



Sure Access Enterprise



Benefits

Secure privileged user activity by using hardware-enforced isolation on the client PC.

Lower cost and administrative overhead by eliminating dedicated privileged workstations (PAW) and enabling secure admin access from a single device.

Simplify endpoint security operations with centralized control, fewer tools, and consistent policy enforcement.

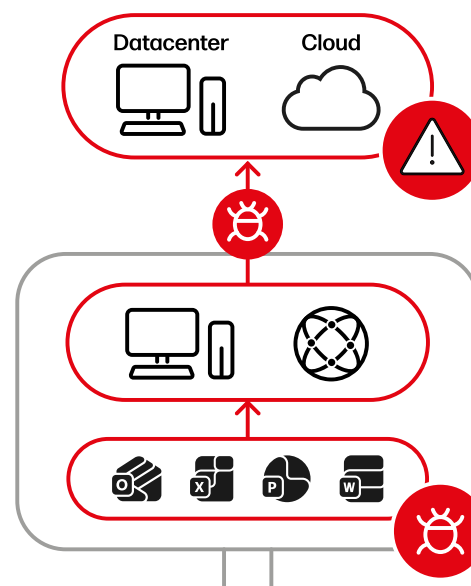
Preserve productivity and availability through transparent protection that doesn't disrupt user workflows.

The privileged or high-value access challenge

One of the most difficult tasks IT teams faces is supporting privileged access to critical systems and data repositories. It's difficult because there must be a balance between enabling staff to work efficiently and protecting the systems and data being accessed.

The challenge is even greater in today's distributed environment. Privileged users remotely access critical systems from PCs outside the office. Both the privileged users and their devices are often targeted by attackers because of the elevated access to sensitive systems they can leverage. The risk includes many types of systems: from on-premises datacenters to cloud apps across all aspects of the business including Development, Finance, HR, and the executive suite.

Traditional PC security relies on layering software controls on top of the operating system (OS). However, if the PC is compromised at the OS level, attackers can still capture keystrokes, scrape screens, tamper with memory, or intercept network traffic.



Attackers can compromise the privileged access PC and then compromise sensitive IT assets in the datacenter or cloud.

The limitations of privileged access workstations

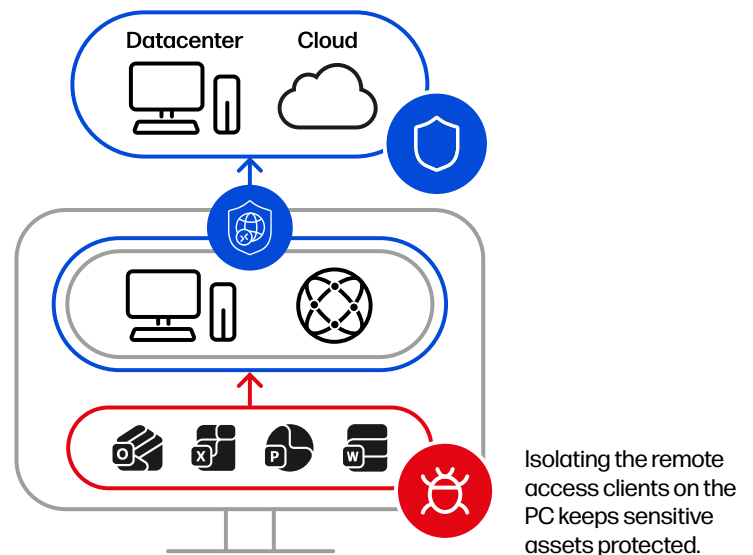
To provide privileged access, some organizations deploy dedicated Privileged Access Workstations (PAWs), which are PCs used only for sensitive access activities. However, this approach creates increased costs, management overhead, and user friction. For these reasons, PAWs are not widely deployed. At the same time, growing regulatory and business demands require stronger assurance, visibility, and control over privileged and sensitive activities. IT admins need stronger, policy-driven security controls for PCs that handle both everyday productivity tasks and access to critical systems.

Hardware-enforced Zero Trust for the work that matters most

HP Sure Access Enterprise (SAE) addresses these challenges by redefining how secure remote access can be achieved on a Windows PC that is also used for day-to-day conventional purposes. Instead of attempting to harden the endpoint OS, SAE assumes the endpoint may be compromised and protects only the privileged access applications that must be secured. It creates a hardware-enforced, isolated virtual environment on the user's PC which is deployed beneath the Windows operating system.

Remote access sessions to sensitive systems run inside protected virtual machines, fully isolated from Windows and any malware present on the device. Even if the PC OS is compromised, the sensitive systems remain protected. Credentials, keystrokes, memory, display output, and network traffic are enclosed within the micro-Virtual Machine which is enforced at the hardware level.

