omnissa®

可視化なくしてセキュリティなし。AIOpsで実現するゼロトラストワークスペース

鈴木立夫 (Suzuki Tatsuo)
シニアテクノロジストラテジスト, テクニカルサービス本部
Omnissa Japan 合同会社

14th April, 2026

Agenda

Omnissa 会社概要

ゼロトラストを阻む「見えないリスク」の実態

セキュリティ衛生の盲点と運用自動化への障壁

AIOps による「深い可観測性」と成果ベースの管理

Omnissa による企業デバイス AIOps の実現

まとめ

Omnissa 会社概要

スマートでシームレスかつ安全な
従業員エクスペリエンスの提供により
働く人々が勤務場所を問わず
最高の仕事ができるよう支援します

Omnissa 会社概要

新生

旧VMware EUC部門から独立

2024年に
デジタルワークスペース専業の
独立企業として誕生

スケール

数百万のエンドポイントを
グローバルで管理

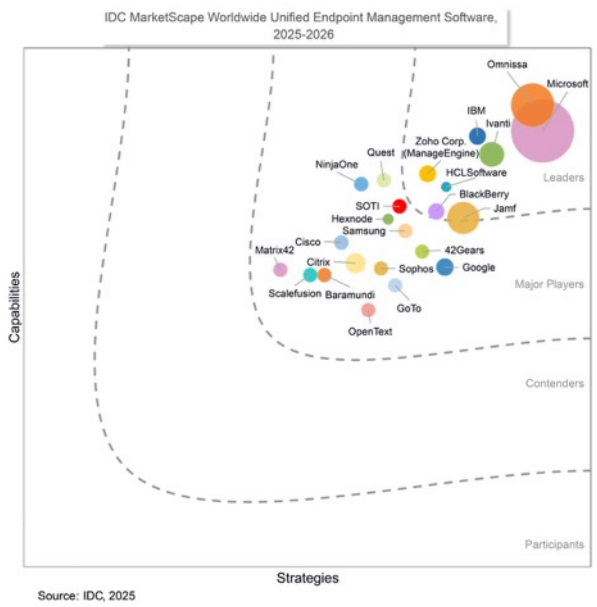
エンタープライズレベルまで
サポートする基盤と実績

外部評価

IDC MarketScape の
統合エンドポイント管理に
関する4つカテゴリにおいて
リーダー

UEM 評価に関する 2025-2026 年版 IDC MarketScape において 4つのカテゴリーで「リーダー」に選出

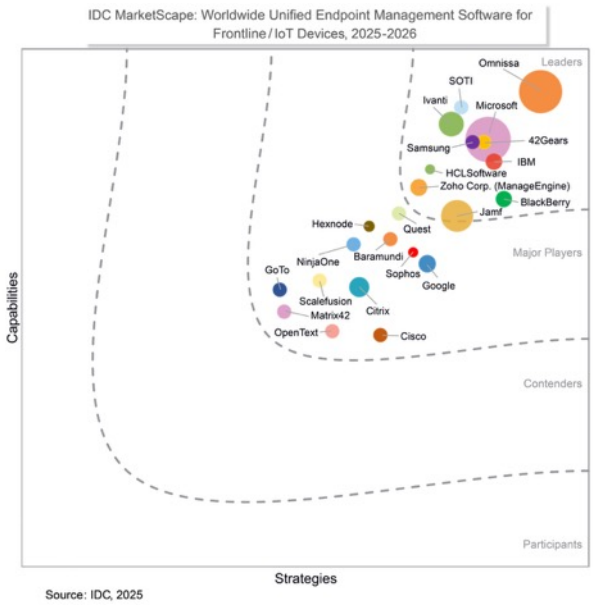
統合エンドポイント管理 （UEM） ソフトウェア



IDC MarketScape: Worldwide Unified Endpoint Management (UEM) Software 2025-2026 Vendor Assessment (IDC #US53003125), Phil Hochmuth, December 2025

7回目のリーダー

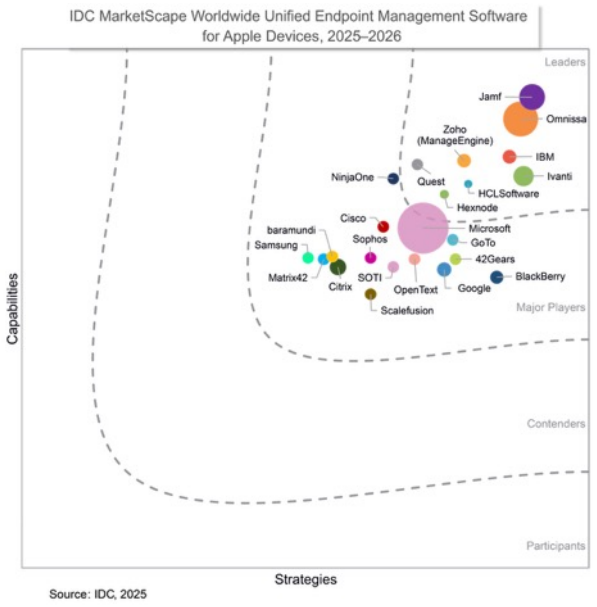
UEM for フロントライン/IoT



IDC MarketScape: Worldwide Unified Endpoint Management Software for Frontline/IoT Devices 2025-2026 Vendor Assessment (IDC #US53003325), Phil Hochmuth, December 2025

