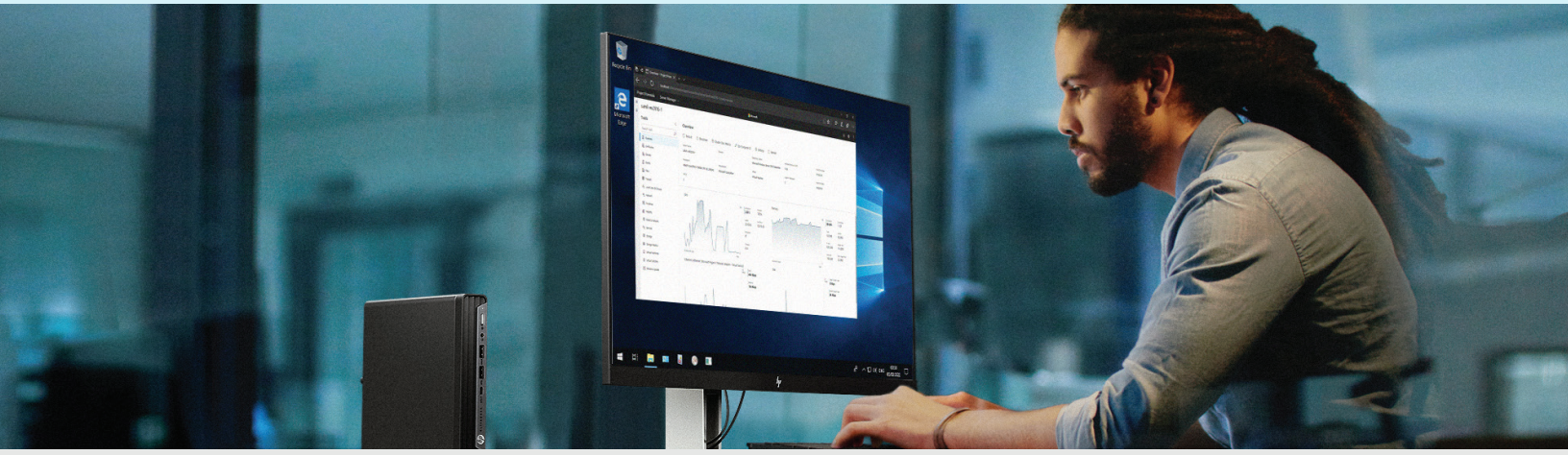
Sure Access Enterprise for Privileged Access Workstations

Simplifying deployment and scaling of high-security remote access



HIGHLIGHTS

- Privileged user activity requires advanced security controls
- Privileged Access Workstations meet the requirement but are expensive and inconvenient for users
- Sure Access Enterprise provides the necessary level of security, but also delivers better IT efficiency and user experience
- SAE supports the key remote access applications used for privileged remote access: RDP, Web, ICA, SSH

Background – The Privileged User Activity Security Challenge

Remote access to sensitive systems, applications and data presents a massive security risk. The threat is that an attacker will compromise the remote access session, usually by first compromising the end-user's computer. The risks from such an attack include data or credential theft, as well as infection, downtime, or even destruction of the high-value system. The risk is particularly high because the level of data access and system control associated with the privileged session. As a result, there often is a compliance or audit control requirement to have a higher level of security controls in place for such activity.

There are numerous privileged user access situations, with the common thread being sensitive system or data access:

- IT system administrators
- People with elevated privileges to data (for example production databases)
- Operational Technology (OT) or IoT remote administration
- Call center staff that must access sensitive data to do their jobs

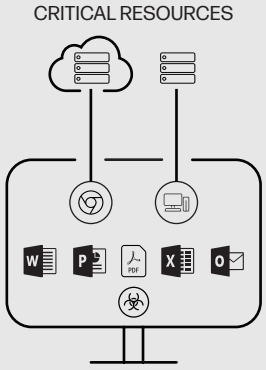
To mitigate this risk, Privileged Access Workstations (PAW) are often considered. There are two common PAW implementations, but both have considerable drawbacks:

Dedicated workstation for sensitive activity	Isolated "secure" space on a general purpose PC
This provides good security, but is expensive due to high IT costs and operational overhead. It also provides a poor user experience, as the user has to have multiple computers, and can't share data between them.	This approach provides better user experience, however because truly isolating the privileged activity is hard to do reliably, security suffers, defeating the purpose. Furthermore, if the secure workspace is totally isolated, data sharing is impossible.

Because of these challenges, what is needed is a solution that meets the high security requirement, but without the downsides:

- Reasonable IT costs and operational overhead
- Good user experience, including data sharing

HP Sure Access Enterprise – Meeting the Privileged Activity Challenge



Sure Access Enterprise supports multiple privileged sessions per PC

Sure Access Enterprise (SAE) is a hardware-enforced software solution designed specifically for the PAW use case. Based on over ten years of innovation and collaboration with leading CPU manufacturers, SAE allows a PC with standard hardware to be used for both privileged and non-privileged user activity.

The key SAE technology is micro-virtualization. A specific user task (for example a remote access RDP session) is run in a micro-VM on the Windows PC. The task is isolated from other tasks, and from the host OS itself. The solution builds a tight wall around the privileged task, with a tiny attack surface and very limited ability for anything "outside" to access what's inside. This Zero Trust approach assumes that even the PC itself can't be trusted. And because the micro-VM is implemented using hardware-based functions built into the CPU, malware can't get around it.

Solutions Flexibility and Management

SAE is built to be flexible. The privileged activity policy definitions can be customized on a per-application (target host) basis and is itself locked down with strong encryption and authentication. SAE supports all the most common remote access methods:

RDP	Web portal	Citrix ICA	SSH

A single PC can support multiple privileged sessions, and data sharing (e.g. cut and paste) can be permitted or denied as required.

All SAE management is done from a single management console. Access policies are created centrally and distributed to the authorized workstations. The console also provides full visibility and logging of privileged sessions, but does not capture any sensitive data within the sessions themselves.

SAE co-exists with multi-factor authentication that the target system might use. It also co-exists with Privileged Activity Management (PAM) solutions that are often used for management of privileged credentials.

Solution Benefits

Sure Access Enterprise provides the ideal combination of security and user experience to support privileged user activity:

SECURITY

- Hardware-enforced micro-virtualization isolates sensitive data from compromise
- Full audit trail of privileged access to support primary or compensating control
- Tamper-proof logging

USER EXPERIENCE

- Single workstation for privileged, non-privileged, and personal activity
- Consistent experience across applications
- Workstation portability – policy not locked to specific hardware

IT EFFICIENCY

- Single workstation lowers cost and IT overhead
- Centralized policy control & distribution
- No need to physically touch workstations to deploy or maintain solution or polices

Summary

Privileged user activity is a frequent target for cyber-attack because of the potential for massive data or availability compromise. The easiest way to attack such activity is by compromising the end-user PC. HP Sure Access Enterprise is a purpose-built solution that isolates and protects high-value activity, enforced by CPU hardware. And SAE supports this privileged activity control with high operational efficiency and consistent user experience.

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

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.

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.

4AA8-1466ENW, May 2022