aon.
7. Data is protected using SSL during data transfer from the device client to the web server. The data can only be accessed through the HP TechPulse web server. For more information on data privacy and protection practices, please consult the HP TechPulse data management FAQ.
8. For a complete listing of Windows 10 supported versions, please refer to the <https://www.hptechpulse.com/requirements>. Note that Windows 7 and 8.1 are not supported by HP Proactive Security.

© 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. Adobe and Acrobat are trademarks of Adobe Systems Incorporated. Google, Chrome, and Chromium are trademarks of Google Inc. Microsoft and Windows are registered trademarks of Microsoft Corporation in the United States and/or other countries.