7回目のリーダー

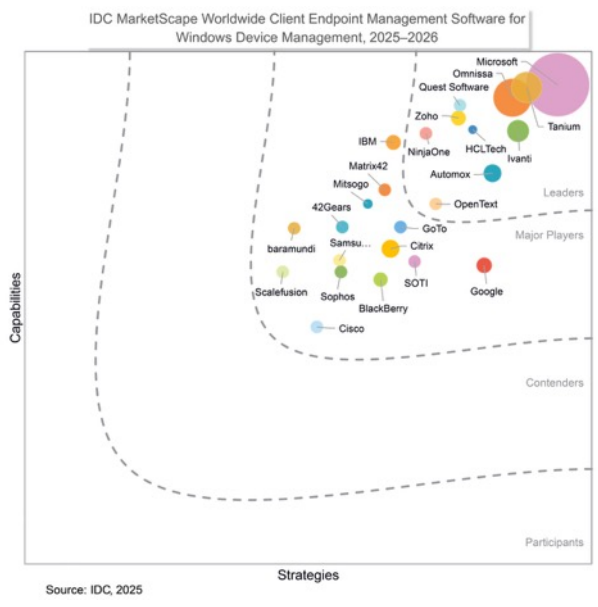
UEM for Apples デバイス



IDC MarketScape: Worldwide Unified Endpoint Management Software for Apple Devices 2025-2026 Vendor Assessment (IDC #US53003225), Phil Hochmuth, December 2025

4回目のリーダー

クライアントエンドポイント管理 for Windows デバイス管理



IDC MarketScape: Worldwide Client Endpoint Management Software for Windows Device Management 2025-2026 Vendor Assessment (IDC #US53002925), Phil Hochmuth, December 2025

2回目のリーダー

Disclaimer: IDC MarketScape vendor assessment model is designed to provide an overview of the competitive fitness of ICT (information and communications technology) suppliers in a given market. The research methodology utilizes a rigorous scoring methodology based on both qualitative and quantitative criteria that results in a single graphical illustration of each vendor's position within a given market. IDC MarketScape provides a clear framework in which the product and service offerings, capabilities and strategies, and current and future market success factors of IT and telecommunications vendors can be meaningfully compared. The framework also provides technology buyers with a 360-degree assessment of the strengths and weaknesses of current and prospective vendors.

omnissa

デジタルワークスペースの現状 2026

概要

- 2025年の世界中・17業種における数百万の端末テレメトリを匿名集計分析
- AI 活用拡大と端末多様化で、IT運用の可視性不足が顕在化
- 観測性強化が生産性・セキュリティ最適化の鍵と結論

https://omnissa.link/sodw2026

ゼロトラストを阻む「見えないリスク」の実態

「運用ポリシー適用＝安全、安定」という誤解

リスク対策のためのルールを管理するだけでは判明しない“見えないリスク”

錯覚

- ✓ 標準化された管理ツールの導入
- ✓ セキュリティポリシーの適用
- ✓ 定期的なデバイス交換

すべてを
「会社としての標準ルールによる管理」
とすることで安全・安定であると思い込む

現実

- ✓ 従来テクノロジーの保守
- ✓ 非管理アプリのシャドーIT対策
- ✓ ユーザー体験の低下

匿名化された数百万台の
稼働テレメトリデータが裏付ける
見えないリスク

AIOps とデバイスデータよる深い可視化がゼロトラストワークスペースに不可欠

見えないリスク：IT 環境の分散化と複雑化

“一人一台の Windows PC ”を前提としたレガシーな管理アプローチは破綻

北米, 西欧, アジアの労働者が
使用しているデバイス数は
3デバイス以上が一般的

1デバイス 16%
2デバイス 31%
3デバイス 24%
4デバイス 13%
5デバイス以上 15%

多くの企業では
従来のツールと最新の
エンドポイント管理ツールを
組み合わせて
5種類のエンドポイントOS
（Windows、macOS、iOS、
Android、Chrome OS）を
管理している

Source; IDC, Worldwide Enterprise Endpoint Device Management Survey, 2025, #US53140825, December 2025

