ivanti

Cybersecurity
INSIDERS

2023 Zero Trust 進捗レポート

ivanti.com/ja

概要

ゼロトラストは、「決して信用せず、常に検証する」という基本的な前提に基づいて構築されており、今日のサイバーセキュリティの実践における礎石となりつつあります。

ITおよびサイバーセキュリティに携わる431人を対象とした調査に基づく「2023Zero Trust進捗レポート」は、今日の組織におけるゼロトラストアクセスモデルをめぐる採用の増加、主要課題、効果的な戦略について包括的な分析を提供しています。

この調査では、回答者の 68% がゼロトラストアクセスモデルの採用を計画しているか、積極的に取り組んでいることが明らかになりました。ゼロトラストへの道筋において、企業はセキュリティへの全体的なアプローチに重点を置いており、57%がIDとアクセス管理（IAM）を優先し、52%がクラウドアプリケーションへのアクセスの安全性を目指している状態です。エンドポイントの検出と対応 （EDR）の補完や脆弱性の修正の改善とともに、これらの優先事項はゼロトラストセキュリティの実践が採用されつつあることを確認する内容となっています。

ネットワークリソースにアクセスするリスクのあるデバイスは、回答者の48%が最重要課題として挙げており、デバイスの厳密な検証と継続的な監視の重要性が強調される結果となっています。回答者の47%が懸念している従業員の過剰な特権アクセスは、ゼロトラストフレームワークで最小特権の原則を導入する必要性を強調しています。

多要素認証 （MFA） への投資は、回答者の 65%が最優先事項として挙げており、ゼロトラストフレームワークにおける重要性を強調しています。ほとんどの組織 （54%）は、ゼロトラストのために 2 ～ 4種類の製品を使用しており、導入で段階的なアプローチが取られていることを示唆しています。

サイバーセキュリティの状況が進化する中、ゼロトラストの原則を採用し、セキュリティの優先度をそれに合わせることは、組織がリスクを効果的に軽減し、資産を保護する上で極めて重要です。

私たちは、この重要な調査を支援してくださったIvantiに感謝するとともに、皆様のIT環境を保護するための継続的な「ジャーニー」に役立つリソースとなることを願っています。

どうぞよろしくお願いいたします。

ホルガー・シュルズ氏（Holger Schulze）

ホルガー・シュルズ氏（Holger Schulze）
CEO兼創立者
Cybersecurity Insiders

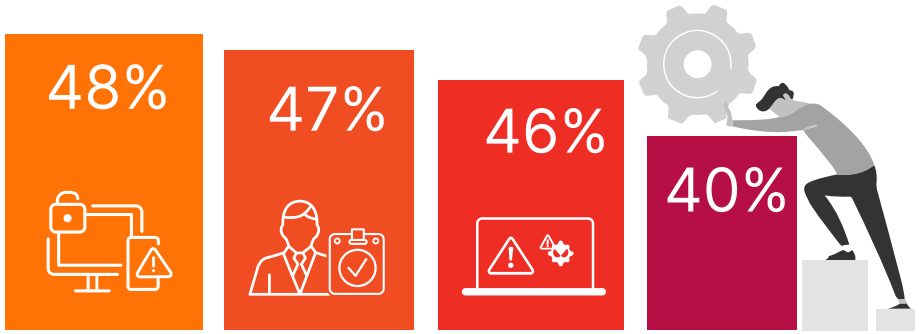
Cybersecurity
INSIDERS

セキュアアクセスの課題

組織がアプリケーションやリソースへのアクセスを確保する上で直面する最重要課題は、ゼロトラストの基本原則と密接に関連しています。 48%で最も懸念が大きいのは、ネットワークリソースにアクセスする危険なデバイスです。この課題は、信頼できるデバイスだけが機密リソースにアクセスできるようにする、ゼロトラストの厳格なデバイス検証と継続的な監視の必要性を強調しています。

