HP Wolf Security

HP WOLF SECURITY

隔離に基づく最新のセキュリティ技術と導入事例

HP Wolf Security

HP Sure Click

HP Sure Access

HP WOLF SECURITY

OS内の防御戦略

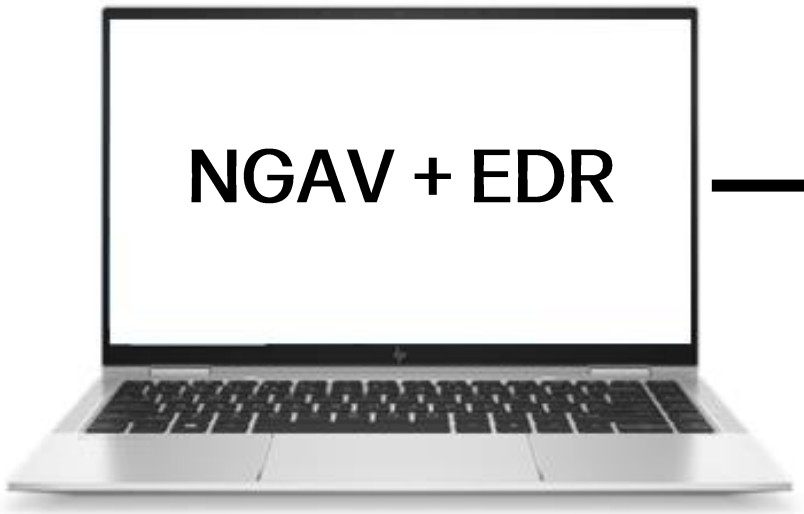
HP WOLF SECURITY

EPP AV/NGAV

可視化 / EDR

隔離

隔離によるNGAV＋EDRの拡張



- ホスト上にはより少ない高リスクプロセス
- オーバーヘッドの削減
- NGAV+EDRの負担およびアラート削減

HP WOLF SECURITY

隔離

- 高リスクのコンテンツを隔離
- インターネット上のWebサイト
- Eメールの添付ファイル
- Webからのダウンロードファイル
- USBドライブ上のファイル

