HP WOLF SECURITY

ハイブリッドワーカー保護の新しい方法

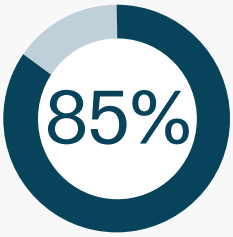
HP WOLF SECURITY レポート

ハイブリッドワーカーを保護するための戦略

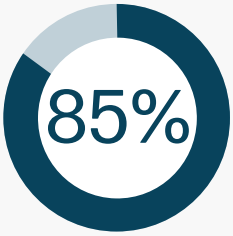
セクション 01

ワークフォースは急速に変化しています。これは、戦略の変更、重点的投資対象、そしてハイブリッド従業員を守るための新しい防御技術に直接影響を与えます。

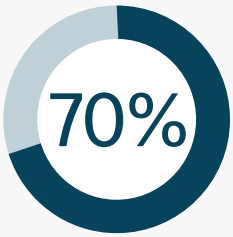
1. 防御戦略の見直し



のセキュリティリーダーが、ハイブリッド従業員に対応するために、サイバーセキュリティ戦略全体に変更を加えています。[i]



がこのようなユーザーには別のツールやポリシーを適用していると回答しています。[i]



がハイブリッド従業員が遠隔地にいる場合、侵害のリスクを最小限に抑えるため、企業ネットワークへのアクセスを制限していると回答しています。[i]

2. 狙いを定めたセキュリティ改善への投資

企業はこのような変化をサポートするために、適宜投資の優先順位を変えています。

86%

がハイブリッド従業員サポートのためにサイバーセキュリティの予算を増やしたと回答しています。[i]

74%

が2023年の予算が増えることを予想しています。[i]

HPセキュリティアドバイザリーボードのメンバーであるジャスティン・ボーン（Justine Bone）氏は、ハイブリッドセキュリティの重視は、取締役会が今日のリスク状況に目覚めたことに起因すると述べています。

「ランサムウェア攻撃のような目に見えるインシデントが増えたことで、上級管理職層の意識が高まったと考えています。これは予算計画にまで波及し、組織を保護する能力についてセキュリティリーダーを安心させています」

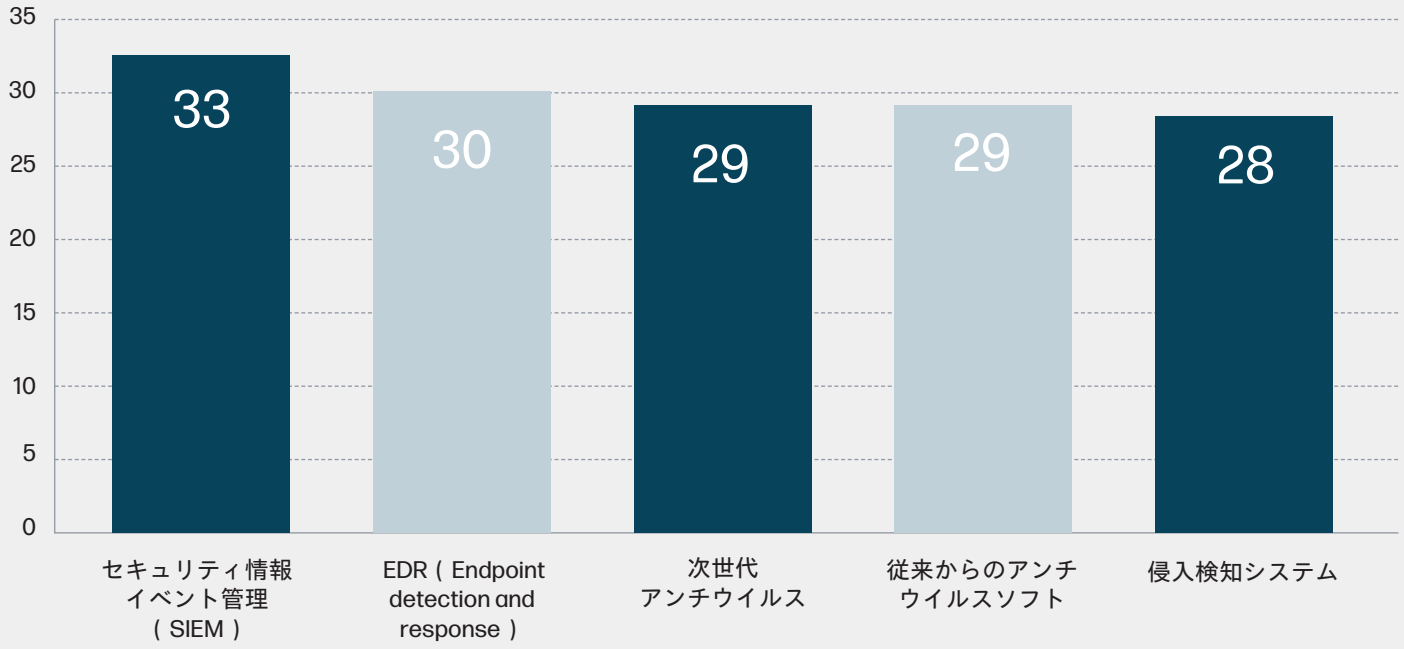
ジャスティン・ボーン（Justine Bone）氏
HPセキュリティアドバイザリーボードメンバー

