HP SURE ACCESS ENTERPRISE

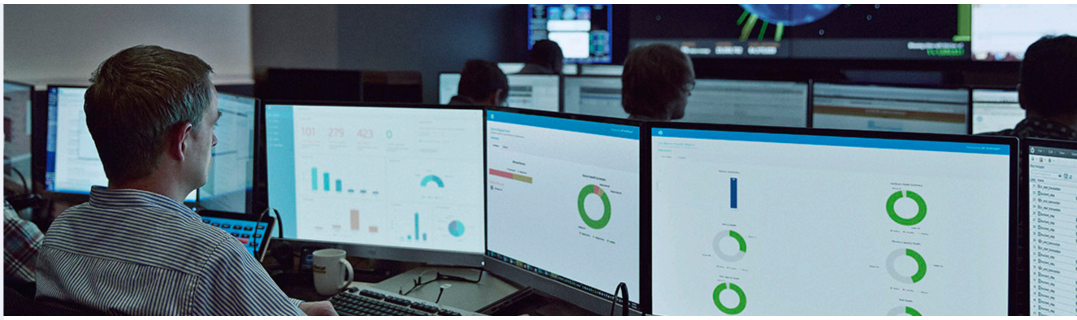
HP WOLF SECURITY

Hardware-enabled security for privileged, mission critical tasks

DATASHEET

HIGHLIGHTS

- Isolate and protect mission critical apps and data from possible compromise.
- Safeguards against keylogging, screen capture, memory tampering, and man-in-the-middle attacks.
- Avoid provisioning separate, dedicated PCs for privileged access.
- Supports RDP, ICA, SSH and web-based remote access.
- Keeps protecting even if device is compromised.
- CPU hardware enforcement for maximum protection.



Product Overview

Certain high-value tasks demand a higher level of security, including

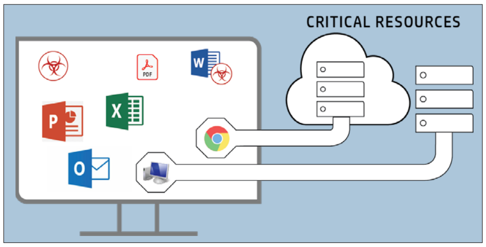
- Privileged User (IT administrator) activity
- Access to highly sensitive data
- Operational Technology (OT), ICS, and IoT remote administration

HP Sure Access Enterprise[1] (SAE) is a unique solution to secure such high-value, high-risk tasks. It creates a hardware-enforced isolated environment on the end-user PC that prevents attacks from compromising remote access or web-based sessions. Unlike the typical approach of applying multiple security products on the endpoint and hoping they'll suffice, SAE flips security on its head and provides **zero-trust, targeted protection for the most important tasks.**

Use Cases

SAE secures remote access to applications, IT, and OT/IoT infrastructure via

- HTML5 web
- Microsoft RDP
- Citrix® ICA
- SSH



Each such session is run within its own secure virtual environment on the end-user PC. Access may be direct to the high-value system, or indirect via a “jumpbox” or bastion host. Attacks including keylogging, screen-scraping, memory access or tampering, and network interception are prevented from compromising the high-value task. Even if the endpoint becomes corrupted by malware, the high-value tasks and the systems they access are isolated and protected.

Benefits

Sure Access Enterprise delivers a wide range of security and operational benefits:

- Much greater security for mission critical systems, data, and applications
- Eliminates need to provision and support dedicated PCs for privileged users
- Meet compliance control objectives for privileged activity
- Improves productivity of key staff and IT Support

SAE replaces dedicated privileged access PCs or Privileged Access Workstations (PAW). Staff members can use a single PC for all activity, while maintaining a high level of security and compliance. Even if a user's endpoint is compromised, it won't pose any risk to the remote system and the sensitive data it contains. Users can only access the sensitive application through the hardware-protected VM, which remains isolated from the Windows OS—and any malware that might attack it.

