HP SURE ACCESS ENTERPRISE

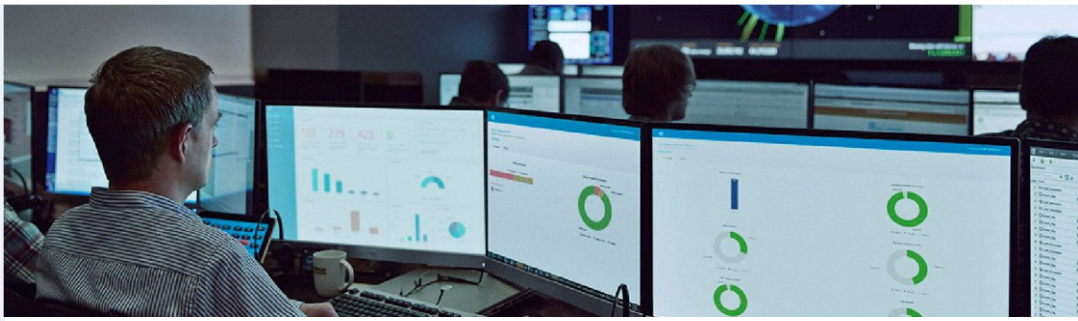
ミッションクリティカルなタスクを行う特権ユーザーのためのハードウェア対応セキュリティ

HP WOLF SECURITY

DATASHEET

ハイライト

- ミッションクリティカルなアプリケーションおよびデータを分離・保護し、潜在的な侵害リスクを低減
- キーログ取得、画面キャプチャ、不正なメモリ改ざん、ならびに中間者攻撃に対する保護機能を提供
- 特権アクセス専用 PC の新規配備は不要
- 多様なリモートアクセス方式（RDP / ICA / SSH / Web）に対応
- デバイスが不正アクセスを受けても保護を継続
- CPU をハードウェアレベルで制御し保護を最大化



製品概要

重要度の高い特定の業務では、より高度なセキュリティ対策が必要となります。

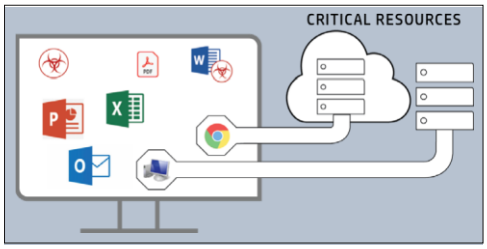
- 特権ユーザー（IT 管理者）の操作状況
- 機密性の高いデータへのアクセス
- OT（運用技術）、産業制御システム（ICS）、および IoT に対するリモート管理機能

HP Sure Access Enterprise（SAE）[1] は、高価値かつ高リスクな業務を保護するために設計された他に類を見ないセキュリティソリューションです。CPU ハードウェアを強制的に分離し、リモートアクセスや Web セッションへの攻撃を遮断します。複数のエンドポイント製品で守る従来のモデルと異なり、ゼロトラスト型の防御で最重要業務を確実に守ります。

ユースケース

アプリケーション、IT、および OT / IoT へのリモートアクセスを、以下の方法で安全に実現します。

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



各セッションは、特権ユーザーの PC 上で独立したセキュアな仮想環境内で実行されます。高価値システムへ直接接続する場合に加え、「ジャンプボックス」や踏み台サーバー（バスチオンホスト）を経由した間接的な接続にも対応します。キーロギング、スクリーンスクレイピング、メモリアクセスや改ざん、ネットワーク盗聴といった各種攻撃が侵害することなく確実に遮断されます。エンドポイントがマルウェアによって侵害された場合でも、業務およびアクセス先のシステムは完全に分離され、保護されます。

導入効果

セキュリティおよび運用の両面において、幅広いメリットを提供します：

- ミッションクリティカルなシステム、データ、アプリケーションに対するセキュリティ強化
- 特権ユーザー向け専用 PC の調達・運用が不要になる
- 特権ユーザーの操作に対するコンプライアンス要件・統制を満たします
- コア人材と IT サポートの生産性向上に貢献します

