Data sheet

# 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 Onboarding 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 Standard or Enhanced plan. 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.
- Install HP Proactive Security agent software on test machines.
- Review HP Proactive Security workflow.
- Install HP Sure Click Advanced on test machines.
- Review HP Sure Click Advanced workflow in your environment.
- Troubleshoot any deployment or configuration issues.
- Review your concerns.
- Troubleshoot compatibility issues.
- Review communication process with HP support.
- Introduction and handoff to CSM (customer success manager) and ongoing support processes.

## Delivery specifications (continued)

### HP responsibilities

- Provide documentation and guidance to deploy the isolation agent on Windows 10 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.[1]

### 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 rapid resolution of critical problems.
- Inform HP personnel of any potential health or safety hazards.

### Customer IT or partner responsibilities

- Establish an HP DaaS account, working with your service partner or HP account representative.
- Complete an online web registration form.
- 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 Management 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.[2]
- 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 Management console may include a partner if you pre-approve a specific individual within the partner organization to have access to your Proactive Management account.

### Onboarding prerequisites

Onboarding is the process of transitioning all devices covered under HP Proactive Management with HP TechPulse to also include HP Proactive Security. 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

- HP Proactive Security (Standard or Enhanced)
- HP Proactive Management (Standard, Enhanced, or Premium)
- HP Proactive Security Enhanced Onboarding service
- Windows 10 1703 or later
- Minimum 8GB system memory
- Intel® Core™ i3, i5, or i7 processor (VTX enabled) or AMD equivalent
- Communications between managed devices and the HP cloud management service require an active Internet connection.

## 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/go/DaaS.

Sign up for updates
hp.com/go/getupdated

Share with colleagues

1. Service Experts are included with the Enhanced plan only.
2. 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.



4AA7-5945ENW, September 2019