従業員の過剰な特権アクセスも重要な課題であり、回答者の 47%が懸念事項として挙げています。ゼロトラストの文脈では、最小特権の原則を実施し、ユーザーが職務を遂行するために必要最小限のアクセス権しか付与しないことの重要性が強調されます。

アプリやリソースへのアクセス保護について、自社が直面している一番の課題は何ですか。[1] [n = 424]



ネットワークリソースにアクセスするリスクのあるデバイスのシャドーIT（未知、未承認、コンプライアンスに抵触するエンドポイント）

従業員の過剰な特権アクセス

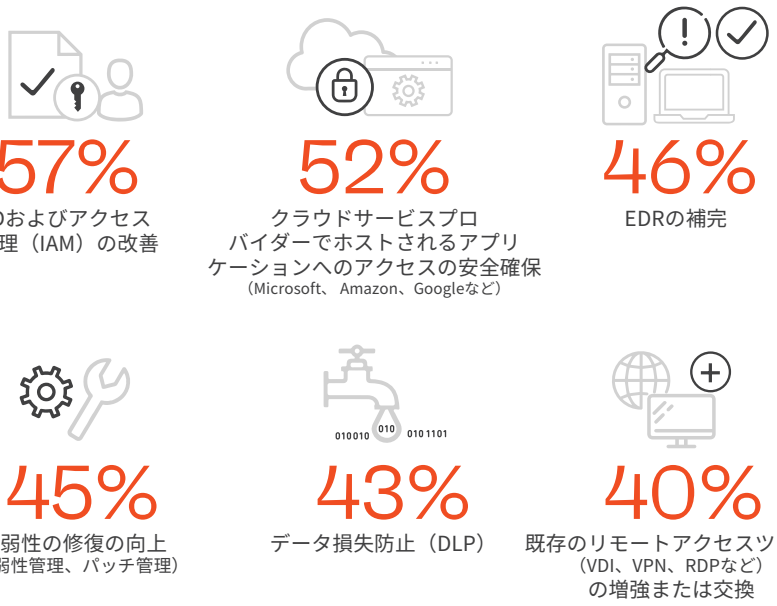
サイバー攻撃（サービス妨害、クロスサイトスクリプティング、中間者攻撃、フィッシングなど）

シャドー IT

ゼロトラストの重点を反映したセキュリティの優先順位

選ばれたセキュリティの優先順位は、組織がセキュリティに全体的なアプローチを採用し、複数の保護レイヤーに対処していることを示唆しています。 IAM（57%）とクラウドアプリケーションへのセキュアなアクセス（52%）に対する強いフォーカスは、ゼロトラストセキュリティと大いに関係があります。なぜなら、これらの優先事項は、ユーザーとデバイスの IDを検証し、リソースへのアクセスを制御するという原則と一致しているからです。さらに、EDRの補完（46%）や脆弱性修正の改善（45%）に重点を置いているのは、継続的な監視とセキュリティ脅威への迅速な対応というゼロトラストの原則を反映しています。全体として、これらの優先順位は、組織が全体的なサイバーセキュリティ体制を強化するために、ゼロトラストセキュリティの実践を採用する傾向が強まっていることを示しています。