予算は増えるかもしれませんが、投資が最も意味ある分野をピンポイントで特定することが重要です。HPの最高情報セキュリティ責任者（CISO）であるジョアンナ・バーキー（Joanna Burkey）は、「どこに投資すべきかを意図することが重要です」と述べています。「優れたガバナンスとは単なるコンプライアンスにとどまらず、予算も含めた会社のリソースを適切に扱うことです。セキュリティの問題は山積しており、どの分野が最もリスクにさらされているかを理解することが重要です」

3. エンドポイント保護へシフト

以上のことから、ハイブリッドワーカーを保護するためのエンタープライズ企業の戦略には、微妙ながらも顕著な変化が生じています。これまでの境界の外から企業に接続する従業員やデバイスが増えるにつれて、サイバーセキュリティテクノロジーは、ネットワークからエンドポイントへと向かっています。

ハイブリッドワーカーを保護するために導入または重視されているセキュリティツール[i]



セキュリティ情報イベント管理（SIEM）によるセキュリティ運用（SecOps）能力の強化に加え、企業はEDR（Endpoint Detection and Response）や次世代アンチウイルス（NGAV）ソリューションに新たな重点を置いています。

4. ゼロトラストの採用

セキュリティリーダーは、現在のセキュリティ体制のメリットを実感しており、75%がハイブリッド従業員を脅威から守る能力に自信を持っています。[i]また、改善の余地があることも認識しています：例えば、35%は、ハイブリッド従業員に対する自社のセキュリティ体制に急を要するギャップがあると回答しています。[i]この問題に対処するため、多くの企業は、既知のデバイスや企業ネットワーク内という理由で「安全」だと決めつけない、ゼロトラスト・アプローチを選択しています。ゼロトラストモデルでは、サービス、ファイル、アカウントなどのリソースを保護するために従来のようなネットワークセグメントではなく、認証と認可が使用されます。[ii]

5. マネージドセキュリティサービスプロバイダ（MSSP）の利用

適切なサイバーセキュリティツールの導入はハイブリッドワーカーの安全確保に貢献しますが、多くのセキュリティリーダーは保護の一部を提供するサードパーティを信頼し利用しています。

3分の2以上（67%）が現在MSSPを利用しており、さらに28%がMSSPを検討中です。MSSPを利用しているセキュリティ・リーダーの半数近く（49%）が、特にハイブリッドワーカーの保護のために利用していると回答しています。[i]

ボーン氏は、MSSPが社内の既存の能力をどのように高めることができるかを検討するよう企業に勧めています。「MSSPを利用することで、企業はその責任を分け合うことができます」と彼女は述べています。「これは、サイバーセキュリティの人材がなかなか見つからない場合や、社内にサイバーセキュリティの能力を組み込むための体制が整っていない場合に特に有効です」

「エンドポイントにフォーカスしたテクノロジーは、ハイブリッド組織において重要性を増しています。企業がゼロトラストモデルを受け入れているためです。これは、我々のお客様にとって最もホットな話題の1つです。

私たちの最大の顧客の1社は、『社内ネットワークを完全になくす』ことを検討しています。我々はネットワークアクセスの制限よりも、セキュリティとハイブリッドワーカーの自由を両立することが可能な新しいアーキテクチャに焦点を当てています」

