

# HP Protected App

## Term License Support



### Product benefits

- Isolate critical applications accessing data you can't afford to be compromised.
- Create a virtual air gap on existing Windows devices.
- Avoid provisioning separate devices for privileged access.
- Empower teleworkers with lower risk and higher compliance.
- Keeps protecting even if device is compromised.

### Product highlights

- Creates secure connection to critical applications.
- Safeguards against keylogging, screen capture, memory tampering, and man-in-the-middle attacks.
- Provides a seamless user experience that maximizes productivity.
- Uses the same micro-virtualization technology as HP Sure Click powered by Bromium.

### Product overview

HP Protected App uses hardware-enforced virtualization-based security to isolate critical applications running on Microsoft Windows clients. The zero-trust solution is deployed on the user's PC, beneath the operating system (OS) layer, where it creates a hardware-protected virtual machine (VM) that is completely isolated from the Windows OS. Through this innovative approach, the solution secures a number of key assets, including memory and CPU state, disk structures, keyboard input, display outputs, and network traffic.

Even if a user's endpoint is compromised, it won't pose any risk to the remote application and the sensitive data it contains, allowing users to work securely on multiple remote Privileged Access Workstation (PAW) from a single device. The user can only access the application through the hardware-protected VM, which remains isolated from the Windows OS—and any malware that might attack it.

### Features and specifications

HP Protected App secures applications in a hardware-enforced Linux<sup>®</sup>-based VM that runs on Windows 10 endpoint.

#### Remote problem diagnosis and support

- Remote Desktop Protocol.
- Citrix<sup>®</sup> ICA

#### Security features

- The latest Intel<sup>®</sup> and AMD CPU technologies to prevent host software from tampering with memory (VT-x, VT-d, UEFI secure boot, and TPM).
- Keylogging and screen-capture obfuscation and protection techniques
- User and application authentication for secure network segmentation
- Application audit logging
- Application control

## Delivery specifications

HP Protected App is available as standard MSIs for endpoints. This can be deployed to endpoints using standard distribution technologies (SCCM, GPO, BigFix, etc.) that already exist in customer environments today. Once installed, the endpoint software will communicate to the Sure Controller, which can be deployed on premises or hosted in the SOC2 Type 2 / ISO 27001 accredited cloud service, available from HP.

The controller will deliver policy and application configuration information to the endpoint, while the endpoint will report threat intelligence, operational, and audit data back to the controller. You have full visibility of your HP Protected App deployment from the controller, and you can create reports and application policies and monitor endpoint security in the auditing system.

Additional services are available from HP that utilize our professional services team to plan, deploy, and support you during your use of the product.

HP Protected App is available to purchase as a subscription term license only.

## Product limitations

### Endpoint requirements

HP Protected App runs on Windows 10 devices with the latest CPUs from Intel® and AMD.

- See <https://support.bromium.com/s/documentation> for detailed endpoint requirements.

### Controller requirements

The HP Sure Controller can be hosted in HP's cloud and delivered as a service, or it can be installed on-premise by the customer.

- See <https://support.bromium.com/s/article/HP-Sure-Click-Enterprise-Managed-Cloud> for cloud-hosted controller requirements.
- See <https://support.bromium.com/s/article/System-requirements-for-Bromium-Enterprise-Controller-BEC> for on-premise controller requirements.

### Supported software

HP Protected App currently supports RDP sessions, Citrix® ICA sessions, and a Chromium-based browser.

- See <https://support.bromium.com/s/documentation> for details.

## Terms and conditions

See complete Care Pack **terms and conditions**.

For additional details, see:

- <https://www.bromium.com/software-license-and-services-agreement/>
- <https://support.bromium.com/s/article/Product-Support-and-End-of-Life-Policy-EOL>
- <https://support.bromium.com/s/sla>

## For more information

Contact your local HP sales representative or channel partner for details.

Sign up for updates  
[hp.com/go/getupdated](https://hp.com/go/getupdated)



Share with colleagues

---

HP services are governed by the applicable HP terms and conditions of service provided or indicated to the customer at the 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.

© 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. AMD is a trademark of Advanced Micro Devices Inc. Citrix is a trademark of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries. Intel is a trademark of Intel Corporation in the United States and other countries. Linux is the registered trademark of Linus Torvalds in the U.S. and other countries. Microsoft and Windows are registered trademarks of Microsoft Corporation in the United States and/or other countries.