ユーザーの責任にしない – クリックを隔離

クリックはユーザーの仕事の一部。悪意があるかどうかはわからない。

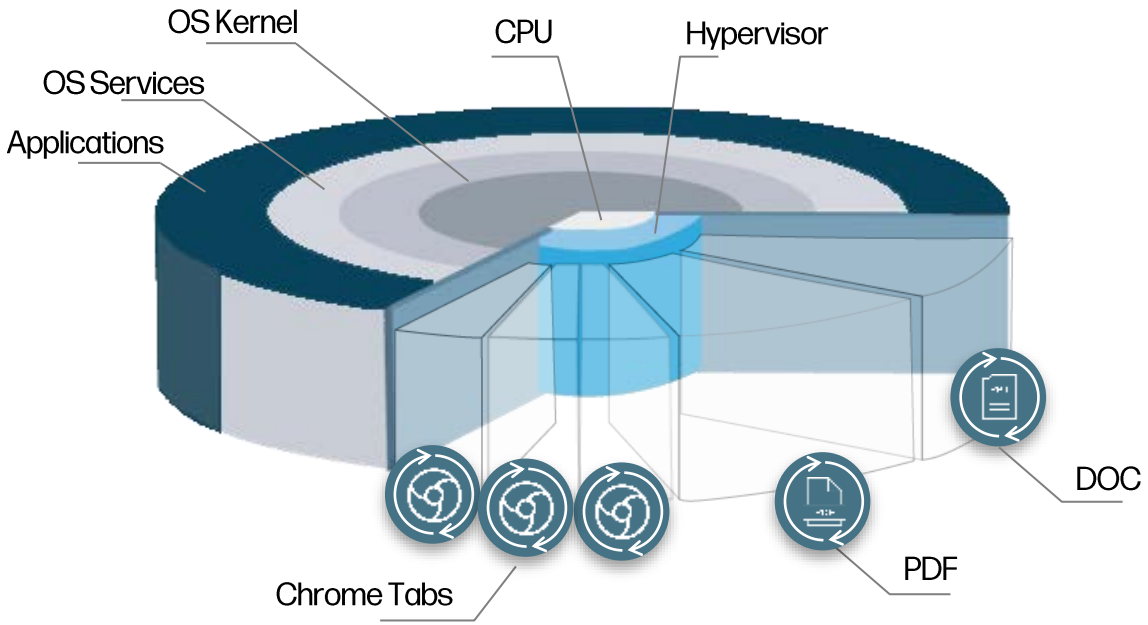
Eメール/チャット経由のWebリンク

Eメールの添付ファイル

ダウンロードファイル

USBドライブ上のファイル

Sure Clickの内部動作



CPUハードウェアで強化した仮想化技術

仮想マシン（VM）をミリ秒で生成

リスクの高いタスク毎に新しいVMを生成

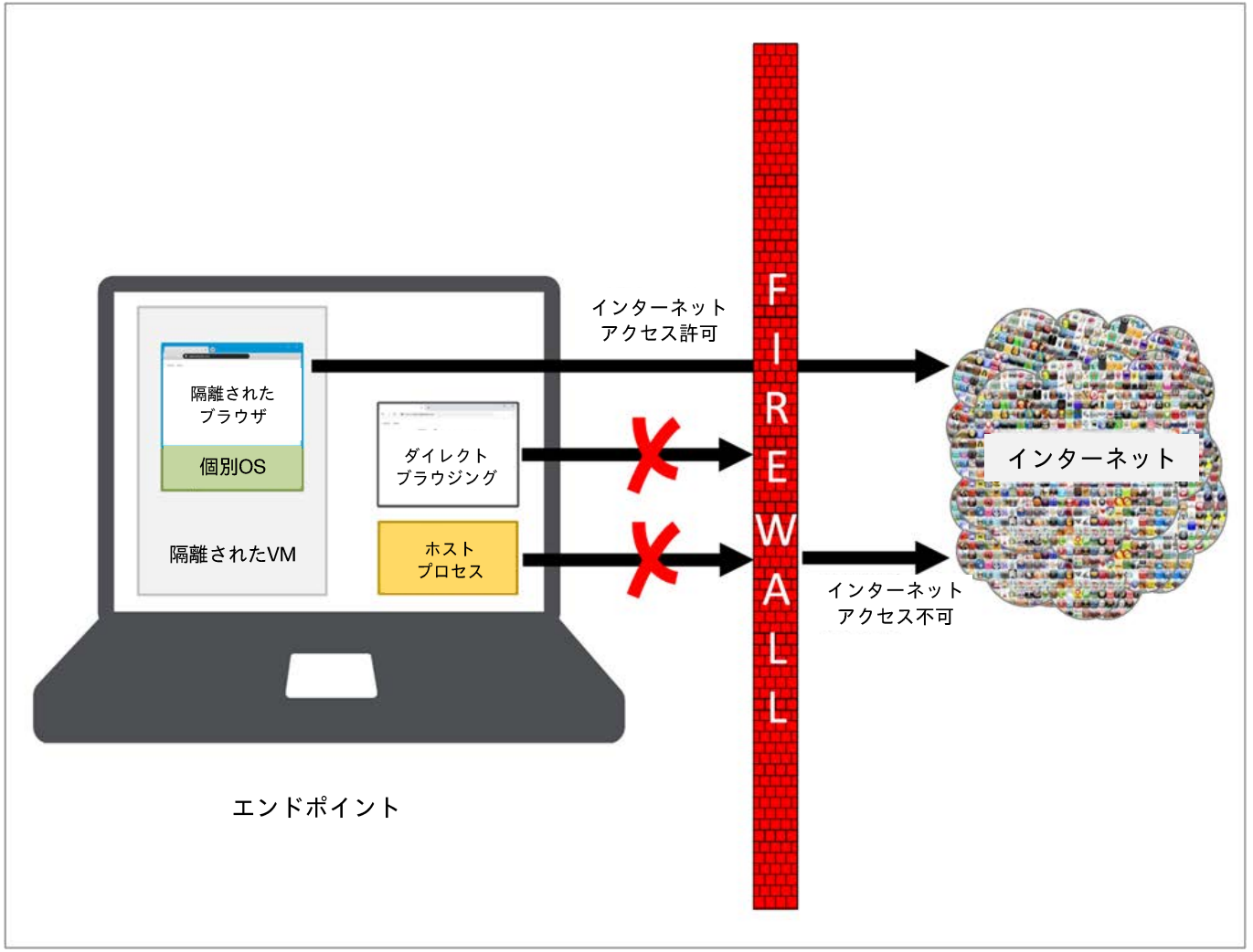
各インスタンスはホストから完全に隔離されて実行

VMが感染したPCやネットワークからの
マルウェアを防御

マルウェアはVMを閉じる際に廃棄

ユーザー事例– ドイツ政府

- ドイツ政府機関 - 4万デバイス
- 完全なインターネット分離を希望
- Sure Click Enterpriseを導入
- ホストPCのプロセスはインターネットに接続できない
- HP Secure Browserのみインターネットにアクセス可能



ユーザー事例 - 自動車製造

- 世界的な大手自動車メーカー
- Eメールの添付ファイル、Webダウンロード、USBドライブ上のファイルを懸念
- ファイルの隔離機能に限定し、100K+のSure Click Enterpriseを導入
- HP Secure Browserやインターネット分離機能は未導入
- Sure ClickがChromeとEdgeからのダウンロードを保護

認証情報の窃取に対する保護

問題点

不正なアクターが偽のサイトを利用してユーザーのログインIDやパスワードを盗み出そうとしています。これらのサイトの多くは、フィッシングメールのリンクとして送られます。