HP Sure Access Enterprise leverages modern Intel® and AMD CPU technologies, including virtualization extensions, TPM, and UEFI Secure Boot, to robustly secure the remote access sessions. Centralized policy management, visibility, and reporting are delivered through the HP Wolf Security Controller, which is available either in the cloud or on-premises. This allows IT teams to define granular access policies, monitor activity, and simplify operations without disrupting users or requiring dedicated hardware.



HP Sure Access Enterprise business outcomes

HP Sure Access Enterprise combines strong security with operational efficiency to protect sensitive data and systems from a wide range of attack vectors. This targeted approach reduces attack surface while avoiding the overhead of managing multiple devices or multiple security agents, lowering total cost of ownership and simplifying endpoint strategy.

From a risk perspective, SAE significantly reduces the likelihood and impact of credential theft, data loss, and lateral movement. Attacks such as keylogging, screen capture, memory tampering, and man-in-the-middle interception are blocked at the hardware level, protecting mission-critical systems even when endpoints are compromised. Centralized management provides IT teams with visibility into privileged activity while minimizing administrative burden.

High-impact use cases

HP Sure Access Enterprise is designed for scenarios where security, trust, and availability are critical:



Secure web-based access to sensitive cloud applications such as development, finance, HR, and executive portals



Remote administration of IT, OT, ICS, and IoT environments using RDP, Citrix ICA, SSH, and HTML5 software clients



Zero Trust endpoint-validated conditional access, ensuring only authorized, fully trusted devices connect to sensitive assets and systems



Privileged Access Workstation (PAW) replacement for secure administrative access without dedicated hardware

A smarter balance of security, productivity, and efficiency

HP Sure Access Enterprise enables IT decision makers to protect what matters most without sacrificing productivity or operational efficiency. By enforcing Zero Trust at the hardware level and isolating only high-risk activities, SAE reduces cyber risk, simplifies endpoint management, and ensures continuous availability, helping organizations move forward securely in an increasingly hostile threat landscape.

System requirements

CPU

- Intel Core i5 and higher, 6th generation minimum
- AMD Ryzen 1 (Zen "1") minimum

Memory and disk space

- 8 GB minimum required

Operating system

- Microsoft Windows 10 and 11 x64 ([Windows Support Policy](#))
- Microsoft Hyper-V
- UEFI boot

Other

- TPM 2.0 (discrete TPMs only)

Terms and conditions

Software and documentation license

- **Perpetual License.** If the Order provides for a perpetual license, the Software is licensed on a perpetual basis and will commence on the date You are notified of availability of the Software for electronic download.
- **Subscription License.** If the Order provides for a Software subscription license, the Software is licensed for a specified period of time and includes Support Services for the licensed period ("Subscription Term") and will commence on the date You are notified of availability of the Software for electronic download. To extend the Subscription Term, You must renew or purchase additional Licensed Units prior to the expiration of the current Subscription Term.

Payment

- **Fees.** Your fees are stated in the applicable Order. Except as otherwise provided in the Order, Your fees will be HP's current list price for Your Software and Services.
- **Payment.** Fees for subscription Software, Cloud Services and/or Support Services will be billed in advance as specified in the applicable Order. Subscriptions added during the Subscription Term will be pro-rated and billed for the remainder of the current Subscription Term. Fees for Professional Services will be billed as specified in the applicable Order. You will pay all amounts due and invoiced within the period specified in the invoice.
- **Suspension of Subscription.** In the event Your account is 10 or more days overdue, in addition to any of its other rights or remedies, HP reserves the right to suspend or terminate the subscription and applicable Software and/or Services.
- **Taxes.** All fees listed in the Order are exclusive of any taxes. You will be responsible for all taxes, including sales or use taxes, VAT, export or import taxes, excluding taxes on HP's net income.

Maintenance terms

These Maintenance Terms form part of the Agreement between You and HP and set forth the terms and conditions under which HP will provide Support Services to You pursuant to the HP maintenance plan purchased by You in relation to the Software. Fees for Support Services shall be prepaid by You along with all applicable taxes, and such fees are non-refundable.

In the event that You have licensed the Software and purchased Support Services through an HP-authorized reseller, You will be entitled to all the rights set forth in these Maintenance Terms for as long as Your maintenance payments are current.