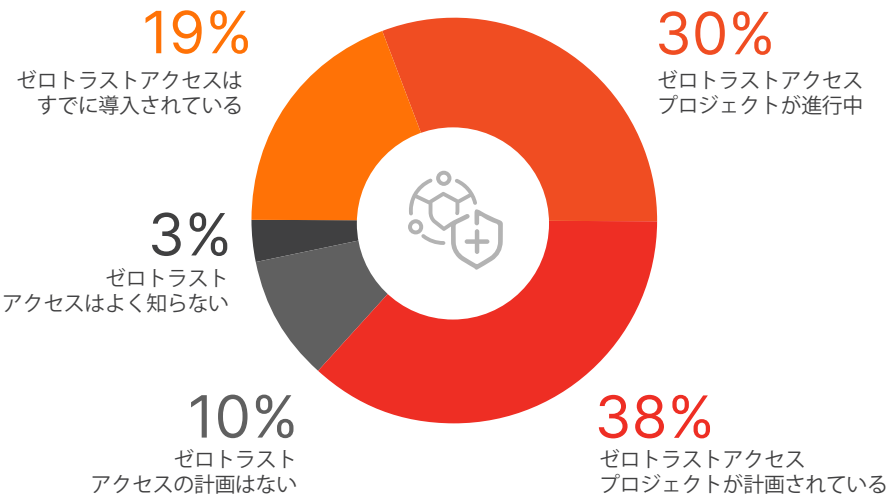
あなたの組織での現在のセキュリティの優先事項は何ですか。 [n = 421]



ゼロトラスト採用計画

ゼロトラストはすでに5社に1社(19%) の組織で導入されています。
回答者の大部分 (38%) はゼロトラストアクセスプロジェクトの実施を計画し、30%がすでに進行中のプロジェクトがあると回答しています。このことは、調査対象となった組織のほとんど (68%) が、ゼロトラストアクセスモデルの採用を計画しているか、積極的に取り組んでいることを示しています。

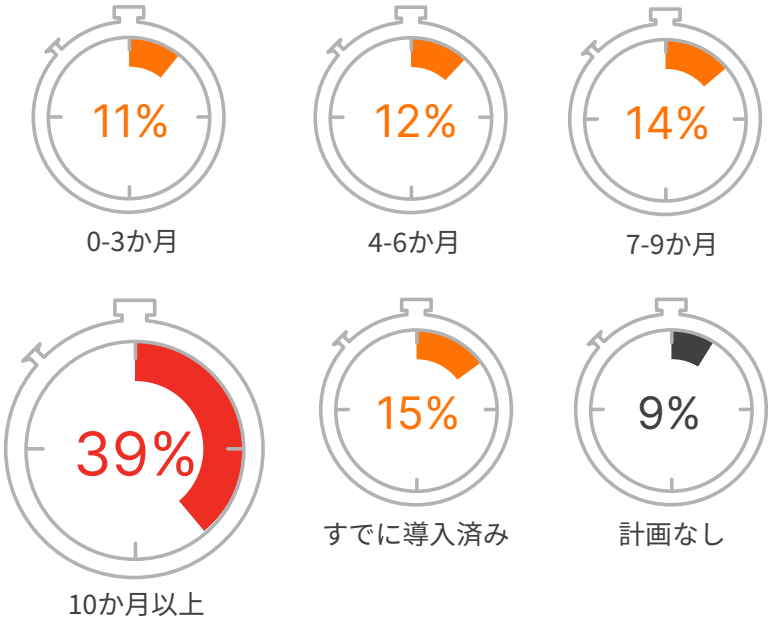
社内でゼロトラストアクセスモデルを採用する計画はありますか。[n = 424]



ゼロトラスト導入のタイムフレーム

ゼロトラストセキュリティの導入は、組織間でさまざまな割合で進んでいます。
かなりの部分がすでにフレームワークを導入していますが (15%) 、
他の部分は比較的早期にゼロトラストを導入する予定であり (37% が 9 か月まで) 、
大半のグループがゼロトラストセキュリティを完全に導入するには10か月以上かかると認識しています (39%) 。