アレックス・サッチャー（Alex Thatcher）
クラウドクライアント担当ディレクター、HP Inc

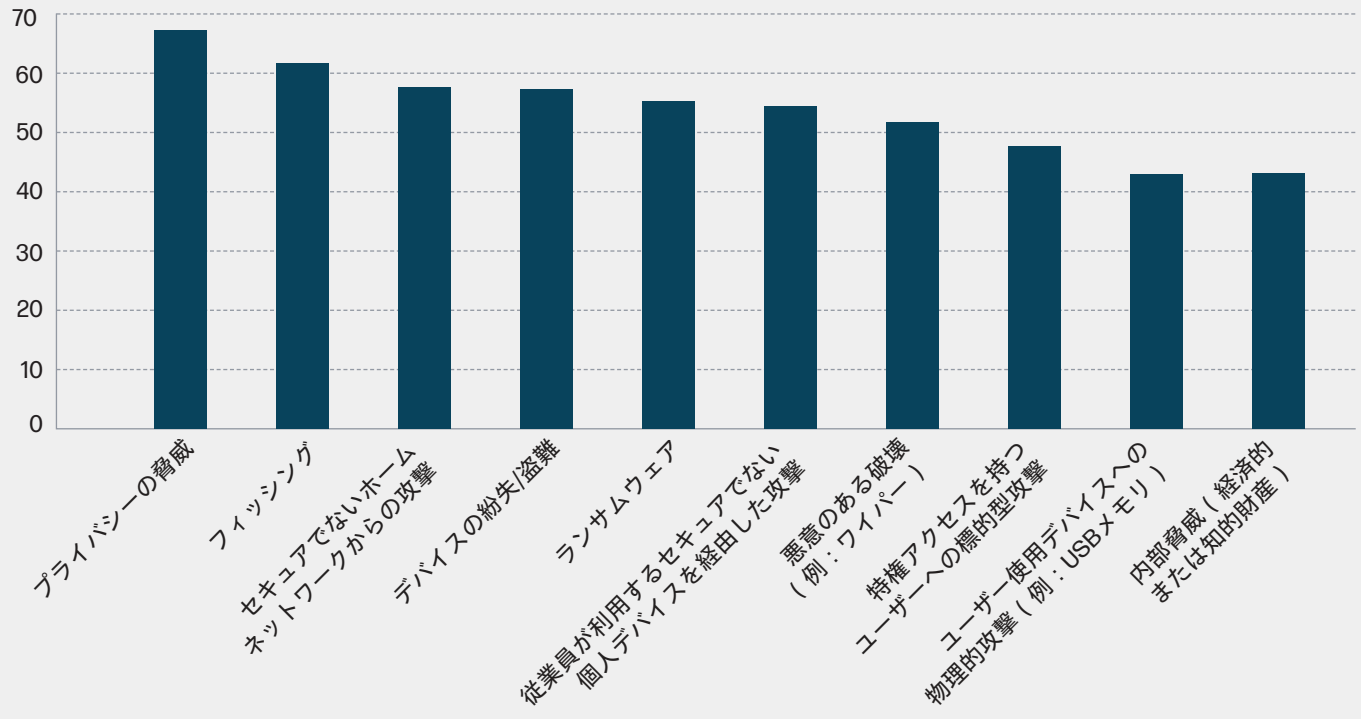
脅威の現状の特定

セクション 02

組織が「どこでも仕事（Work from everywhere）」モデルに移行する中、セキュリティリーダーは、これがビジネスリスクにどのような影響を与えるかをよく理解しています。そして、さまざまな外部脅威を特定しそれらに対処するための行動を起こしています。

我々の調査では、これらのリーダーは全体的にサイバーセキュリティの脅威を痛切に認識していることがわかりました。また、トップ10のうち9つが従業員のエンドポイントデバイスに関するものでした。

セキュリティ脅威に対する現在の懸念レベル[i]



従業員や会社による不注意な情報漏えい、コンプライアンスの不備など、プライバシー侵害も大きな関心事となっています。実際これらの脅威は、ランサムウェアやビジネスメール詐欺といった他の脅威を差し置いて、リーダーが最も懸念している脅威となっています。

ここで、セキュリティ機能を内蔵した最新のデバイスがソリューションの一翼を担います。ハイブリッドワーカーにこれらのデバイスを導入することで、エンドポイントでの侵害を防止、検知、封じ込めをすることができ、セキュリティリーダーを安心させることができます。また、プライバシー侵害（企業環境の外にデータが漏れること）を防ぎ、企業のゼロトラストへの取り組みを支援することにもつながります。