1. Maintenance terms and fees. The term of your Support Services is for the period specified in the applicable fulfillment notice provided to you by HP upon your order. At the end of the initial term (and each renewal term thereafter, if any), the Support Services will expire unless You renew the Support Services by paying HP, or the applicable reseller, the fees for Support Services. HP may terminate Support Services if You fail to make pay the agreed fees for more than ten (10) days following written notice of delinquency. Either party may terminate this Agreement if the other party materially breaches this Agreement and fails to cure such breach within thirty(30) days after receipt of written notice of breach.

2. Maintenance updates and upgrades. During the initial or a renewal term of the Support Services, HP will make any Update and Upgrade releases for the Software available to you, subject to HP's End of Life policy set forth at <https://enterprisesecurity.hp.com/support/s/article/Product-Support-and-End-of-Life-Policy-EOL> (the "EOL Policy"). An "Update" shall mean a generally available release of the same edition of the same Software that HP makes available from time to time. An "Upgrade" shall mean a generally available release of the same Software that HP makes available from time to time that includes: (i) new editions of the Software that provide major enhancements to the features or functions, as determined by HP in its sole discretion; and/or (ii) new editions of the Software that provide additional features or perform additional functions. Upgrades do not include new products that HP introduces and markets as distinct licensed products. HP may designate a particular release of the Software as an Update or an Upgrade in its sole discretion. Updates and Upgrades shall be considered part of the Software and subject to the terms and conditions of the applicable [License Agreement](#).

3. Software defects. HP shall correct any defects or malfunctions in the Software or the Documentation discovered during the term of Your Support Services as per HP's development schedule and the Priority Levels described below, subject to the EOL Policy. HP has no obligation to provide Support Services related to Errors, as defined below, that arise out of or result from: (1) modifications to Software made by you or a third party not authorized by HP; (2) Your operation or use of the Software other than as specified in the Documentation; (3) any End User failure, including failure to promptly install any Update or Upgrade; (4) continued use of a Software release after HP has recommended You install an Update or Upgrade; or (5) any material breach of the Agreement by You.

4. Telephone and email support. HP will provide You with all reasonably necessary telephone and email consultation and support and instruction requested by You in connection with Your use and operation of the Software or any problems with the Software, as per the service levels described in Section 6 below and subject to the EOL Policy. You agree to provide HP with information regarding the Software problems, including transmission of certain diagnostic, technical, usage and related information and information about Your computers, systems, network and any third party software or hardware that may impact Your usage of the Software.

5. Notification of errors. You will designate up to three (3) authorized employees/agents (or replacement individuals) (each a "Contact") who are permitted to request Support Services under the Agreement and have access to HP's Customer Support portal (<https://enterprisesecurity.hp.com/support>). Each Contact will be knowledgeable about the Software. These Contacts may request Support Services by sending reports and queries to hsec-support@hp.com. HP may also provide to You a list of persons (in increasing positions of authority) and their telephone numbers (the "Calling List") for You to contact to report an error. When reporting any Error, You shall provide the classification of the Error and a reasonably detailed explanation, together with underlying data, to substantiate the Error and to assist HP in its efforts to diagnose and correct the Error.

6. Service levels. HP shall provide You with the following Support Service levels:

6.1. Classification and Resolution of Errors: An "Error" is defined as a reproducible failure of the Software to performance in substantial conformity to the specifications in the Documentation, whose origin can be isolated to a single cause. Errors are classified as follows:

6.1.1. Priority 1 Error (Production Down).

6.1.1.1. Definition. Except for HP Wolf Security Controller (HPWSC), a Priority 1 Error is any Error that renders You unable to use the Software on more than 50%, or 1,000 end points, whichever is lower, where it is installed, resulting in a critical impact to Your business operations. For BEC, a Priority 1 Error is defined as any issue that renders Sure Controller completely unusable.

6.1.1.2. Key Deliverables. In response to a Priority 1 Error, HP will immediately provide an appropriate resource and deliver a resolution. Unless otherwise agreed, HP will service Priority 1 Errors on a continual effort basis until the Error is resolved. Resolution of Priority 1 Errors may include temporary solutions, enabling Your business to operate until a more comprehensive solution is provided. Priority 1 Error support requires: (1) Appropriate End User personnel are available 24x7 to work with the HP support analyst; and (2) End User system access and/or system information is available 24x7. Your failure to provide the required resources will result in the Priority 1 Error being downgraded to a non-critical Error and will be serviced during HP's normal business hours ("Normal Business Hours").

6.1.2. Priority 2 Error (Significant Business Impact).

6.1.2.1. Definition. A Priority 2 Error is any Error that renders the Software severely limited in its functionality, as specified in the Documentation, but still usable. Components of a Priority 2 Error include: (1) a critical component of the Software (e.g. security IE browsing) is not responding or producing error messages; (2) the issue is critical to Your business operations;

6.1.2.2. Key Deliverables. Priority 2 Errors will be serviced as critical during Normal Business Hours until the Error is resolved. Priority 2 Error support requires: (1) Appropriate End User personnel are during Normal Business Hours to work with the HP support analyst; and (2) End User system access and/or system information is available during Normal Business Hours.