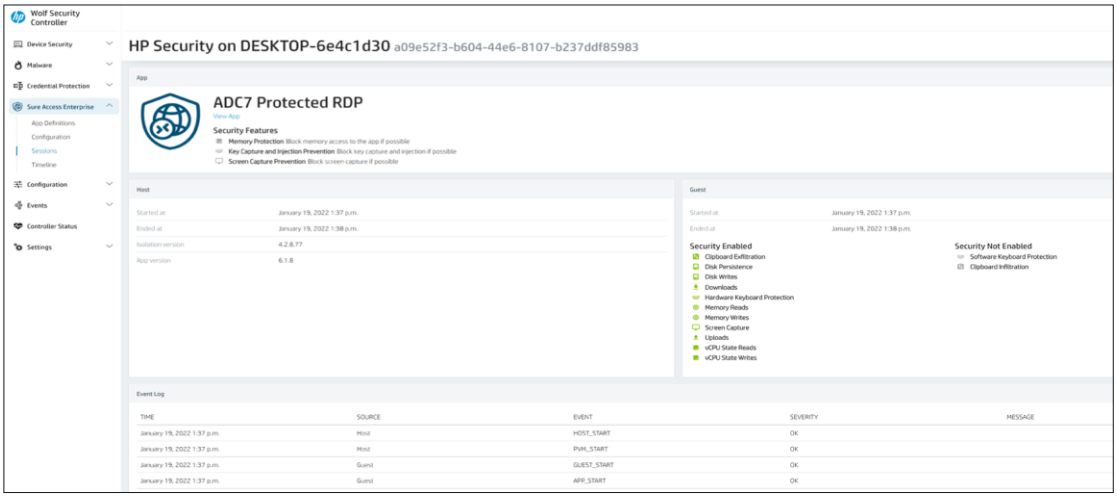
特権アクセス用の専用 PC を不要にします。単一のパソコンであらゆる業務を実行し、高いセキュリティレベルとコンプライアンスを維持できます。エンドポイントが侵害されても、リモートシステムおよびその機密データにリスクが及ぶことはありません。ハードウェアで保護された仮想マシン(VM）を介してのみ機密性の高いアプリケーションにアクセス可能であり、Windows OS から完全に分離されています。そのため、OS を標的とするマルウェアの影響を一切受けず、安全性が確保されます。

ハードウェアレベルで実現する強固なセキュリティ

Windows クライアント上で稼働する重要なアプリケーションを分離するために、ハードウェア強制型の仮想化セキュリティを採用しています。本ソリューションはユーザーPC 上、OS（オペレーティングシステム）層の下で動作し、Windows OS から完全に分離されたハードウェア保護型の仮想マシン（VM）を構築します。この革新的なアプローチにより、メモリや CPU 状態、ディスク構造、キーボード入力、さらにはネットワーク通信に至るまで、重要なシステム要素を包括的かつ確実に保護します。

一元化された管理

HP Sure Access Enterprise は、「HP Wolf Security Controller」[2] で一元管理できます。オンプレミスまたはクラウド環境に展開可能で、企業全体にわたる SAE のセキュリティポリシーを包括的かつ強力に統制します。各エンドポイントは、稼働状況や監査データをコントローラーへ集約し、運用負荷の大幅な削減とコンプライアンスレポートの簡素化を実現します。
保護対象のアプリケーション、ユーザー、またはエンドポイントデバイスを軸に可視化できる、直感的な「タイムライン」レポート機能も提供されます。



HP Sure Access Enterprise アプリケーション単位のきめ細かなポリシーと安全なログ管理をサポートします

主なセキュリティ機能

- 最新の Intel® CPU テクノロジー（VT-x、VT-d、UEFI セキュアブート、TPM2）でホストソフトウェアによるメモリアクセスを防止
- キーロギングと画面キャプチャに対する難読化技術と保護機能を提供
- セキュアなネットワークセグメンテーションを実現するためデバイス・ユーザーおよびアプリケーションの認証機能
- 証明書ベースのデバイス認証と多要素認証
- 特権アクセス管理と IPSec リモートアクセスの統合
- 包括的な監査およびログ管理機能と、エンドポイントログの暗号化
- 単一の管理コンソールと脅威インテリジェンスを活用した、HP Sure Click Enterprise との統合に対応

1 HP Sure Access Enterprise をご利用いただくには、Windows 10 Pro または Enterprise が必要です。HP のサービスは、購入時にお客様へ提供または提示される該当の HP サービス利用規約に従って提供されます。お客様は、適用される各国の法令に基づき追加の法的権利を有する場合があり、これらの権利は HP のサービス利用規約または製品に付属する HP 限定保証によっていかなる影響も受けるものではありません。システム要件の詳細については、以下のサイトをご参照ください：System Requirements for HP Sure Click Enterprise

2 HP Wolf Security Controller は、デバイスおよびアプリケーションの運用状況を可視化する管理・分析基盤であり、単体サービスとしての提供は行っていません。GDPR に準拠し、ISO27001、ISO27017、SOC 2 Type 2 といった国際的なセキュリティ認証を取得しており、高い信頼性を備えています。本ソリューションの利用には HP クラウドへの接続を含むインターネット環境が必要です。
詳細なシステム要件：HP Wolf Security - Endpoint Management Products | HP® Official Site

4AA8-1110ENW, January 2022

HP WOLF SECURITY