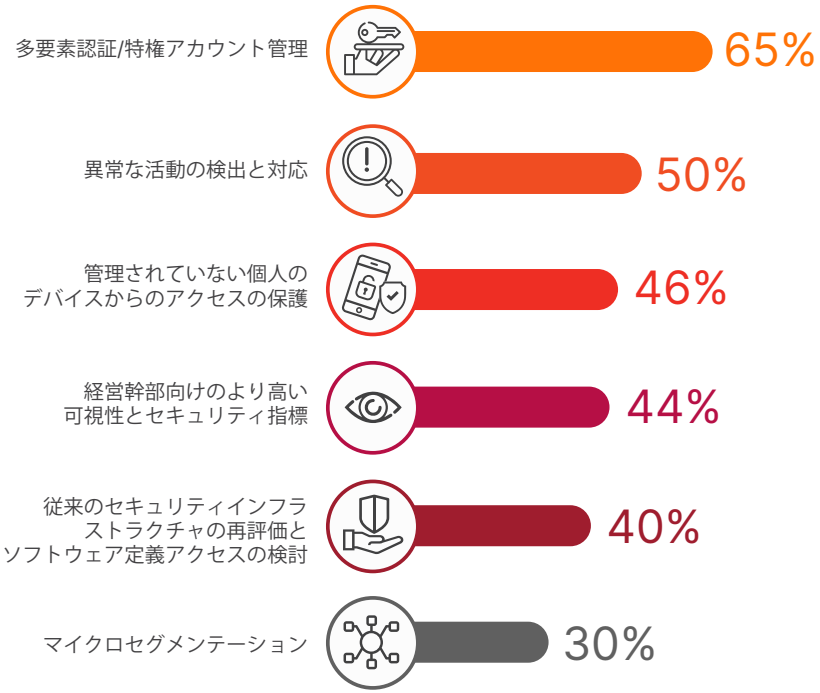
ゼロトラストセキュリティを導入する可能性が最も高い時期はいつですか。[n = 423]



セキュアアクセスの優先度

組織は、多要素認証（MFA）（65%）、リアルタイムの脅威検知 （50%）、個人デバイスからのアクセスの保護（46%）など、ゼロトラストの原則に密接に沿った複数のアクセスの保護に関する優先事項に注力しています。これは、「決して信用せず、常に検証する」というゼロトラストの原則によく合致しており、機密性の高いリソースへのアクセスを許可する前に、ユーザーが適切に認証され、承認されることを実現します。

今後 1〜2 年間において、セキュアアクセスの優先課題は何ですか。 [n = 430]

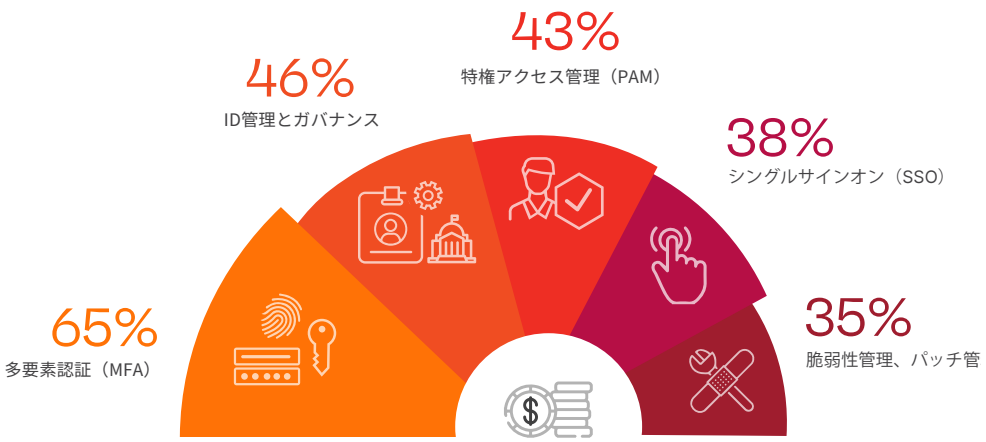


投資計画

IDアクセスおよびゼロトラスト管理に対する組織の投資の優先順位は、ユーザー認証の強化、アクセス権の管理、および全体的なシステムセキュリティの維持に集中しています。 ゼロトラストの重要な構成要素であるMFAは最優先事項として際立っており、回答者の65%が投資を計画しています。