見えないリスク：「標準化による管理」の限界とシャドー境界の拡大

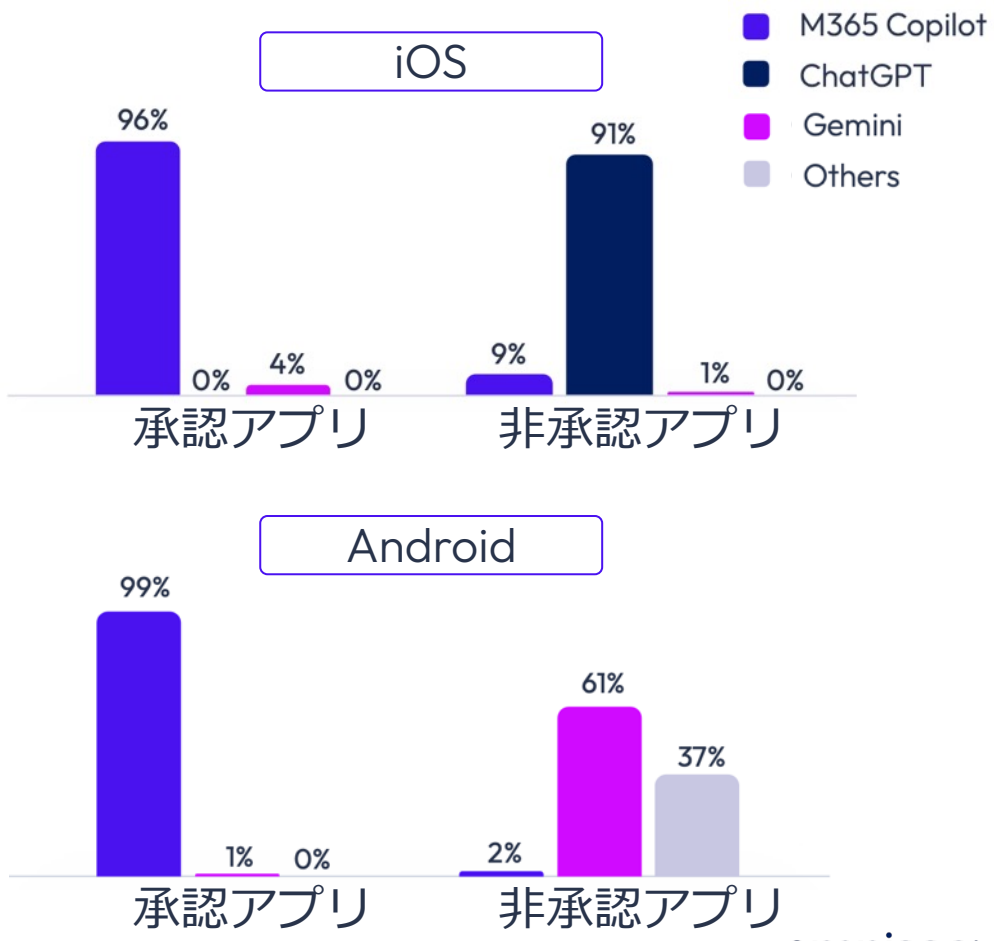
AIアシスタントはすべてのプラットフォームで YoY 1,000% 近くの導入増加率

企業版を導入したものの
個人版もインストールする傾向
(ex. Copilot vs ChatGPT)

企業利用版では
機能の不十分さや制約による
満足度のギャップを示唆

非承認アプリに企業情報を
入力することでデータ流出の可能性

AI アシスタント導入状況



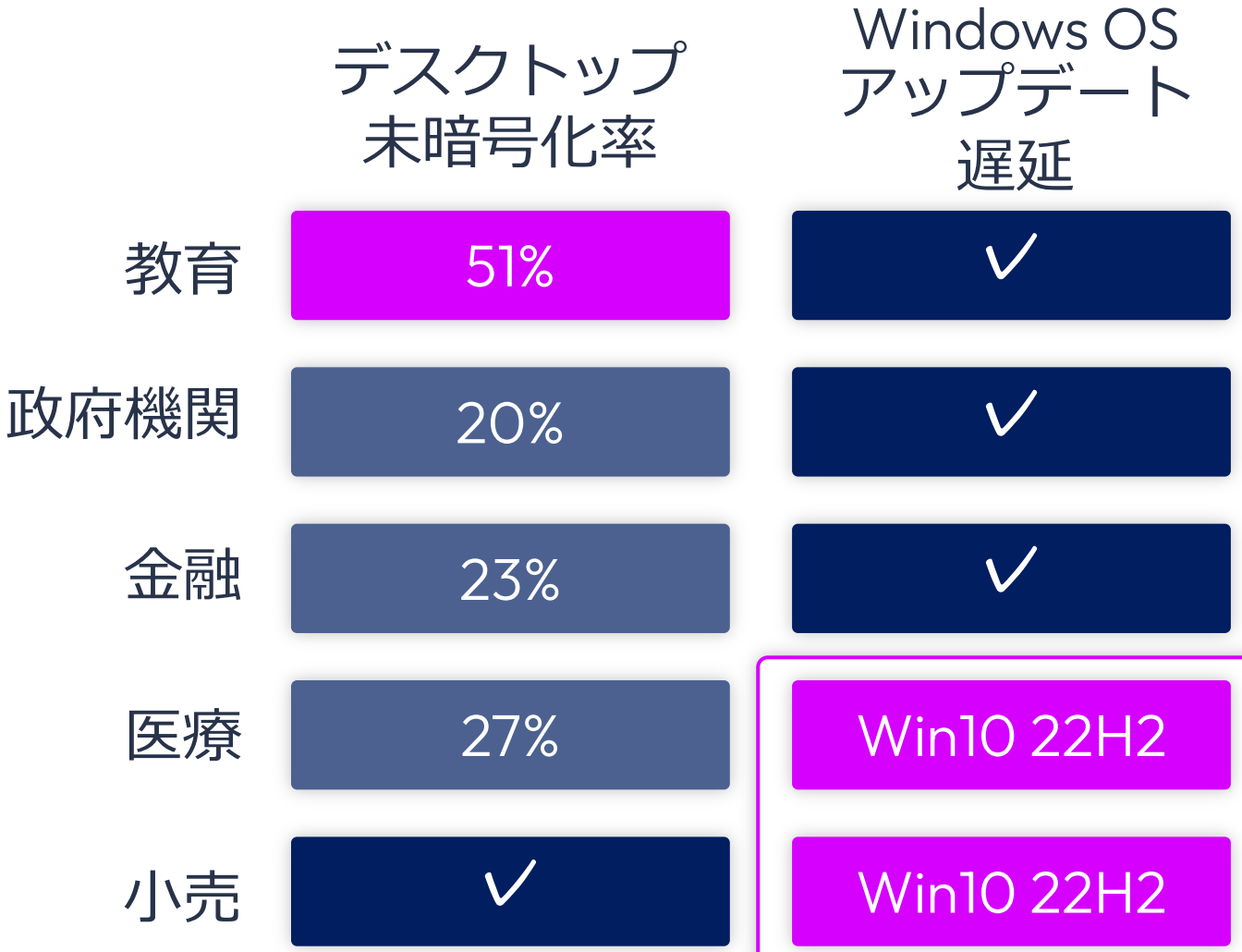
Source: Omnissa State of Digital Workspace 2026

