Human-Centric セキュリティ

Human-Centric セキュリティを先進的なデジタル ワークスペースに実装する

デジタル変革の時代において、プルーフポイントの包括的でマルチレイヤーの保護プラットフォームがHuman-Centricセキュリティを実現する仕組み

proofpoint®

エグゼクティブ サマリー

デジタル ワークスペースの先進化に伴い、働き方は根本から変化しています。組織はクラウドに対応し、従業員は、複雑な混合環境のもとで共同作業を行っています。メール、コラボレーション ツールやメッセージング ツール、ソーシャルメディア プラットフォーム、SaaS アプリ、LLM（大規模言語モデル）、ファイル共有サービスなどが使用されています。

このような転換によって、イノベーションが急速に進み、柔軟性が大幅に向上しています。しかし、同時に、攻撃者につけ込まれるリスクの高い、新たな領域も多く生まれています。知識労働者がデータの生成、保存、アクセスを行う環境はもはや、ネットワークとエンドポイントの保護にフォーカスしていた従来のセキュリティ戦略では対応しきれないものになっています。こうした変化に対応するには、組織や個人の働き方に合わせた、先進的なアーキテクチャが必要です。サイバー脅威の主な標的はインフラではなく、ユーザーであるという現実に対処するアーキテクチャです。

このホワイトペーパーでは、プルーフポイントがどのように業界ファーストを実現しているかについて説明します。先進的な防御戦略の中心に「人」を据えることで、こうした新たな現実に対処する、Human-Centric 包括的なセキュリティ プラットフォームをご紹介します。

ホワイトペーパーの内容

- 今日のデジタル ワークスペースにおいて人を保護することがこれまで以上に重要である理由
- プルーフポイントのプラットフォームが解決できる Human-Centric 問題の説明
- 脅威をプロアクティブに検知し、ユーザーをリアルタイムでガイドして保護し、調査と対応を効率化するアーキテクチャを稼働させる主要テクノロジーについて掘り下げる

人は新たな境界：Human-Centric セキュリティが重要である理由

今日のサイバーセキュリティ課題の中心には「人」がいます。フィッシング、アカウント乗っ取り、内部リスク、データ持ち出しなど、Human-Centric 脅威は、侵害の大部分を占めるようになっています。最新の攻撃のほとんどは、テクノロジーの脆弱性ではなく、人を悪用しています。ますます複雑になるデジタル ワークスペースにおいて、攻撃者は、人をだまし、人の注意をそらし、人を言いくるめます。

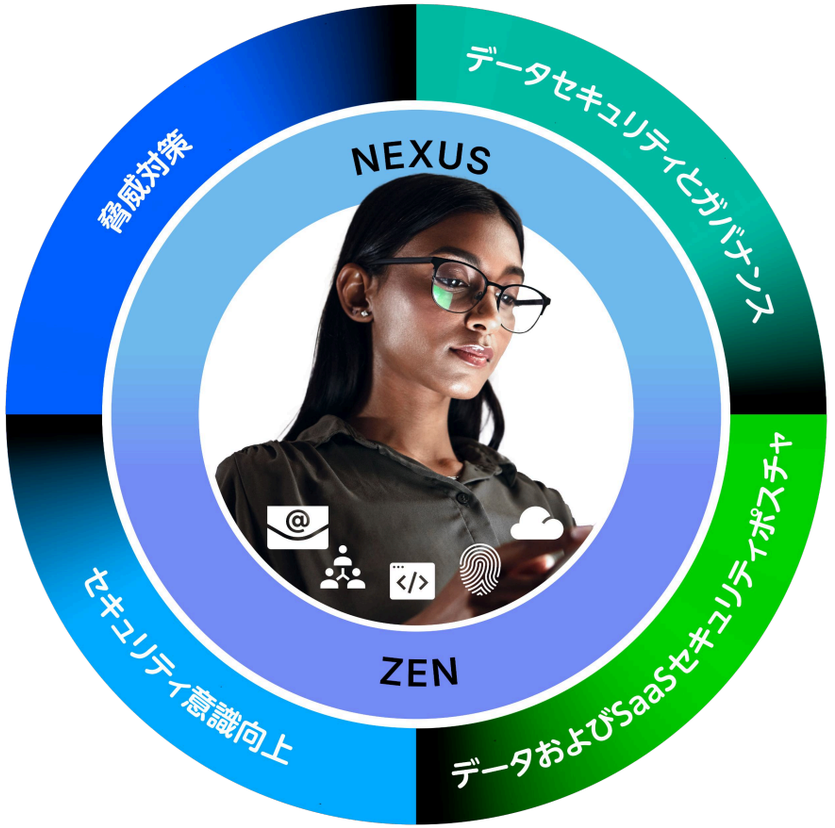
従来のセキュリティモデルは、ネットワークやエンドポイントの保護にフォーカスしています。しかし、最新の脅威は人の脆弱性を狙っています。プルーフポイントのサイバーセキュリティ プラットフォームを利用すれば、組織は、Human-Centricなアプローチを採用することで、人とデータを守ることができます。プルーフポイントのプラットフォームは、脅威の阻止、情報の保護、ユーザーの誘導、データとSaaSセキュリティ ポスチャの強化という4つの重要な課題に対処するための最善のソリューションを提供します。

THREAT PROTECTION - 脅威対策

人を標的にする脅威を阻止

SECURITY AWARENESS - セキュリティ意識向上

従業員に継続的なガイダンスを提供



DATA SECURITY & GOVERNANCE - データセキュリティとガバナンス

情報漏えいとコミュニケーションの管理

DATA & SAAS SECURITY POSTURE - データとSaaSセキュリティポスチャ

データやSaaSのリスクを修復

図1：プルーフポイントの Human-Centric セキュリティ プラットフォームは4つの重要エリアにおいて最善のソリューションを提供します。

proofpoint.