「エンドポイントの保護をマスターした組織は、ハイブリッド時代に最も強い組織となるでしょう」と、HP Inc パーソナルシステム セキュリティグローバル責任者イアン・プラット（Ian Pratt）博士は述べています。「優れたエンドポイントセキュリティはユーザーを保護するだけでなく、ITチームの信頼度を高め、分散した従業員をよりよく監督し管理することを可能にします」

ハイブリッド企業の次なる展開への備え

今後12ヶ月間について尋ねたところ、回答者はハイブリッドワーカーのエンドポイントに関連するいくつかのリスクを指摘しました：

36% は従業員のセキュアでないホームネットワーク経由の攻撃を懸念しています。[i]

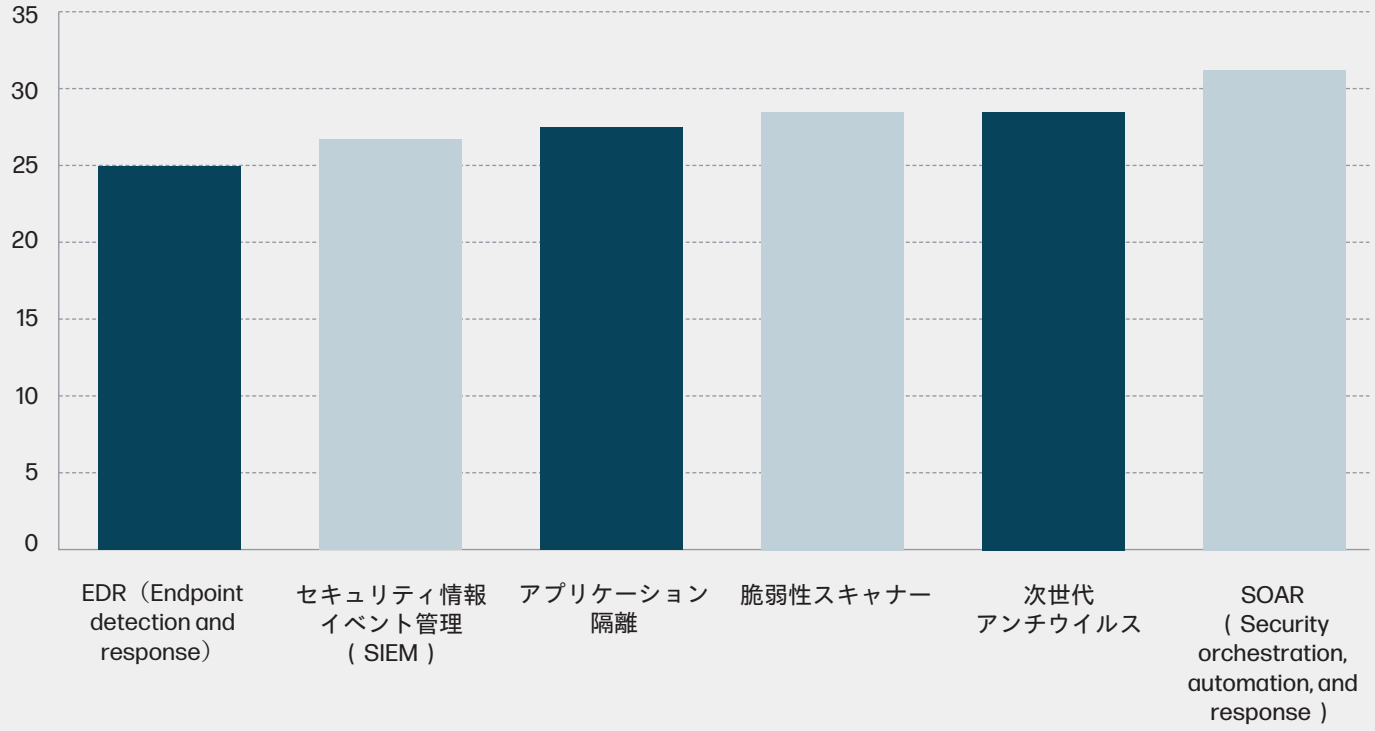
30% は従業員が使用するセキュアでない個人デバイスを経由した攻撃について懸念しています。[i]

30% はユーザー使用デバイスへの物理的攻撃（例：侵害されたUSBメモリ）を懸念しています。[i]