解決策

認証情報保護機能は、既知の悪意のあるサイトへの認証情報の入力をブロックし、サイトが疑わしい場合はユーザーに警告を行います。

認証情報の窃取に歯止めをかける

with Sure Click Credential Protection

*Google Transparency Report

悪意のあるサイトでユーザーが認証情報を入力するのを阻止

検証済みサイトでは認証情報の入力に支障なし

既知の悪意のあるサイトでは認証情報の入力をブロック

不審なサイトの場合はユーザーに警告

評価の低いサイトでの認証情報入力を制御する機能

Wolf Pro Security と Sure Click Enterprise で提供

HP Sure Access Enterprise

HP WOLF SECURITY

強固な隔離が権限昇格を防ぐ

リスクの高い攻撃経路の隔離

検知に依存しない防御

Sure Click Enterprise

高価値アプリとデータの隔離

侵害時における完全性の維持

Sure Access Enterprise

特権アカウントの保護

問題点

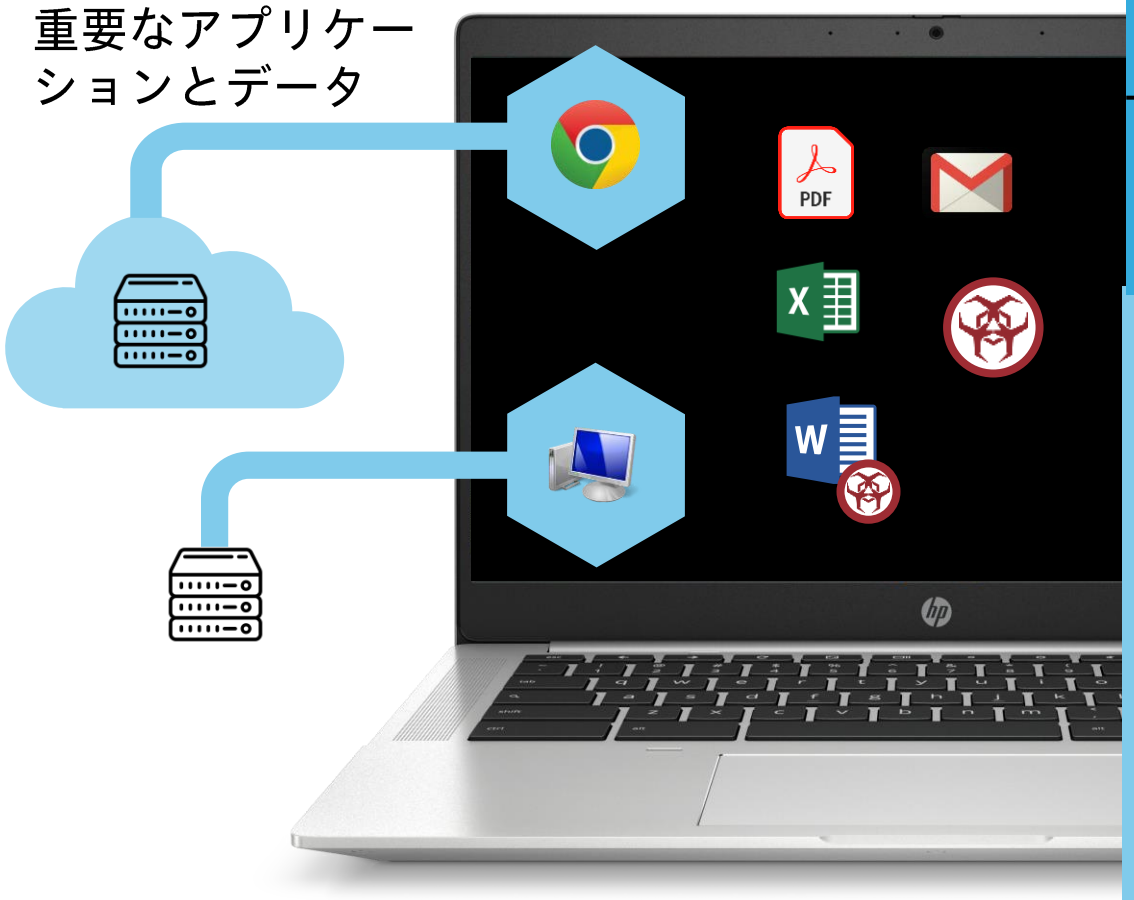
IT管理者などの特権を持つアカウントは、PCが侵害された場合にハッカーに盗まれる可能性のある、非常に機密性の高い情報にアクセスすることができます。

解決策

HP Sure Access Enterpriseは、PC上にハードウェアで強化された隔離環境を構築し、リモートアクセスやWebベースのセッションが攻撃によって侵害されることを防ぎます。