omnissa

セキュリティ衛生の盲点と運用自動化への障壁と隠れている影

セキュリティ衛生の盲点：崩れゆくコンプライアンス

ポリシーベースの静的な管理はデバイスやユースケースの多様性に追いついていない



ポリシーを適用した事実は
その有効性を保証しない

持続的な観測性がなければ
重大な脆弱性が
IT部門の死角で増殖する

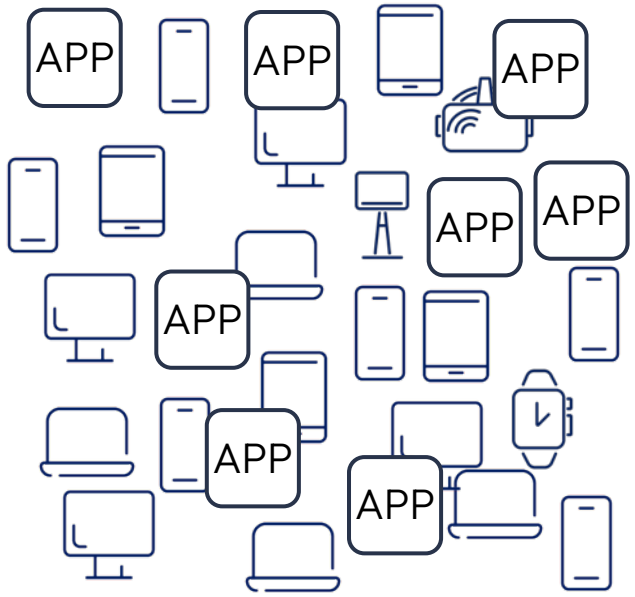
レガシーアプリ起因の
OSアップデートの遅延が
特に顕著

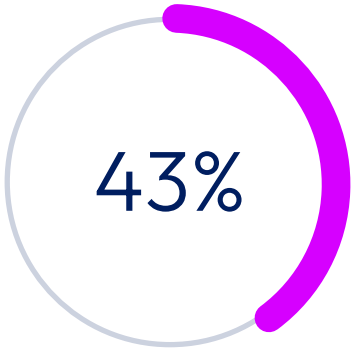
Source: Omnissa State of Digital Workspace 2026

運用自動化への障壁：手作業の限界が引き起こす「可視性の空白」

IT 部門は常にタスクに追われてる

デバイスとアプリの爆発的増加 ＋ リアクティブなチェックリスト管理 ＝ 見えないリスクの増加





Windows の OS アップデートはユーザー任せ

自動化に至までに既存で対応しなければならない作業が膨大に

Source; IDC, Worldwide Enterprise Endpoint Device Management Survey, 2025, #US53140825, Dec 2025