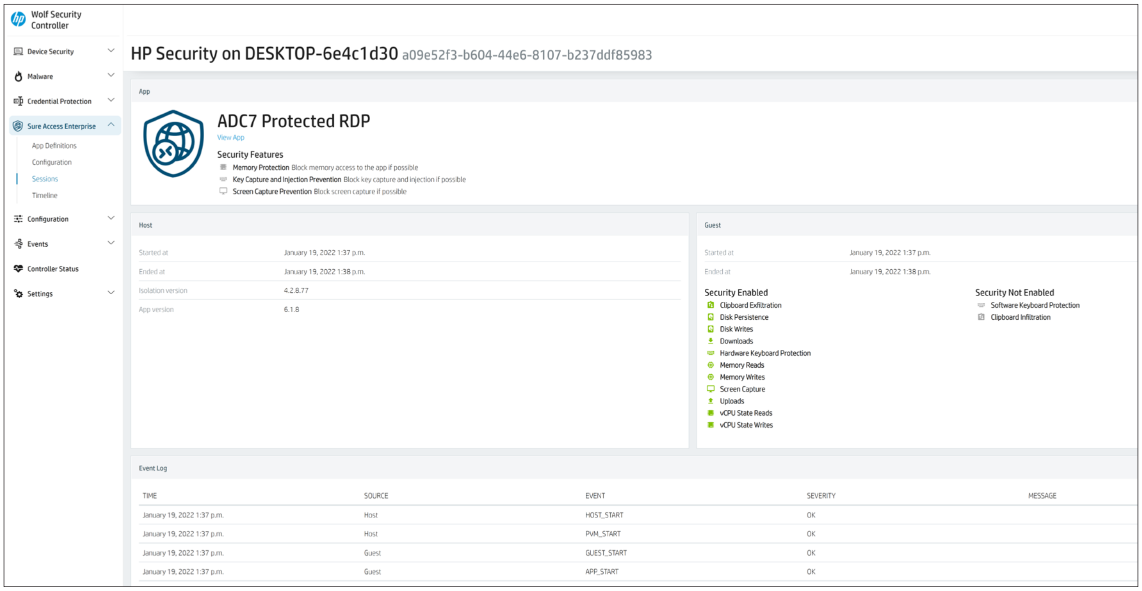
HARDWARE-ENABLED SECURITY

HP Sure Access Enterprise uses hardware-enforced virtualization-based security to isolate critical applications running on Microsoft Windows clients. The 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 elements, including memory and CPU state, disk structures, keyboard input, and network traffic.

CENTRALIZED MANAGEMENT

HP Sure Access Enterprise is centrally managed using the HP Wolf Security Controller[2]. The Controller is deployed either on-premises or in the cloud, and provides full control over SAE security policies across the enterprise. SAE endpoints report operational and audit data back to the Controller, lowering operational overhead and simplifying compliance reporting. An intuitive "timeline" report is available, centered on protected application, user, or endpoint device.

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



HP Security on DESKTOP-6e4c1d30 a09e52f3-b604-44e6-8107-b237ddf85983

App

ADC7 Protected RDP

View App

Security Features

- Memory Protection Block memory access to the app if possible
- Key Capture and Injection Prevention Block key capture and injection if possible
- Screen Capture Prevention Block screen capture if possible

Host

Started at	January 19, 2022 1:37 p.m.
Ended at	January 19, 2022 1:38 p.m.
Isolation version	4.2.8.77
App version	6.1.8

Guest

Started at	January 19, 2022 1:37 p.m.
Ended at	January 19, 2022 1:38 p.m.

Security Enabled

- Clipboard Exfiltration
- Disk Persistence
- Disk Writes
- Downloads
- Hardware Keyboard Protection
- Memory Reads
- Memory Writes
- Screen Capture
- Uploads
- vCPU State Reads
- vCPU State Writes

Security Not Enabled

- Software Keyboard Protection
- Clipboard Infiltration

Event Log

TIME	SOURCE	EVENT	SEVERITY	MESSAGE
January 19, 2022 1:37 p.m.	Host	HOST_START	OK	
January 19, 2022 1:37 p.m.	Host	PVM_START	OK	
January 19, 2022 1:37 p.m.	Guest	GUEST_START	OK	
January 19, 2022 1:37 p.m.	Guest	APP_START	OK	

HP Sure Access Enterprise supports granular per-application polices and secure logging

SECURITY FEATURES

- Uses latest Intel® CPU technologies to prevent host software from accessing memory (VT-x, VT-d, UEFI secure boot, and TPM2).
- Keylogging and screen-capture obfuscation and protection techniques
- Device, user and application authentication for secure network segmentation
- Certificate-based device & multi-factor authentication support
- Integrations with Privileged Administration Management (PAM) and IPSec Remote Access
- Full audit and logging; endpoint log encryption
- HP Sure Click Enterprise integration with single administrative console and threat intelligence
- Supports HP and non-HP endpoints

PRODUCT SPECIFICATIONS

Endpoint requirements

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

Controller requirements

The HP Wolf Security Controller can be hosted in HP's cloud and delivered as a service, or it can be installed on premises.

- 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-premises controller requirements.

TERMS AND CONDITIONS

For additional details, see:

- https://enterprisesecurity.hp.com/s/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

[1] HP Sure Access Enterprise requires Windows 10 Pro or Enterprise. 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. For full system requirements, please visit www.hpdaas.com/requirements.

[2] HP Wolf Security Controller is a management and analytics platform that provides critical data around devices and applications and is not sold as a standalone service. HP Wolf Security Controller follows stringent GDPR privacy regulations and is ISO27001, ISO27017 and SOC2 Type2 certified for Information Security. Internet access with connection to the HP Cloud is required. For full system requirements, please visit **http://www.hpdaas.com/**requirements.

HP WOLF SECURITY

4AA8-1110ENW, January 2022