どのような場合にも保護を続ける

with HP Sure Access Enterprise



Protected VMによるアプリケーションの隔離

キーストロークの傍受やインジェクション

実行やI/Oの状態へのアクセス

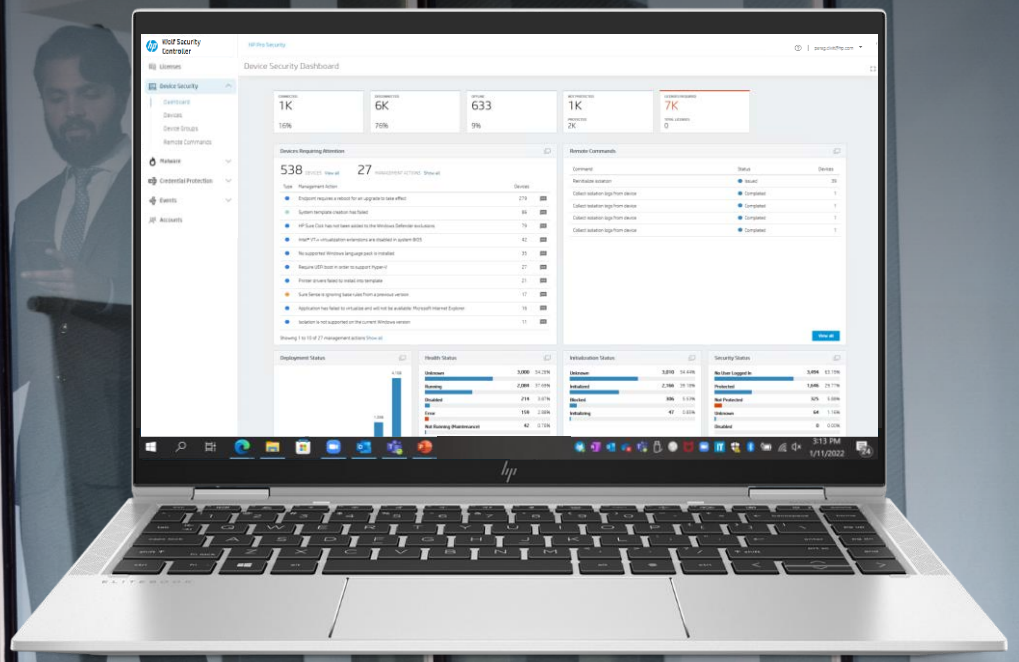
表示画面のスクリーンショット

ユーザー事例 – カナダ政府

- カナダ政府機関の2,000人以上のIT管理者が対象
- IT管理者アカウントが侵害されることを懸念
- IT管理者は2台+のPCを使用（IT管理業務用とEメール/インターネット用に別々のPC）
- Sure Access導入によりIT管理者のPCを1台に集約
- IT管理者はCitrixを使用し、Sure Accessで保護されたVMから起動したCitrixセッションのみが管理用ネットワークに接続可能（SCEP/PKIはSure Accessに統合）