これらの優先事項はゼロトラストの基本原則を反映しており、組織全体でこのセキュリティフレームワークを採用することが重視されるようになっていることを示しています。

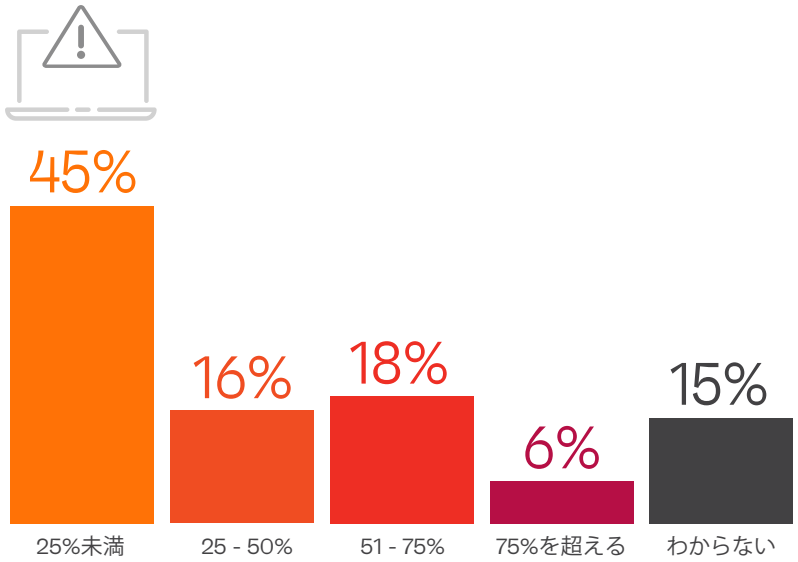
次のIDアクセス/ゼロトラスト制御のうち、あなたの組織で今後12か月で優先的に投資すべきことは何ですか？ 2 [n = 431]



過剰なアクセス特権のリスク

回答者の半数近く（45%）は、過剰な特権アクセスによるセキュリティインシデントの割合は25%未満であったと回答。このことは、過剰な特権アクセスは懸念事項ではあるものの、多くの組織では、セキュリティインシデントの主要因ではありません。 組織の 3分の 1（34%）が、過剰なアクセス権限に起因するインシデントの 25% ～ 75% を経験しています。 これらの調査結果は、過剰なアクセス権限に関連するセキュリティリスクを最小化するために、最小権限の原則であるゼロトラストを実施することの重要性を強調しています。

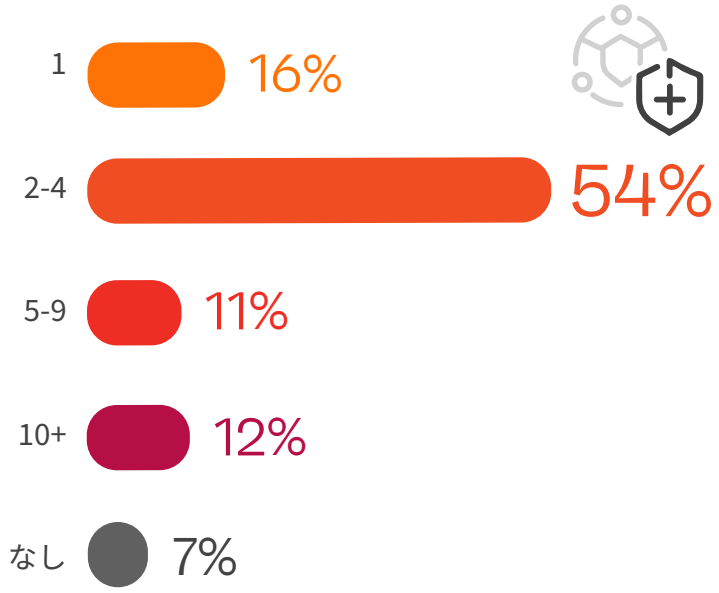
過去12か月間に発生した組織のセキュリティインシデントのうち、エンドユーザーが日常業務に必要な範囲を超えたアクセス権限を持っていたことが原因と思われるインシデントの割合はどのくらいですか？ [n = 431]



