

HP Proactive Security Enhanced Onboarding



Service benefits

- Integrate Proactive Security in complex environments
- Identify and implement exclusions and proxies
- Define change control, deploy/upgrade processes, freeze hours

Service highlights

- Three-day, onsite, onboarding workshop
- Environment and architecture analysis
- Documentation of user flow and organization whitelist

Service overview

HP Proactive Security Enhanced Onboarding¹ manages the integration of HP Proactive Security into your existing security stack. The service includes design and deployment along with policy settings and custom integration.

Features and specifications

HP Proactive Security Onboarding is a service extension to the HP Proactive Security. Installing HP Proactive Security into enterprise environments with 5,000 or more devices can lead to unforeseen complications best addressed by a professional services team. HP installation engineers will analyze your IT security infrastructure and determine the correct policy settings to ensure that HP Proactive Security is optimized for your environment.

Delivery specifications

Onsite workshop

HP will conduct an onsite workshop for onboarding and solution implementation over three concurrent days, including the following activities.

- Review pre-work.
- Review HP Proactive Security workflow.
- Install HP Proactive Security agent on test machines.
- Troubleshoot any deployment or configuration issues.
- Review your concerns.
- Troubleshoot compatibility issues.
- Review of the communication process with HP support.
- Introduction and handoff to CSM (customer success manager) if applicable and ongoing support processes.

Delivery specifications (continued)

HP responsibilities

- Provide documentation and guidance to deploy the HP Proactive Security agent on managed devices.
- Develop and implement the onboarding project plan.
- Identify URLs for the whitelist of company-specific websites.
- Identify company IP address ranges not subject to isolation.
- Communicate progress throughout the onboarding process.
- Diagnose and resolve installation issues.
- Verify successful implementation.
- Transition customer support for HP Proactive Security to HP Service Experts.²

Customer responsibilities

- Provide adequate workspace for use by HP personnel, including necessary access to facilities, systems, passwords, remote logins, etc.
- Assign project representatives to accompany HP personnel while onsite.
- Establish clear lines of communication for the rapid resolution of critical problems.
- Inform HP personnel of any potential health or safety hazards.

Customer IT or partner responsibilities

- Establish an HP account, working with your service partner or HP account representative.
- Work with HP to install the HP Proactive Security agent onto your managed devices.
- Request to add or remove managed users and devices, whitelisted browser sites, and company IP address ranges not subject to isolation.
- Log on to the HP Proactive Security console to view dashboards, reports, and incidents.
- Review security reports and respond as necessary.
- Complete the Aon CyQu survey to better understand your security position.³
- Troubleshoot common end-user support issues before escalating to HP support.
- Renew, change, or cancel your HP DaaS account.

Note: Personnel authorized to access your HP Proactive Security console may include a partner if you pre-approve a specific individual within the partner organization to have access to your account.

Onboarding prerequisites

Onboarding is the process to get you ready to use the purchased services, including setup your account, deploy agents and configure the security policies. You are responsible for providing the required information to the Enhanced Onboarding manager.

- Primary contact information (name, email, phone, location) for the individual who will work with HP to deploy the software agent to your devices.
- Company address.
- User Principal Name (UPN).



Service limitations

System requirements

- Customer's devices need to meet the system requirements of HP Proactive Security.

Terms and conditions

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

For more information

Contact your local HP sales representative or channel partner 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 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.

2. Service Experts provide ongoing support and management for Proactive Security Customers.

3. 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.

© Copyright 2020 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. AMD is a trademark of Advanced Micro Devices Inc. Intel and Core are trademarks of Intel Corporation in the United States and other countries. Microsoft and Windows are registered trademarks of Microsoft Corporation in the United States and/or other countries.

4AA7-5945ENW, April 2020