もう一つの影：生産性を奪う「声無きデジタルフリクション」

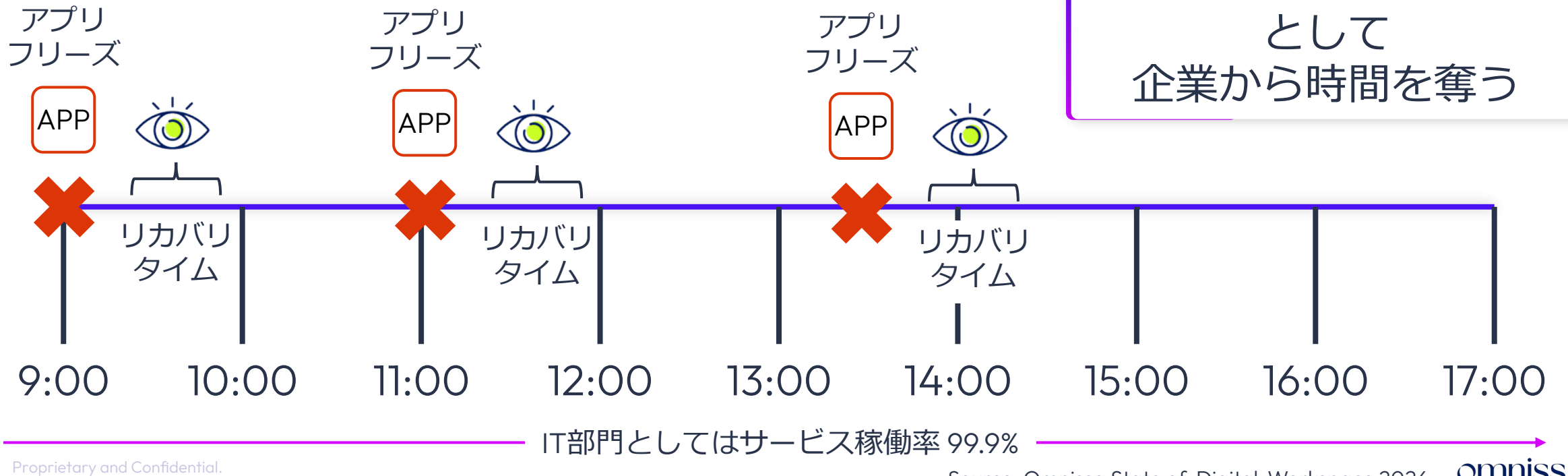
利用者の企業 IT の快適度にかかわる、デジタル従業員体験の低下

Windows アプリのハングアップ： mac の 7.5倍
Windows の強制シャットダウン： mac の 3.1倍

日常的なトラブルはユーザーの当たり前に

デバイスに問題発生後
集中力の復帰に
平均23分15秒

目に見えない生産性税
として
企業から時間を奪う



Source: Omnissa State of Digital Workspace 2026

omnissa

AIOps による「深い可観測性（オブザーバビリティ）」と成果ベースの管理

「深い可観測性」の獲得：あらゆる弱点を照らし出す

ハードウェアの挙動からユーザー体験に至るまですべてのコンテキストをつなぎ合わせる

見えないリスクに対処するためには
AIOpsを用いてデバイスの

ハードウェア状態

アプリの使用状況

ネットワーク品質

等のテレメトリデータと

利用者の感情

も統合的に収集・分析する

「深い可観測性」が不可欠

レイヤー 4
利用者の感情
(ex. Service Desk へのリクエスト)

レイヤー3
アプリ利用状況
(ex. クラッシュ, シャドーアプリ)

レイヤー 2
OS・設定・ネットワーク
(ex. パッチ状態, 証明書, NW品質)

レイヤー 1
ハードウェア状態
(ex. バッテリー, 温度)

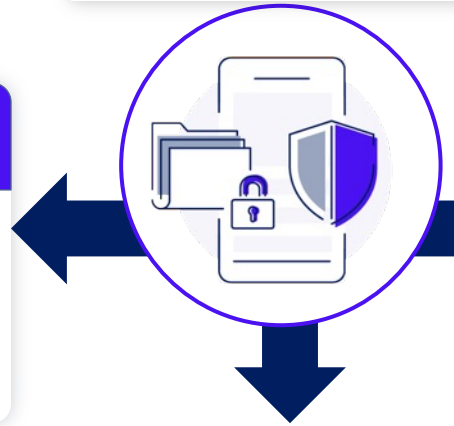
Source: Omnissa State of Digital Workspace 2026

omnissa

セキュリティエコシステムとの統合：コンテキストの共有

UEM に対する統合要件のトップ3

UEM



クラウドベースの ID システム

ユーザーの振る舞いや認証状態、
デバイスの正常性を紐付けて
条件付きアクセスを動的に実現

エンドポイントセキュリティ

脅威の検知と同時に
UEM側でデバイスを即座に
ネットワークから隔離

SIEM プラットフォーム

エンドポイントのリスクスコアを
正規化して全社的なセキュリティ
シグナルとして相関分析

コンテキストを共有した可視化こそがゼロトラストをさらに強固へ

Source; IDC, Worldwide Enterprise Endpoint Device Management Survey, 2025, #US53140825, Dec 2025