上記のような問題は決して新しいものではありません。多くのリーダーが大規模なハイブリッドワークが普及する以前から、これらの問題に取り組んでいましたが、 従業員のワークフローを邪魔することなく、強固な保護を提供するソリューションを見つけた企業はそう多くはないでしょう。予め組み込まれたセキュリティがこの問題を解決してくれます。企業は、ハードウェア、ファームウェア、OS、アプリケーションの各層でセキュリティ機能を備えたソリューションに価値を見いだし始めているのです。

実際、セキュリティリーダーは、エンドポイントに特化したセキュリティと、分散した従業員を監督するためのツールへの投資を倍増させようとしています。これらは、組織全体でゼロトラストを展開する際に役立つものです。 今後12カ月間に導入する予定のテクノロジーの上位は、SecOpsツールとエンドポイントプロテクションの組み合わせです。

セキュリティリーダーが今後12ヶ月で
導入する予定のテクノロジー[i]



ボーン（Bone）氏は、デバイスベースのセキュリティは、ハイブリッドセキュリティ戦略にとって重要な第一歩であると指摘しています。「『セキュア・バイ・デフォルト』が期待されるようになりました。これは、使い勝手に影響を与えないセキュリティ機能がデバイスに予め組み込まれていることを意味します」と彼女は述べています。「そして、ハイブリッド従業員とハイブリッドセキュリティチーム自体の複雑さが、組織が求める監視と制御を提供するSIEMとSOARの導入を後押ししています」

特に隔離技術は、ほとんどの組織でハイブリッド保護戦略の重要な要素となっているようです。潜在的な感染が広がらないように、タスクやアプリケーションをインフラストラクチャの他の要素から分離することに価値を見出しています。

- 79%が「ハイブリッドワーク中のデバイスを保護するために、隔離技術がポイントになる」ことに同意しています。[i]
- セキュリティリーダーの30%が未知で潜在的有害なドキュメントやリンクに対処するために、現在アプリケーション隔離を利用しています。[i]
- さらに28%が今後12ヶ月以内に導入する意向であり、近い将来に導入するツールとして3番目に人気のあるツールとなるでしょう。[i]

「今日のマイクロ仮想化技術は、Eメールの添付ファイルを開いたり、未知のリンクをクリックしたりといった潜在的にリスクの高い作業を、デバイス内の隔離されたコンテナで実行できることを意味します」とプラット（Pratt）博士は述べています。「以前は軍事組織や政府機関だけが利用していましたが、より多くの組織が利用できるようになり、エンドユーザーが透過的に利用できるようになりました」

用語集：ハイブリッドワーカーの保護

今回の調査でセキュリティリーダーの間で人気が高まっている、あるいは議論のテーマとしての要求が増えている技術として、以下のようなものが浮かび上がりました。

エンドポイント

ネットワークに接続されたリモートコンピューティングデバイスで、一般的にはユーザーまたは環境とのインタラクションに使用されます。（例：PC、プリンター、スマートフォン、IoTデバイス）

ゼロトラスト

かつて企業は、すべてが会社の所有物である信頼できるデバイス、ネットワーク、場所に基づきセキュリティポリシーを決めていました。ハイブリッドワークとクラウドは、リソースがどこにあろうと、どの場所やデバイスからのリクエストであろうと、認証と認可に基づいてリソースへのアクセスを許可する、新しいゼロトラスト時代をもたらしました。

マネージドセキュリティサービスプロバイダ（MSSP）

企業のセキュリティ機能を支援するために、外部の専門知識やリソースを提供する組織です。MSSPは、24時間365日の監視やオフィス外の従業員へのリモートサポートなど、自社で提供することが困難なビスを多数提供しています。

EDR（ENDPOINT DETECTION AND RESPONSE）

ユーザーデバイス（PC、ノートPC、モバイルなど）のシステム動作を監視し、疑わしい行動を検知した際にアラートを発するテクノロジーです。また、EDRソリューションは脅威を封じ込め、ITチームが適切に対応するための支援を行います。

CASB（CLOUD ACCESS SECURITY BROKER）

クラウドサービスは、今日のハイブリッド組織に不可欠です。CASBは、ITチームがクラウドリソースへのアクセスを管理・制御することを容易にします。不正あるいは悪意のあるユーザーへのアクセスを制限しながら必要なサービスを提供することにより、ITチームは従業員のクラウドリソースへのアクセスを簡素化することができます。

