

HP Proactive Security and Proactive Management



Service benefits

- Protect your data and devices
- Guard against malicious websites and attachments
- Identify and address potential device issues before they become problems

Service highlights

- Advanced isolation technology guards against malware
- HP TechPulse analytics provide security and device health insights and reports
- Aon CyQu assessment helps evaluate your security position

Service overview

HP Proactive Security and Proactive Management provides endpoint security and device management capabilities. Proactive Security delivers real-time malware protection for computing endpoints, and security and threat analytics to help you strengthen your security position.¹ Proactive Management with HP TechPulse analytics helps boost productivity and optimize uptime for your devices.² Reports, incident tracking, and a consolidated cloud-based dashboard help you track hardware and software inventory and monitor device health, as well as anticipate, understand, and respond to security threats.^{3,4}

Service features

Advanced isolation technology

Viruses, ransomware, and other malware continue to pose a major threat to IT infrastructure. Go beyond definition-based anti-virus solutions with real-time threat isolation technology, using micro virtual machines (VM) to contain zero-day email, browser, and file attacks and prevent them from harming your network.⁵ Users can view attachments and websites without compromising the security of your network and without interrupting their workflow or changing their behaviors.

Analytics and reporting

Stay informed and get a holistic view of your device protection status and detailed findings on attempted and blocked attacks with HP TechPulse—all from a one-stop dashboard available through the HP DaaS portal. HP TechPulse provides proactive management and security features including:

- Device and application inventory and device and operating system health.
- One-stop dashboard with inventory, incidents, and reports, system health, and proactive incident notifications.
- Predictive analytics to identify systems at risk for disk, battery, or full-system thermal failure so action can be taken before a problem occurs.
- Alerts for devices that are non-compliant with encryption, firewall, and antivirus policies.

Security assessment

We're collaborating with Aon to offer additional cybersecurity solutions that include assessment, incident response, and cyber insurance services. The Aon Cyber Quotient (CyQu) self-assessment tool and security score help you evaluate your security position relative to your industry peers.⁶

Delivery specifications

HP responsibilities

- Troubleshoot installation and connectivity issues.
- Provide assistance and answers to service-related questions.
- Add new URLs to the whitelist of company-specific websites.

Customer responsibilities

- Establish an HP DaaS account with an HP representative or HP DaaS reseller.
- Install client on your devices.
- Enroll devices using the instructions provided by HP.
- Ensure compliance with software application licensing requirements.
- Review hardware, software, and security reports and respond as necessary.
- Request data deletion on devices that are reported missing or stolen.
- Request and provide URL whitelisting webpages.
- Troubleshoot common end-user support issues before escalating to HP support.
- Roll back OS updates in case of failure.
- Renew, change, or cancel your HP DaaS account.
- Complete the Aon CyQu survey online.

Onboarding

Onboarding is the process of bringing covered devices into the Proactive Security and Proactive Management solution. An HP Service Expert will create an account for you and provide necessary account information in a welcome email, along with directions about how to obtain assistance if you need it.⁷

Onboarding prerequisites

Before transitioning your devices to Proactive Security and Proactive Management, you must provide the following information:

- Primary contact information (name, email, phone, location)
- Your company address
- Your active directory DNS domain name
- A list of report administrators

Onboarding process

- **Phase 1: Registration.** You will receive a license key and a link to an online registration form.
- **Phase 2: Information gathering.** A representative will schedule a conference call to provide recommendations on how to proceed.
- **Phase 3: Recommendations and account creation.** HP will create your account in the HP DaaS security platform, beginning with default security configurations and whitelisting any additional URLs you require.
- **Phase 4: Deployment.** A representative will contact you to commence device enrollment and resolve any issues.

Delivery specifications (continued)

Information privacy

Devices managed through Proactive Security and Proactive Management will have a software agent installed to collect asset and event information related to the device. User-sensitive data including credentials, files, content, and personal details will not be captured. Collected data will be stored in a secure cloud repository.

Service limitations

General limitations

- Aon services are currently available in the United States only.
- Proactive Security and Proactive Management is hosted on Amazon Web Services (AWS).

System requirements

- Proactive Security and Proactive Management requires multi-vendor client devices running Windows 10 1703 or later, with a minimum of 8GB memory and 6GB free hard drive space.
- Communications between managed devices and the HP cloud management service require an active Internet connection.
- Systems used to access the security portal must meet the requirements listed at hpdaas.com/requirements.

Terms and conditions

See HP DaaS [terms and conditions](#).

For more information

Contact your local HP sales representative or channel partner for details or visit hp.com/go/DaaS.

Sign up for updates
hp.com/go/getupdated



Share with colleagues

1. Threat analysis provided by HP Service Experts is a forensic process that occurs after a malware event has been blocked or isolated by HP Sure Click Advanced software. It is not an ongoing, real-time monitoring service. HP Sure Click Advanced automatically isolates untrusted or malicious content, ensuring protection before the analysis. HP Proactive Security and Proactive Management 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.
2. HP does not track or monitor details that identify which URLs users visit. Reporting focuses on identifying threats and their source in HP TechPulse. HP TechPulse is GDPR and ISO 27001 compliant. Please see the HP DaaS Security white paper for details.
3. Dashboard for HP Proactive Management is on the HP DaaS Portal. HP unified endpoint management is provided by HP Service Experts in HP DaaS Enhanced or Premium plans. Service Experts deliver service using VMware Workspace ONE powered by AirWatch. Customers using Microsoft Intune may have our Experts manage using licenses they already have. Please check the availability of options in your country.
4. HP Proactive Management plans and/or included components may vary by region, by operating system, or by authorized HP service partner. Please contact your local HP representative or authorized partner for specific details in your location. HP services are governed by the applicable HP terms and conditions of service provided or indicated to customer at time of purchase. Customers 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.
5. 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.
6. Purchasers of the HP Proactive Security Service in the United States receive the Aon CyQu self-assessment and security score. \$0 retainer and one-hour free consultation included with optional incident response service from Aon. HP onboarding service representatives will provide instructions. Aon services are available in the United States only.
7. HP Service Experts who conduct threat analysis and monitor isolation activity for HP Proactive Security are included with the Enhanced plan only.

© Copyright 2019 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. Apple and Mac are trademarks of Apple Inc., registered in the United States and other countries. Android is a trademark of Google Inc. Microsoft and Windows are registered trademarks of Microsoft Corporation in the United States and/or other countries.