「成果ベース」の管理 ：ポリシー適用を超えた運用モデルの進化

ただデバイスを管理するのではなく管理をした上でビジネスがどう変化するか

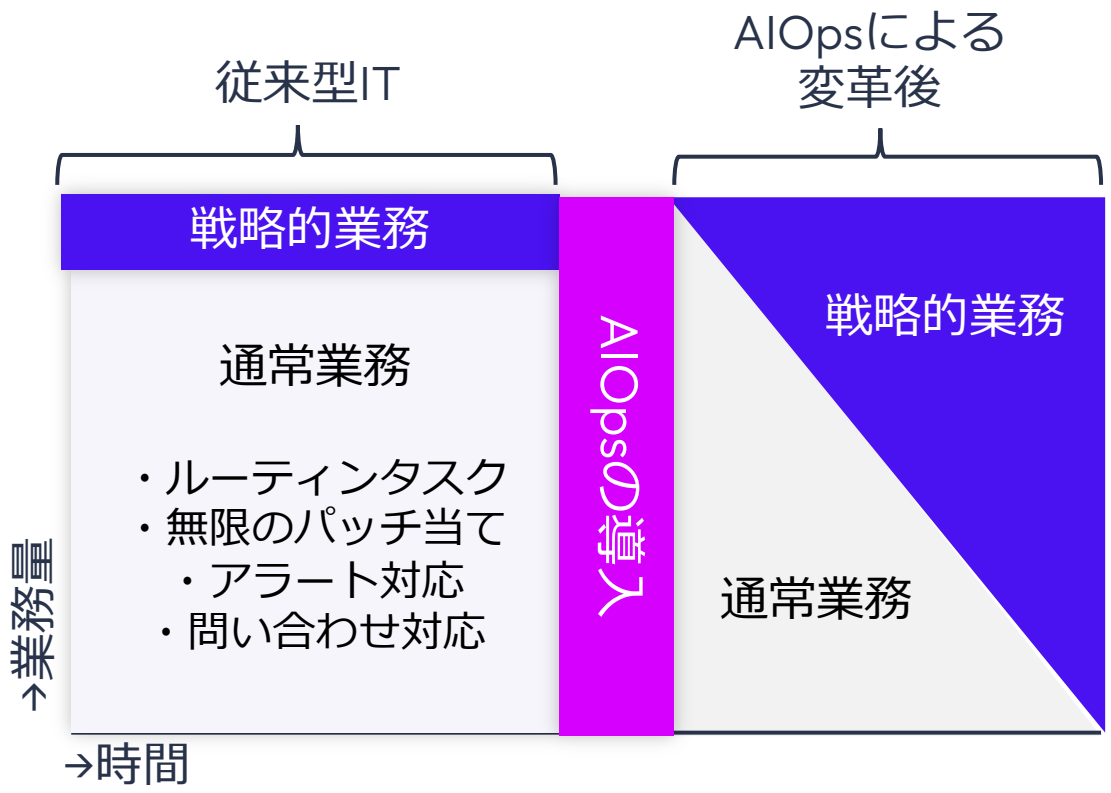
比較軸	従来型による管理	AIOps によるゼロトラスト
焦点	静的で画一的なポリシーベース	成果ベース （動的でビジネスの中断がないかを評価）
管理手法	サイロ化されたツール群	エンドツーエンドの総合的で深い可観測性
修復	人力での事後対応	自律的検知と自動修復
結果	ルーチンタスクとアラートの消化	戦略的業務とイノベーションへのシフト

2026 年、大企業も中小企業も同様に、ベンダーに対して、静的な強制から、「デバイスはパッチへの耐性がある」、「ユーザーは 8 時間のオフライン作業でも安全に作業できる」、「エンドポイントの AI ワークロードは許容可能なリスクとコストのパラメータ内で実行される」といった ビジネス中心の目標を捉える成果ベースの管理へと移行するよう求めています[1]

[1] Source; IDC, Five Trends to Watch in Endpoint Management in 2026, #US54178826, 2026

「成果ベースの管理」の成果：IT 部門は「戦略的」業務へ

通常業務を AIOps でコントロールすることで戦略的な攻めの IT を実現



現在、企業の半数以上が脅威の検出や
スクリプト生成といった戦術的な機能にAIを活用し
ており、60%以上が、AIによって俊敏性が向上し、
手動プロセスからスタッフを解放できる
と予測しています[1]

組み込みAIは、継続的な行動監視、リアルタイム
検知、自律的な脅威封じ込めアクションを通じて
エンドポイントセキュリティを変革し、
それによって検知および対応までの
平均時間（MTTD/MTTR）を短縮します[2]

AIOps は IT 管理者の仕事を奪うのではなく、ビジネス価値の生み出すための余白を創出

[1] Source; IDC, Five Trends to Watch in Endpoint Management in 2026, #US54178826, Jan 2026
[2] Source; IDC, Five Key Trends for Enterprise Client Computing Platforms in 2026, #US53134426, Feb 2026

モデル例：コンテキストアウェアな自律的アクセス制御

サプライチェーンのリスク最小化と生産性最大化のための統制方法

「サプライチェーンや委託先を狙った攻撃」が組織向け10大脅威の2位に位置しており
セキュリティ対策が手薄な子会社や委託先の端末が侵入の踏み台にされるリスクが継続している