次世代アンチウイルス

従来のアンチウイルスソフトは、シグネチャに依存して既知のマルウェアを検知し検疫していました。 次世代アンチウイルスは、AIと機械学習を使用して、エンドポイント上の正常な動作を識別して脅威を阻止します。

アプリケーション隔離

アプリケーション隔離は、リスクの高いアクティビティを使い捨ての仮想コンテナ内に隔離することで、既知および未知の脅威からエンドポイントを保護します。例えば、Eメールの添付ファイルやWebリンク、ブラウザのダウンロードに含まれる悪意のあるコンテンツに「うっかり」にアクセスしようとするユーザーを保護することに有効です。

結論

ハイブリッドワークがこれほど早く常識になったということは、大企業であっても変化に対応できる可能性があることを示しています。実際、このような変化を遂げることで、より強くレジリエンスを持つ組織になっているのです。

ジョアンナ・バーキー（Joanna Burkey）
HP最高情報セキュリティ責任者
（CISO）、HP Inc

セキュリティリーダーは、この課題を明確に認識し、その多くを克服し、さらに防御を強化しようとしています。ハイブリッドワーカーが進化し続けるにつれて、攻撃者が彼らに対して繰り出す脅威も進化していくでしょう。防御側が防御を維持し、理想的には向上させたいのであれば、立ち止まっているわけにはいきません。

投資の優先順位をどこに置くかを正確に把握し対策を行うことは、個々の企業、そのリスク許容度、そして現在の市場ポジションに依存します。しかし、本レポートの調査結果は、ハイブリッドセキュリティへの方向性を示唆するものです。

エンドポイントは、攻撃の標的となっているので、依然として防御の中心です。そのため、我々はセキュリティリーダーに、ハイブリッドセキュリティ戦略においてエンドポイントを最重要視することをお勧めします。

隔離技術は、多くのナレッジワーカーを標的とする攻撃の影響を軽減することで、その脅威を軽減することができます。また、従業員やリソースが自社ネットワークの外に置かれることが多くなった企業にとって、ゼロトラストアプローチは理にかなっています。最後に、多くの企業がMSSPが自社のレジリエンスを向上させるのに役立つことを理解するでしょう。

ハイブリッドワーカーの進化に伴い、ビジネスリスクも増加しています。重要な分野に的を絞って投資することで、セキュリティリーダーは変化を先取りし、組織を保護することができます。

レポート寄稿者

ジョアンナ・バーキー（Joanna Burkey）
HP最高情報セキュリティ責任者（CISO）、HP Inc

イアン・プラット（Ian Pratt）博士
HPパーソナルシステムズ事業セキュリティ部門グローバル責任者、HP Inc

アレックス・サッチャー（Alex Thatcher）
クラウドクライアント担当ディレクター、HP Inc

ジャスティン・ボーン（Justine Bone）氏
HPセキュリティアドバイザリーボードメンバー

HP Wolf Securityについて

HP Wolf Securityはハードウェアで強化されたセキュリティとエンドポイントに特化したセキュリティサービスによるHPのポートフォリオの一部で、組織がサイバー犯罪者からPC、プリンター、そして人々を保護できるように設計されています。

HP Wolf Securityは、ハードウェアレベルから始まり、ソフトウェアやサービスに至る、包括的なエンドポイント保護とレジリエンスを提供します。https://jp.ext.hp.com/business-solution/wolf/をご覧ください。

メソドロジー

[i]HPは従業員数2,500名以上の企業のセキュリティ意思決定者168名を対象に調査を実施しました。調査は、2022年7月から8月にかけて、米国、英国、フランス、ドイツ、日本の各地で行われました。

すべてのセキュリティリーダーは、サイバーセキュリティオペレーションチームを監督または管理しています。

ハイブリッド組織とは、オフィスで働く従業員、リモートで働く従業員、あるいはその両方が混在するさまざまな従業員を持つ組織と定義されます。

リファレンス

[ii] 米国立標準技術研究所（NIST）、Zero Trust Architecture (2020) [オンライン] https://www.nist.gov/publications/zero-trust-architecture

HP Wolf Security for BusinessはWindows 10または11 Pro以上が必要で、HPのさまざまなセキュリティ機能を含み、HP Pro、Elite、RPOS、Workstation製品で利用可能です。含まれるセキュリティ機能については、製品詳細をご覧ください。