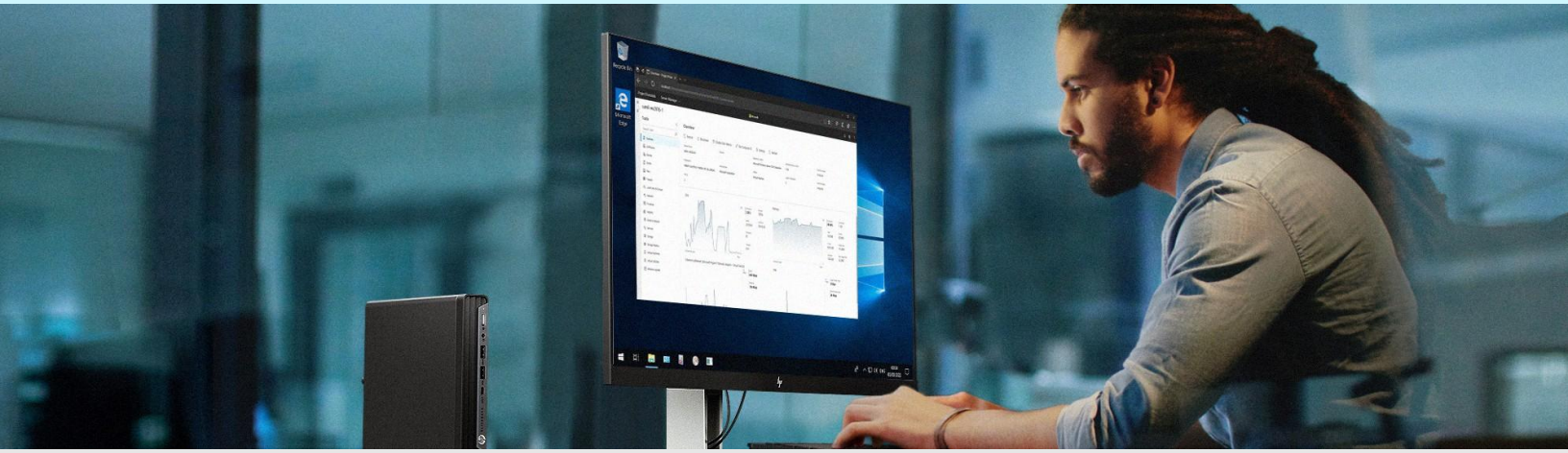
Sure Access Enterprise per workstation con accesso privilegiato

Semplificazione dell'implementazione e della scalabilità dell'accesso remoto ad alta sicurezza



HIGHLIGHTS

- L'attività degli utenti privilegiati richiede controlli di sicurezza avanzati
- Le workstation con accesso privilegiato (PAW) soddisfano i requisiti, ma sono costose e scomode per gli utenti
- Sure Access Enterprise (SAE) offre il livello di sicurezza necessario e offre inoltre una migliore efficienza IT e un'esperienza utente ottimizzata
- SAE supporta le principali applicazioni utilizzate per l'accesso remoto privilegiato: RDP - Web - ICA - SSH - PcoIP

Contesto - La sfida della sicurezza dell'attività degli utenti privilegiati

L'accesso remoto a sistemi, applicazioni e dati sensibili presenta un enorme rischio per la sicurezza. La minaccia è che un attaccante comprometta la sessione di accesso remoto, solitamente compromettendo prima il computer dell'utente finale.
I rischi di un tale attacco includono il furto di dati o credenziali, nonché infezioni, tempi di inattività o persino la distruzione del sistema di alto valore. Il rischio è particolarmente elevato a causa del livello di accesso ai dati e del controllo del sistema associato alla sessione privilegiata.
Di conseguenza, spesso vi è un requisito di conformità o controllo di audit per avere un livello più elevato di controlli di sicurezza per tali attività.

Ci sono numerose situazioni di accesso degli utenti privilegiati, con il filo conduttore dell'accesso a sistemi o dati sensibili:

- Amministratori dei sistemi informatici
- Persone con privilegi elevati per i dati (ad esempio, database di produzione)
- Amministrazione remota di tecnologia operativa (OT) o Internet of Things (IoT)
- Personale del call center che deve accedere a dati sensibili per svolgere il proprio lavoro

Per mitigare questo rischio, vengono spesso prese in considerazione le workstation con accesso privilegiato (PAW). Esistono due implementazioni PAW comuni, ma entrambe presentano notevoli svantaggi:

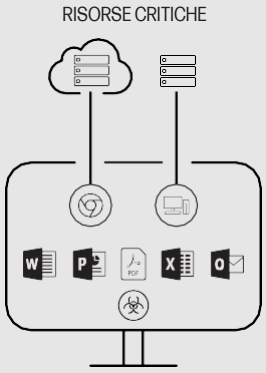
Postazione di lavoro dedicata per attività sensibili	Spazio isolato "sicuro" su un PC generico
Ciò offre una buona sicurezza, ma è costoso a causa degli elevati costi IT e del sovraccarico operativo. Fornisce anche un'esperienza utente scadente, poiché l'utente deve disporre di più computer e non può condividere dati tra di essi.	Questo approccio offre una migliore esperienza utente, tuttavia, poiché isolare veramente l'attività privilegiata è difficile da fare in modo affidabile, la sicurezza ne risente, vanificando lo scopo. Inoltre, se lo spazio di lavoro sicuro è totalmente isolato, la condivisione dei dati è impossibile.