深い可観測性の獲得

自社・委託先を含む
端末の老朽化や
セキュリティ逸脱を
横断的に把握

見えない経営リスクを
可視化

エコシステムとの統合・自動化

IAMや資産管理と連携し
リスクが許容範囲を超えた
端末を自動判定・制御

委託先端末の
アクセス制御と更新対応を
人手に頼らず実行

成果ベースの管理

「端末年数」ではなく
サプライチェーン全体で
安全かつ生産的に業務を
継続できているかを
成果指標として管理

ゼロトラストは IT 施策ではなく、経営成果を測るための指標

Source; IPA 情報セキュリティ白書2025 第1章コラム

Omnissa による
企業デバイス AIOps の実現

Omnissa Platform

ヒューマンエクスペリエンスを軸にデジタル業務を展開

+

エンドユーザー向け

ナレッジワーカーや現場の従業員など、
あらゆるペルソナ（職種・役割）に対して、いつでもどこでも安全で快適なデジタルワーク体験を提供

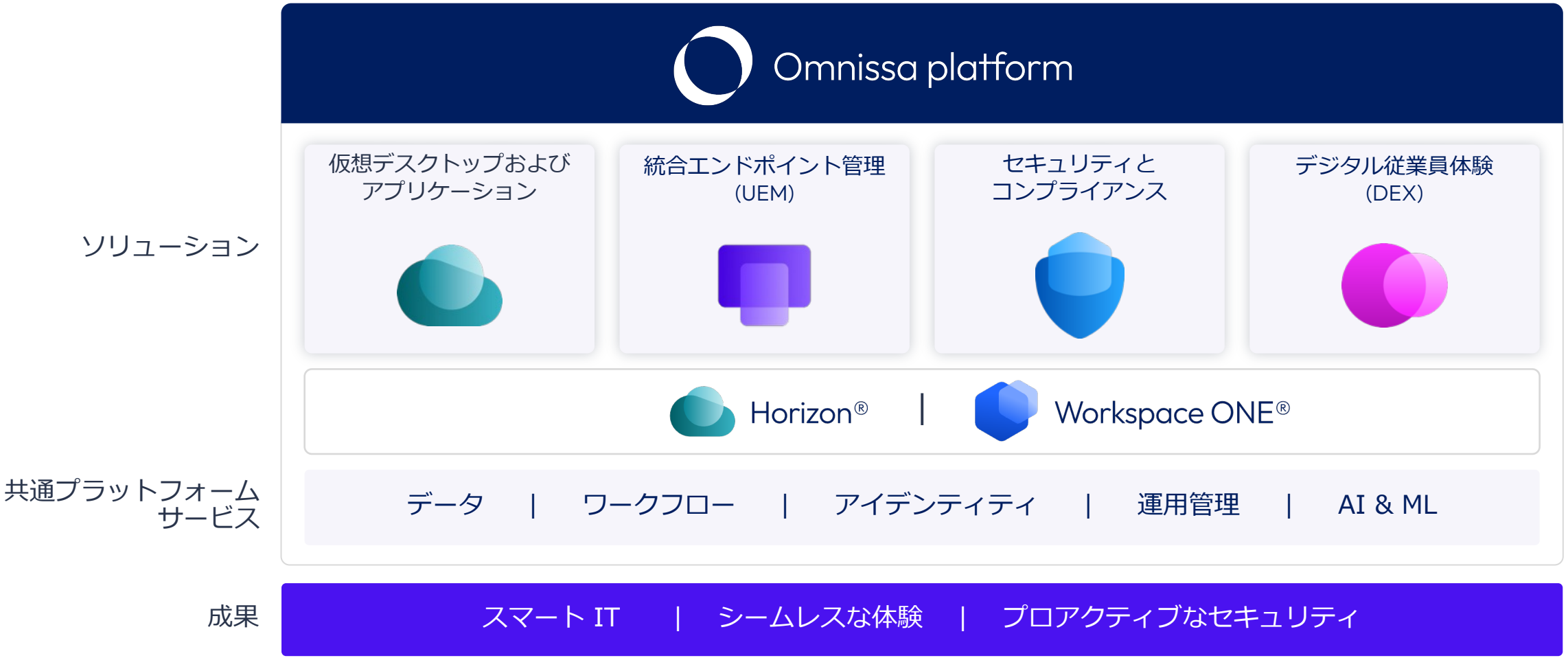
IT スタッフ向け

既存業務をシンプルにし
新たなニーズにも迅速に対応

omnissa®

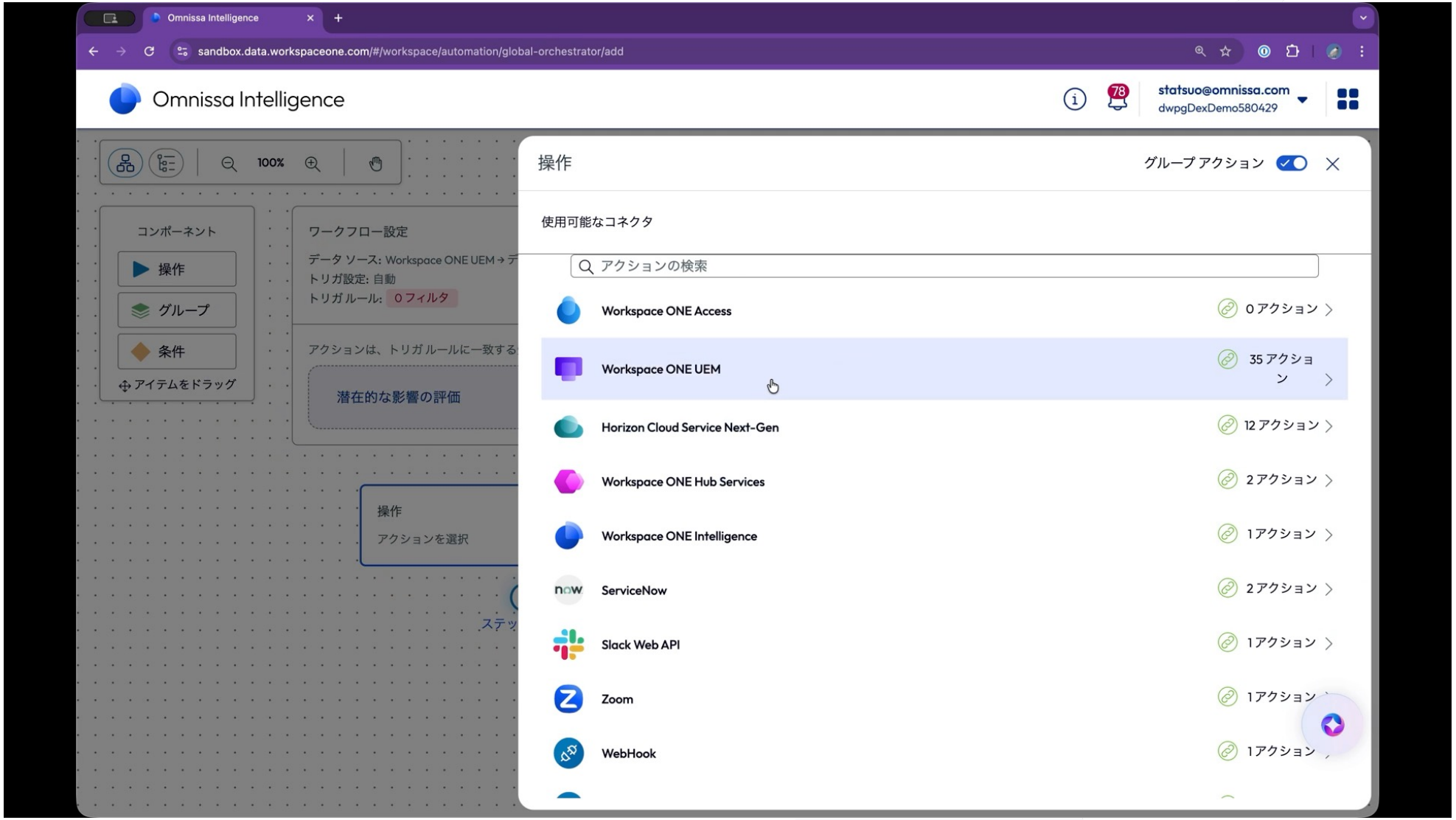
AI を搭載した次世代デジタルワークプラットフォーム

あらゆる場所で、スマートでシームレスかつセキュアな体験を提供するために



（デモ）スマートIT実現のための運用次世代化

コンテキストアウェアな自律的アクセス制御の支援例



（導入事例） Yapi Kredi 銀行

トルコ全土に展開するモバイルワークフォース

背景

- 9,500台のデバイス管理と機密データ保護の必要性
- 従来の支店モデルを超えた柔軟なサービス提供
- 政府のデジタル化と金融包摂方針への対応

課題