あらゆる場所から社有PCを管理

HP Wolf Security Controllerで安心安全に



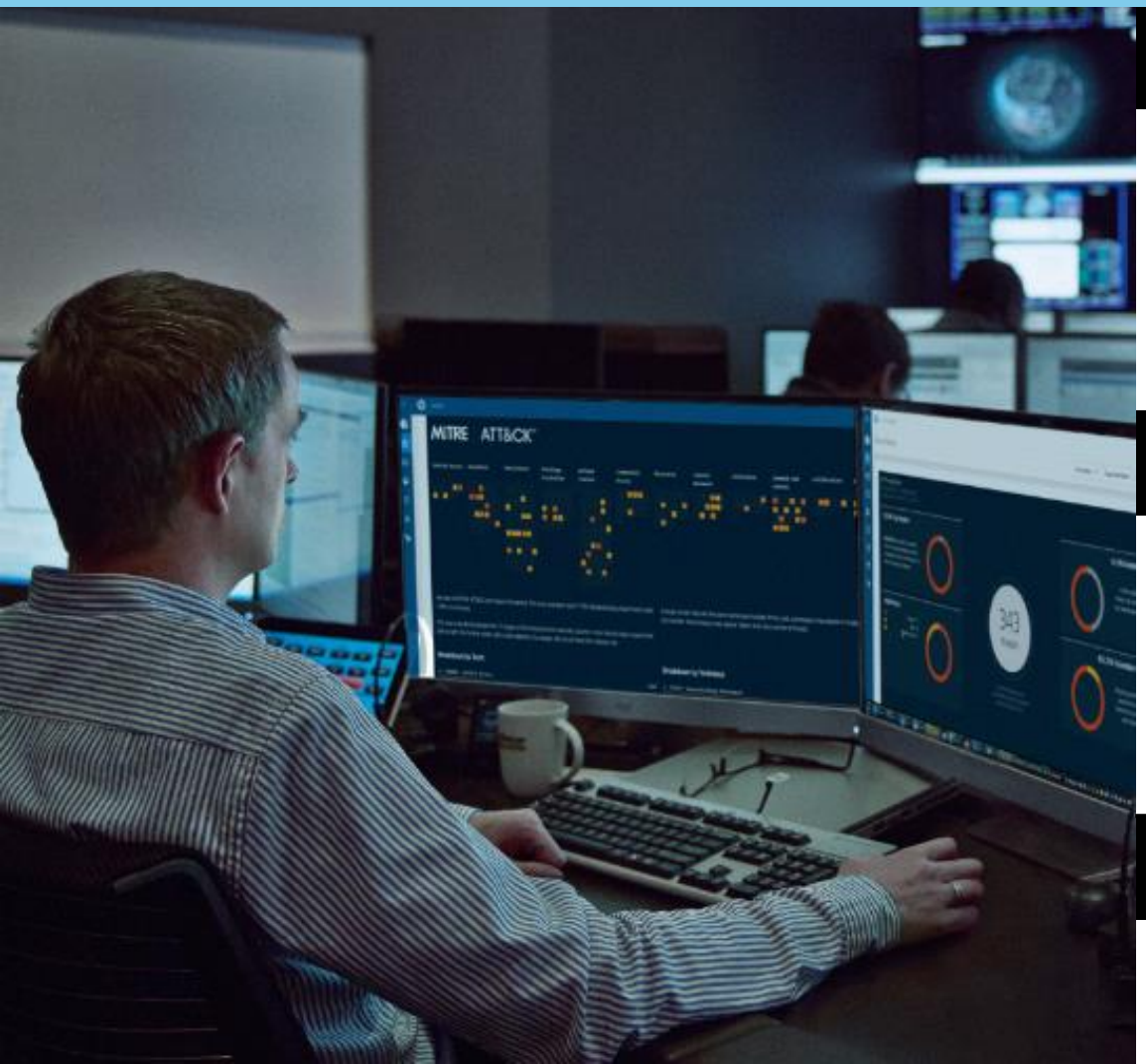
シームレスに拡張できるクラウドファースト・プラットフォームとして実装

パートナーによるマネージドサービスに最適化

HPのソリューションと統合

次世代の脅威インテリジェンスを活用

マルウェアから学び豊富な脅威データでプロアクティブに対応



ユニークな特徴

- イントロスペクション
- フライトレコーダー
- ユーザー操作
- 完全なキルチェーン分析
- 管理された環境で異常検知を実現

得られる情報

- MITRE ATT&ACK™ 指標
- プロセス相関グラフ
- システム&APIコール
- Eメールのヘッダー情報
- ネットワークトラフィック
- 全てのファイルとアーティファクト

リアルタイムの脅威インテリジェンス・フィード

- STIX/TAXII
- 統合 API
- Splunk コネクター

HP Wolf Security Controller

あらゆる規制や環境に対応できる柔軟性

クラウド環境

- HPのAWSクラウド上で稼働
- HPによる管理とアップデート
- 以下のAWSリージョンを選択可能
- 米国、ドイツ、日本

HP WOLF SECURITY

オンプレミス環境

- お客様による全ての導入と管理
- 標準的なMS技術 (IIS & SQL) による構築
- あらゆるプライベート/パブリック・データセンターで実行可能
- クラウドへの接続不要