A causa di queste sfide, ciò che è necessario è una soluzione che soddisfi gli elevati requisiti di sicurezza, ma senza gli svantaggi:

Costi IT e costi operativi ragionevoli

Buona esperienza utente, compresa la condivisione

HP Sure Access Enterprise – Superare la sfida delle attività privilegiate



Sure Access Enterprise supporta più sessioni privilegiate per PC

Sure Access Enterprise[1] (SAE) è una soluzione software rinforzata dall'hardware progettata specificamente per il caso d'uso PAW (Privileged Access Workstation). Basata su oltre dieci anni di innovazione e collaborazione con i principali produttori di CPU, SAE consente a un PC con hardware standard di essere utilizzato sia per attività privilegiate che non privilegiate.

La tecnologia chiave di SAE è la micro-virtualizzazione. Un processo specifico dell'utente (ad esempio una sessione RDP di accesso remoto) viene eseguito in una micro-VM sul PC Windows. Il processo è isolato dagli altri processi e dal sistema operativo stesso. La soluzione costruisce una barriera stretta attorno alla sessione privilegiata, con una superficie di attacco ridotta e una capacità molto limitata per qualsiasi cosa "esterna" di accedere a ciò che è all'interno. Questo approccio Zero Trust presuppone che anche il PC stesso non possa essere considerato affidabile. E poiché la micro-VM è implementata utilizzando funzioni basate sull'hardware integrate nella CPU, il malware non può aggirarla.

Flessibilità e Gestione della Soluzione

SAE è concepito per essere flessibile. Le definizioni dei criteri delle attività con privilegi possono essere personalizzate in base all'applicazione (host di destinazione) e sono bloccate con crittografia e autenticazione avanzate. SAE supporta tutti i metodi di accesso remoto più comuni:

RDP	Portale web	Citrix ICA	SSH	PCoIP

Un singolo PC può supportare più sessioni privilegiate e la condivisione dei dati (ad esempio, taglia e incolla) può essere consentita o negata a seconda delle esigenze.

Tutta la gestione SAE viene eseguita da un'unica console di gestione. I criteri di accesso vengono creati centralmente e distribuiti alle workstation autorizzate. La console fornisce inoltre visibilità e registrazione complete delle sessioni privilegiate, ma non acquisisce dati sensibili all'interno delle sessioni stesse.

SAE coesiste con l'autenticazione a più fattori che il sistema di destinazione potrebbe utilizzare. Coesiste anche con le soluzioni PAM (Privileged Access Management) che vengono spesso utilizzate per la gestione delle credenziali privilegiate.

Vantaggi della soluzione

Sure Access Enterprise offre la combinazione ideale di sicurezza ed esperienza utente per supportare l'attività degli utenti privilegiati:

SICUREZZA

- La micro-virtualizzazione rinforzata dall'hardware isola i dati sensibili da compromissioni.
- Tracciamento completo degli accessi privilegiati per supportare il controllo primario o compensativo.
- Logging a prova di manomissione.

ESPERIENZA UTENTE

- Postazione singola per attività privilegiate, non privilegiate e personali
- Esperienza coerente in tutte le applicazioni
- Portabilità della workstation - criterio non bloccato su hardware specifico

EFFICIENZA IT

- Una singola postazione di lavoro riduce i costi e il sovraccarico IT
- Controllo e distribuzione centralizzati delle policy
- Non è necessario avere accesso fisico alle workstation per distribuire o gestire la soluzione o le policy

Sommario

Le attività degli utenti privilegiati sono un obiettivo frequente per gli attacchi informatici a causa del potenziale di compromissione massiccia dei dati o della disponibilità. Il modo più semplice per attaccare tali attività è compromettendo il PC dell'utente finale. HP Sure Access Enterprise è una soluzione, che sfrutta le funzionalità di virtualizzazione della CPU, appositamente progettata per isolare e proteggere le attività ad alto valore. SAE supporta inoltre questo controllo delle attività privilegiate con un'elevata efficienza operativa e un'esperienza utente coerente.

Specifiche del prodotto

Requisiti dell'endpoint

- Vedere https://enterprisesecurity.hp.com/s/article/System-Requirements-for-HP-Sure-Access-Enterprise per i requisiti aggiornati.

Termini e condizioni

Per ulteriori dettagli, consultare:

- https://enterprisesecurity.hp.com/s/software-license-and- services-agreement
- https://enterprisesecurity.hp.com/s/sla

[1]HP Sure Access Enterprise è venduto separatamente. Per i requisiti di sistema completi, visitare la pagina Requisiti di sistema per HP Sure Access Enterprise .

4AA8-1466ENW, Nov 2022