ゼロトラストへの階層的アプローチ

回答者の大多数（54%）は、ゼロトラスト・セキュアアクセスのために2～4の製品を使用しています。これは、ほとんどの組織がゼロトラストの実装に階層的なアプローチをとっており、アクセス管理、デバイス検証、ネットワークセグメンテーションなど、フレームワークのさまざまな側面に対応するために複数の製品を利用していることを示しています。ゼロトラストの文脈において、これらの調査結果は、組織が安全なアクセスプログラムを実施する際に、異なるアプローチと複雑さのレベルを採用することを推奨しています。

あなたの組織でゼロトラストのセキュアアクセスプログラムに使用する（または現在使用している）製品はいくつありますか？ [n = 429]



ゼロトラストのベストプラクティス

ゼロトラストとは、組織のネットワーク内に固有の信頼がないことを前提とし、すべてのユーザー、デバイス、要求について厳格な検証を実施するセキュリティモデルです。ゼロトラストを効果的に実施するために、組織は以下の重要なベストプラクティスを考慮する必要があります。

多要素認証（MFA）の導入:
従来のユーザー名やパスワードに加え、バイオメトリクスやトークンなど、複数の方法を用いて認証を強化します。

最小特権の原則の採用（POLP）:
職務を遂行するために最低限必要なアクセス権のみをユーザーに付与し、内部脅威やデータ漏洩を最小限に抑えます。

デバイスの継続的な検証と監視:
厳格なデバイス検証と継続的な監視を実施することで、信頼できるデバイスのみが機密リソースにアクセスできるようにします。

クラウドアプリケーションへの安全なアクセス:
クラウドリソースへのアクセスを許可する際にゼロトラスト原則を採用し、暗号化、アクセス制御、ログなどのセキュリティ対策を採用します。

アクセス制御の定期的な見直しと更新:
アクセス制御を継続的に評価、調整し、組織の役割と責任の変化に合わせて、適切かつ安全なアクセス制御を維持します。

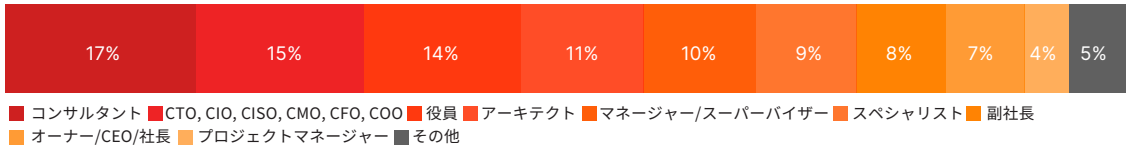
異常検知と対応の導入:
EDRやXDRなどの高度な検知、対応テクノロジーを導入し、脅威を迅速に特定します。

セキュリティ意識向上トレーニングの実施:
ゼロトラストの原則、安全なオンライン慣行、潜在的なセキュリティ脅威の認識と報告方法について従業員を教育し、ヒューマンエラーに起因するセキュリティインシデントの可能性を低減します。

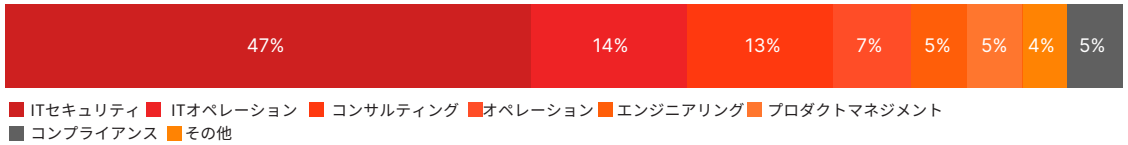
調査方法と統計

このレポートは、ゼロトラストセキュリティに関連する最新の企業の採用傾向、課題、ギャップ、およびソリューションの優先傾向を明らかにすることを目的とし、2023 年 3 月にアメリカの IT およびサイバーセキュリティに携わる 431 人を対象に行われた包括的なオンライン調査の結果を基にしています。 回答者は技術系エグゼクティブからITセキュリティの現場の専門家まで多岐にわたり、複数の業界からのさまざまな規模の組織をバランスよく含んでいます。