お客様はクラウドあるいはオンプレミスを選択可能

HP Wolf Security

組織規模やPCベンダーに関わらず世界最高のセキュリティを実現

HP Wolf Pro

- シンプルな設定済みの構成
- 専門知識の限られた組織向け
- 小規模～中規模企業向けの設計
- 最小限のカスタマイズ
- クラウド接続が必須

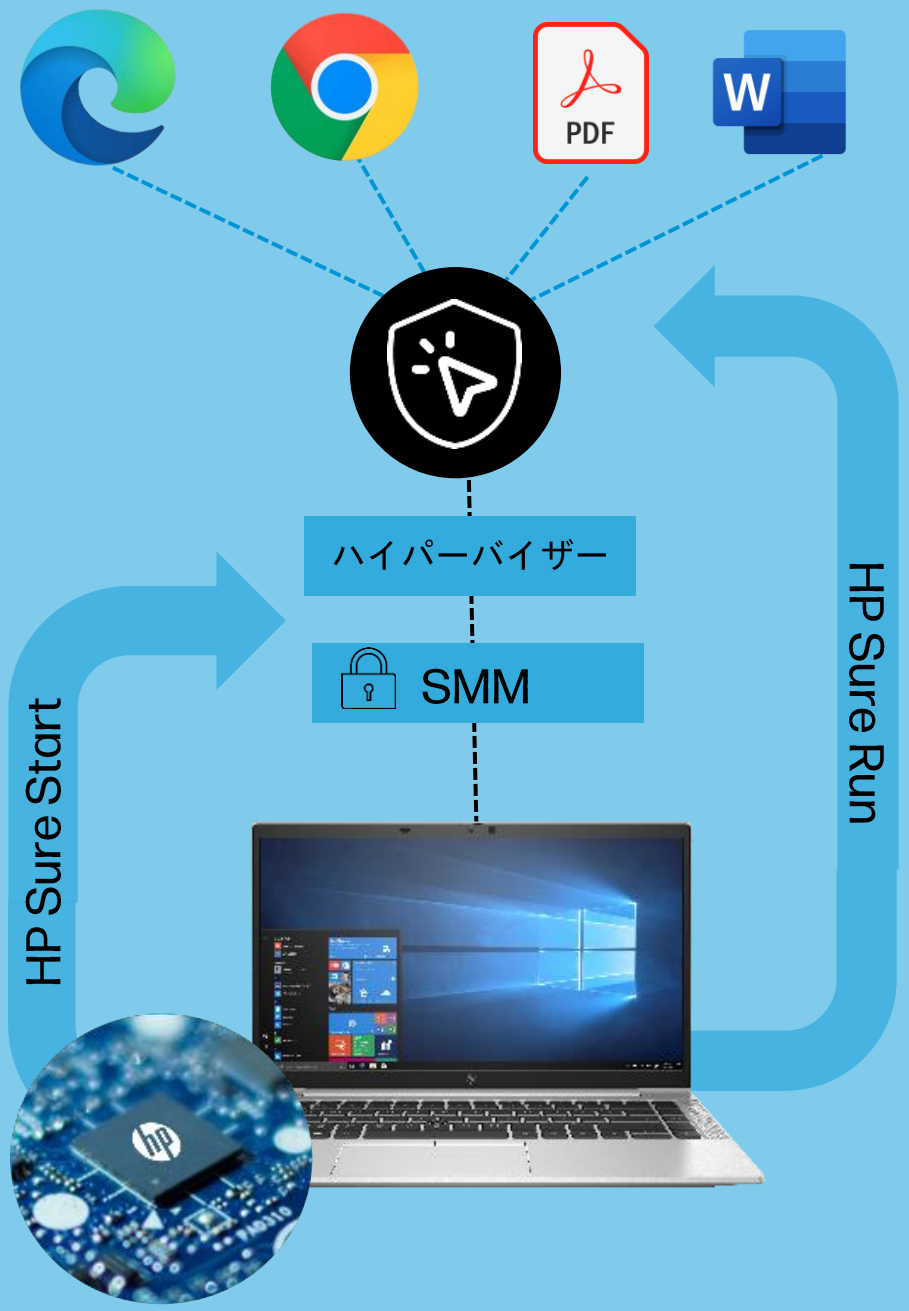
HP Wolf Enterprise

- 大企業向け
- 成熟度の高い組織向けの設計
- 高度なカスタマイズが可能
- クラウド接続はオプション

HP Wolf Securityはあらゆるベンダーの Windows 10/11デバイスをサポート

HPでさらにセキュアに

プラットフォームのセキュリティと統合



Thank you.