HP DaaS Proactive Security

Service benefits

- Make endpoints more secure
- Guard against malicious websites and attachments
- Protect your data and devices

Service highlights

- Advanced isolation technology guards against malware[2]
- HP TechPulse analytics provides security insights and reports
- Aon CyQu assessment helps evaluate your security position[3]

Service overview

Enhance the secure management capabilities of HP Device as a Service (DaaS) with HP DaaS Proactive Security.[1] It provides real-time malware protection for computing endpoints, security and threat analytics, and specialized expertise to help you strengthen your security position. Threat isolation technology helps protect against malware introduced through email, browsers, and Office or PDF files. It extends the security insights and reports provided by HP TechPulse analytics. As a result, you can help protect against, understand, and respond to threats.

Features and specifications

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.[2] Users can view attachments and websites without compromising the security of your network and without interrupting their workflow or changing their behaviors.

HP TechPulse analytics

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 Service Experts

Strengthen your security position, stay ahead of attacks, and prevent negative impact on your business with our specialized Service Experts who monitor reports, analyze threats, and help you plan. HP Service Experts will perform quarterly security threat analyses and respond to security alerts.[4]

Aon

We're collaborating with Aon to offer additional cyber security solutions that include assessment, incident response, and insurance services. The Aon Cyber Quotient (CyQu) self-assessment tool and security score help you evaluate your security position relative to your industry peers, and Aon provides a $0 incident response retainer with an hour of consultation in the event of a security breach.[3]

DaaS Proactive Security plans

Service features	Standard plan (self-managed)	Enhanced plan (HP-managed)
Threat protection from email attachments, phishing links and downloads	✓	✓
Security insights from HP TechPulse	✓	✓
Aon CyQu evaluation, incident response, and insurance eligibility[3]	✓	✓
Isolation policy enforcement: HP Service Experts can manage advanced protection technology status	—	✓
Analysis: HP Service Experts will perform a kill switch analysis of isolated threats, and provide recommendations on best practices for users and devices that see a high volume of threats, as needed	—	✓
Security event investigation and notification: HP Service Experts will notify you when devices are no longer protected due to tampering by end users, or changes to system configuration	—	✓

Delivery specifications

Service options

- **Standard:** The standard, self-managed version of DaaS Proactive Security is available for standard, enhanced, and premium DaaS plans. Under the self-managed option, you assume responsibility for enrolling your devices and contacting HP for assistance if required.
- **Enhanced:** The enhanced version of DaaS Proactive Security is only available if you also have an enhanced or premium DaaS plan. With the enhanced plan, an HP onboarding program manager will assist you in the installation and configuration of the service, and HP Service Experts with cybersecurity expertise will provide ongoing monitoring and support.

HP responsibilities

Service Expert responsibilities for Standard plans:

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

Service Expert responsibilities for Enhanced plans:

- Ensure that advanced isolation technology is installed and enabled.
- Provide quarterly security threat analysis reports.
- Investigate security alerts and take appropriate action.
- Monitor service and coordinate troubleshooting and assistance.
- Provide Level 2 and Level 3 support and coordinate with your service desk.

Customer responsibilities

- Review dashboards, reports, and incidents on the HP DaaS Proactive Management dashboard.
- Review security reports and respond as necessary.
- Request and provide URL whitelisting webpages.
- Troubleshoot and perform triage for common end-user support issues before escalating to HP support.
- Renew, change, or cancel your HP DaaS account.
- Complete the CyQu survey online.[3]

System requirements

- DaaS Proactive Security requires multi-vendor client devices running Windows 10 1703 or later, with a minimum of 8GB memory and 6GB free hard drive space.
- DaaS Proactive Security requires HP TechPulse, which is included in any HP DaaS or HP DaaS Proactive Management plan. The HP DaaS Proactive Security Enhanced plan requires customers to be enrolled in an Enhanced or Premium HP DaaS.
- Communications between managed devices and the HP cloud management service require an active Internet connection.
- See hpdaas.com/requirements for additional details.

Delivery specifications (continued)

Onboarding

Onboarding is the process of bringing covered devices into the DaaS Proactive Security solution. An onboarding program manager will be assigned to manage the onboarding process if you have an HP DaaS Enhanced or Premium plan. If you have a standard, self-managed plan, 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.

Onboarding prerequisites

Before transitioning your devices to the DaaS Proactive Security, you must provide the following information to your onboarding program manager, HP account manager, and/or service partner:

- Primary contact information (name, email, phone, location)
- Your company address
- Your active directory DNS domain name
- A list of report admins
- A list of devices to be managed by HP Proactive Management, including model and serial numbers (for Enhanced or Premium DaaS plans only)

Onboarding process

- **Phase 1: Registration:** You will receive a license key and a link to an online registration form.
- **Phase 2: Information gathering:** An onboarding program manager will be assigned to manage your onboarding process. They 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:** The onboarding program manager will meet with you to commence device enrollment and resolve any issues.
- **Phase 5: Transition to ongoing support and management (Enhanced plans only):** When onboarding is complete, service will transition to HP Service Experts, who will provide ongoing support and management for the contract term.

Onboarding program manager responsibilities

- Create the HP DaaS Proactive Management account.
- Add or remove HP DaaS Proactive Management dashboard users.
- Grant user account access.
- Gather and consolidate required environment information.
- Provide documentation and guidance to deploy the analytics agent.
- Develop and implement the onboarding project plan.
- Provide progress updates.
- Verify successful implementation.
- Transition customer support for the HP DaaS Proactive Management capability to HP Service Experts.
- Diagnose and resolve installation issues.
- Provide ongoing support.

Service limitations

- HP Service Expert availability for DaaS Proactive Security Enhanced plan:
  - **North America:** English support available Monday through Friday (excluding HP holidays) from 6:00 a.m. to 6:00 p.m. MT.
  - **Latin America:** English and Spanish support available Monday through Friday (excluding HP holidays) from 7:00 a.m. to 6:00 p.m. GMT–5.
  - **Europe, Middle East, Africa:** English, French, and German support available Monday through Friday (excluding HP holidays) from 8:00 a.m. to 6:00 p.m. CET.
  - **Asia Pacific, Japan:** English and Chinese support available 24 hours a day; Japanese is supported 9:00 a.m. to 9:00 p.m. Japan Standard Time, 7 days a week (excluding HP holidays).
- Aon services are currently available only in the United States.
- HP DaaS Proactive Management and HP DaaS Proactive Security platforms are hosted on Amazon Web Services (AWS).

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. System requirements for HP DaaS Proactive Security are: multi-vendor client devices running Windows 10 1703 or later with a minimum of 8GB memory and 6GB free hard drive space to install the software client. HP DaaS Proactive Security requires HP TechPulse, which is included in any HP DaaS or HP DaaS Proactive Management plan. The HP DaaS Proactive Security Enhanced plan requires customers to be enrolled in an Enhanced or Premium HP DaaS or HP DaaS Proactive Management plan.
2. HP Sure Click Advanced technology is included with HP DaaS Proactive Security and requires Windows 10 and Microsoft Internet Explorer, Google Chrome, or Chromium are supported. Supported attachments include Microsoft Office (Word, Excel, PowerPoint) and PDF files, when Microsoft Office or Adobe Acrobat are installed.
3. Aon services are only available in the United States.
4. Service Experts available in the Proactive Security 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. 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.

4AA7-4656ENW, March 2019