役職

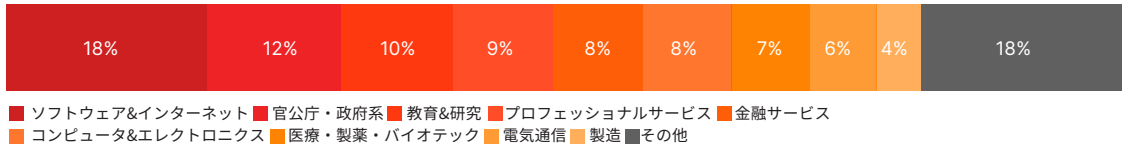


部署



企業規模（人）

業種



ivanti.com/ja
03-6432-4180
contact@ivanti.co.jp

Ivantiは「Everywhere Workplace（場所にとらわれない働き方）」の実現を支援します。 「Everywhere Workplace」では、働く場所にかかわらず、従業員は多種多様なデバイスでさまざまなネットワークからITアプリケーションやデータにアクセスし、高い生産性を保つことができます。

Ivanti Neuronsの自動化プラットフォームは、業界をリードする統合エンドポイント管理、ゼロトラストセキュリティ、エンタープライズサービス管理ソリューションを一体化することでデバイスの自己修復と自己保護を可能にしながら、ユーザーのセルフサービス機能を強化した統合ITプラットフォームです。

アメリカのビジネス誌「フォーチュン」が選ぶ100社のうち78社を含む、4万以上の顧客がIvantiを導入し、クラウドからエッジまでのIT資産の検出、管理、保護、サービス提供を行い、いつでもどこでも従業員に優れたエンドユーザー体験を提供しています。

詳細については、ivanti.com にアクセスし、 @GoIvanti をフォローしてください。

1 手作業によるプロセスは複雑で、迅速な対応が遅れる 37%｜パートナーによるアプリやリソースへの安全でないアクセス 33%｜リソースにアクセスする脆弱なJailbreak（脱獄）、または紛失したモバイルデバイス 17%

2 マイクロセグメンテーション 34%｜仮想プライベートネットワーク（VPN） 33%｜エンタープライズモバイル管理（EMM）29% フィッシング対策 28%｜クラウドアクセスセキュリティブローカー（CASB） 28%｜ ゼロトラストネットワークアクセスの完全制御 27% Webアプリケーションファイヤーウォール（WAF）26%｜ネットワークアクセス制御（NAC）25%｜アイデンティティ解析 24%｜ソフトウェア定義による 境界（SDP） 24%｜脅威からネットワーク機器を不可視にする 20%｜データ損失防止（DLP） 17%｜モバイル脅威防御 16%｜エンタープライズ・ディレクトリ・サービス 13%｜デジタル著作権管理（DRM） 9%｜その他 5

Cybersecurity
INSIDERS

Cybersecurity Insidersは、50万人以上の会員を擁する情報セキュリティ専門家のためのオンラインコミュニティであり、あらゆる業界、企業規模、セキュリティの役割において、サイバーセキュリティの向上と組織の保護に尽力する最高の知識を結集しています。

私たちは、サイバーセキュリティのマーケティング担当者にユニークなマーケティングの機会を提供し、この適格な視聴者にアプローチし、事実に基づいた第三者検証のソートリーダーシップコンテンツ、需要創出プログラム、サイバーセキュリティ市場におけるブランドの可視性を提供します。

詳しくは www.cybersecurity-insiders.comをご覧ください。