6.1.3. Priority 3 Error (Limited Business Impact).

6.1.3.1. Definition. A Priority 3 Error is any Error that results in the Software being usable with some non-critical features of the Software being unavailable. Components of a Priority 3 Error include: (1) Issues that affect Your ability to meet upcoming deadlines; (2) Software components returning errors messages or not responding; (3) degraded Software performance is negatively impacting Your business operations

6.1.3.2. Key Results. Priority 3 Errors will be serviced during Normal Business Hours until the Error is resolved. Priority 3 Error support requires: (1) Appropriate End User personnel are during Normal Business Hours to work with the HP support analyst; and (2) End User system access and/or system information is available during Normal Business Hours.

6.1.4. Priority 4 Error (Minimal Business Impact).

6.1.4.1. Definitions. A Priority 4 Error is any Error that is below Priority 3 and does not significantly impact Your business operations or for which a reasonable workaround has been implemented. Components of a Priority 4 Error include: (1) general questions such as “how-to” or syntax questions; (2) issues with little or no impact on Your business operations;

6.1.4.2. Key Results. Priority 4 Errors will be serviced as general issues during Normal Business Hours until the Error is resolved. Priority 4 Error support requires: (1) Appropriate End User personnel are during Normal Business Hours to work with the HP support analyst; and (2) End User system access and/or system information is available during Normal Business Hours.

6.2. Initial Response Time and Coverage.

6.2.1. Response Definitions. “Response Time” is the time between You reporting an issue to HP by opening a support ticket and the time in which a HP support analysis has responded to Your issue.

6.2.2. Response Time. HP shall use commercially reasonable efforts to respond to Your initial Error reports with off-site telephone consultation, assistance and advice in accordance with this Section 6.2.2. HP’s will respond to Your initial Error report either with; (1) a potential problem resolution, or (2) a request for more information that would permit HP to determine the next steps towards potential problem resolution. If it is determined, at HP’s sole discretion, that the Error reported requires escalation within the HP development organization or requires extensive time to research the reported Error, HP will advise You of the potential time necessary to provide a potential workaround or a resolution. HP’s response times to Your initial Error reports and coverage hours for actively working an Error are as follows:

Priority 1 Error	4 Hours	24 hours, 7 days a week
Priority 2 Error	12 Hours	3 AM to 8 PM, Eastern, Monday to Friday
Priority 3 Error	1 Day	3 AM to 8 PM, Eastern, Monday to Friday
Priority 4 Error	1 Week	3 AM to 8 PM, Eastern, Monday to Friday

7. End user’s obligations.

7.1. Contact Person(s). You will provide HP with a list of Contacts as specified in Section 5 above. HP is not responsible for Your failure to update your Contacts as maybe necessary.

7.2. Supporting Data. You will provide reasonable supporting data to aid in the identification and resolution of the issue.

7.3. Installation. You will be responsible for installing any error correction, Update or, if applicable, Upgrade.

7.4. Current Release. Unless otherwise agreed, You will to run the current release of the Software. HP will provide support for the current and two previous releases of the Software.

7.5. EOL Policy. You acknowledge and agree that HP’s obligations are subject to the EOL Policy.

8. Transferring maintenance. Support Services may not be transferred or assigned without HP’s express written approval and, in any event, may only be transferred or assigned along with the Software and the applicable Agreement.

1. HP Sure Access Enterprise is sold separately. For full system requirements, please visit [System Requirements for HP Sure Access Enterprise](#) for details.

See SAE License at: enterprisesecurity.hp.com

For purchases from HP through hp.com, this data sheet is governed by the terms of sale applicable to your purchase, as made available on the website where you made the purchase.

For all other purchases from HP, this data sheet is governed by HP’s Portfolio Customer Terms for the country of the HP affiliate accepting the order (“Lead Country”). A copy of these terms for all countries where HP has a direct presence can be found at [HP Portfolio Customer Terms](#). However, if the customer has a separately signed agreement with HP (“Custom Agreement”), the Custom Agreement will govern in the Lead Country. If the customer has a Custom Agreement and places orders or accepts delivery in countries other than the Lead Country, HP’s Portfolio Customer Terms for such country take precedence over the Custom Agreement only to the extent they reflect local law or business practice.

For purchases from an authorized HP Partner, this datasheet is governed by your terms with the HP Partner.