- 多様なOSとメーカのデバイス管理が困難
- Mac の管理不可、MFA未対応
- セキュリティ要件を満たせず
- 手動スクリプトへの依存と運用負荷

ソリューション

- Mac を含む全デバイスの統合管理
- Freestyle Orchestrator による自動化
- Omnissa Intelligence SDK でアプリ・ネットワークの可視化

成果

- MFA 導入によるセキュリティ強化
- iPad による現場業務の効率化と収益向上
- 自動 OS アップデートとリモートログ取得
- ユーザーからの感謝の声と苦情の減少

私たちの目標は、潜在的な問題を積極的に特定し、
自動的な予防措置を講じる自律型システムを構築することです。
Workspace ONE UEMは、その目標を達成するために
不可欠な要素です。

Uğur Koçer

Windows Applications Design and Planning Manager, Yapi Kredi Technology

まとめ

まとめ：AIOps で実現するゼロトラストワークスペースに向けて

さまざまなデバイスで企業価値を最大限に高めるために

すべてのデバイスに
深い可観測性と自動対応

セキュリティ
エコシステムとの統合

成果ベース管理で
IT 部門を
戦略家へシフト

成功の鍵は「継続的な可観測性」と「データ主導の自動対応」

omnissa

デジタルワークスペースの現状 2026

概要

- 2025年の世界中・17業種における数百万の端末テレメトリを匿名集計分析
- AI 活用拡大と端末多様化で、IT運用の可視性不足が顕在化
- 観測性強化が生産性・セキュリティ最適化の鍵と結論

https://omnissa.link/sodw2026

omnissa

omnissa®

ご静聴いただき
ありがとうございました