マルチレイヤーの包括的な保護プラットフォーム

プルーフポイントの包括的なプラットフォームは、以下を実現するマルチレイヤーのアーキテクチャを基盤にしています。

- 高度なAI、機械学習、リアルタイムの脅威インテリジェンスといった機能を用いて、デジタル ワークスペースにおいて**プロアクティブに脅威を検知**
- 業務がどこで行われていようと、従業員とデータを保護する、**エンドユーザーのコントロール ポイントの広範なセットを提供**
- 「人」を標的にした攻撃に対するレジリエンスを高められるよう**ユーザーにアラートを提供し、ガイドし、サポート**
- **調査と対応を効率化**

これらの機能は、3つの主要テクノロジーによって稼働しています。Nexus、Zen、Threat Protection Workbenchです。次のセクションでは、これらの機能について見ていきましょう。

Nexus

AIと脅威インテリジェンスを活用した検知機能

Proofpoint Nexus®は、プルーフポイントのアーキテクチャの検知レイヤーです。AI、機械学習、リアルタイムの脅威インテリジェンスを活用した、統合型検知フレームワークです。

Nexusはさまざまなモデルタイプを統合しています。どのモデルも、従業員が働くすべての方法において、特定のリスクシグナルを分析するよう設計されています。メール、クラウドアプリ、コラボレーション ツール、ブラウザが対象です。

Nexus検知フレームワークの主要コンポーネント

Nexus TI (Threat Intelligence) は、既知および未知の攻撃者、キャンペーン、インフラからシグナルを継続的に取り込み、プルーフポイント製品に、コンテキスト豊富な検知と、進化する脅威技術に適応できる能力を提供します。

Nexus LM (Language Model) は、高度なAI言語モデルのパワーを活用し、ビジネスメール詐欺（BEC, Business Email Compromise）といった、ソーシャル エンジニアリング攻撃で使用されるメッセージのトーン、緊急性、言語的構造を評価します。

Nexus RG (Relationship Graph) は、ユーザー アクティビティ、行動履歴、役割の機密度の関連付けを行い、リスクのある行動の可能性や高リスクの個人に対する標的型攻撃の可能性を評価します。

Nexus ML (Machine Learning) は、コミュニケーション ツールやコラボレーション ツールにおいて通常とは異なる行動を検知し、侵害されたアカウントまたは内部関係者の不正使用による、微細ながらも影響力のあるシグナルを特定します。

Nexus CV (Computer Vision) は、レイアウト、ロゴの位置、デザインの模倣を分析することで、ブランドのなりすましや、視覚的詐欺戦術を認識します。高度なコンピューター ビジョン技術により、Nexus CVは、フィッシングサイト、QRコード、悪意のある添付ファイル、なりすましメールなどの視覚的要素に隠された脅威を検知します。

Nexusは、高度なフィッシング攻撃、認証情報の盗難、なりすまし試行、ランサムウェアキャンペーンを検知します。実例を1つあげるとすると、Nexusは、財務部門を標的にした請求書詐欺を招く、サプライヤー侵害を特定しました。Nexusは、通常とは異なる表現や視覚的な不一致を特定し、グローバルなデータセットから収集された既存の脅威インテリジェンスを活用することで、この攻撃を未然に防ぎました。

Nexusはまた、データの保護においても優れています。もう一つの実例では、ある従業員が顧客データを承認されていない生成AIツールに貼り付けた際、Nexusは機密データパターンを検知し、リスクスコアを評価して、この操作をブロックしました。

Nexusは、**1日26億件以上のメールを分析し、1日4億5,000万件以上のURLを調査し**、数百の攻撃者によるシグナルの関連付けを行っています。この巨大な規模により、脅威状況全体において精度と対応を強化することができます。

proofpoint.

Zen

コントロール ポイントとコンテキストに基づくユーザーガイダンス

Proofpoint Zen™は、プルーフポイントのアーキテクチャのエンフォースメント＆ユーザー ガイダンス レイヤーです。ユーザーが働く場所でセキュリティ ポリシーを適用します。Zenスイートのコントロール ポイントは、インテリジェンスをリアルタイムの保護やポリシーに沿ったコーチングに変換します。これにより、ユーザーは、時間を割くことなく安全な決定を行うことができます。

Zenスイートの主要コンポーネント

Zen for Outlook は、セキュリティツールをメールワークフローに組み込むことで、防御の第一線としてユーザーをサポートします。Nexusのリアルタイムの脅威インテリジェンスを用いて、不審なメールを受け取ったユーザーにはインライン警告を表示します。簡単に報告することもできます。リスクのある行動に対してはスマートナッジを提供し、機密データがアウトバウンド メールに含まれている場合はアラートを提供します。

ZenWeb は、Chromiumベースのブラウザの軽量な拡張機能で、SaaS、ファイル共有ツールや生成AIツールにおけるWebアクティビティを保護し、フィッシングサイトからユーザーを保護します。Nexus脅威モデルによるライブ検知を使用して、ユーザーの生産性を損なうことなく、リアルタイムの脅威検知と防止を提供します。

Zen Endpoint DLP/Insider Threat Management は、ユーザーの行動をエンドポイントで監視することで、情報漏えいや内部脅威に対し、デバイスレベルの保護を提供します。USBの使用状況、クリップボードのアクティビティ、ファイル同期の操作、アプリの挙動を監視します。不審なユーザー行動のスクリーンショットやユーザー アクティビティのタイムラインを作成します。

Zen Cloud API Connectors は、Microsoft 365、Google Drive、Slack、Boxなど、クラウドベースのSaaSプラットフォームにセキュリティを拡大します。ファイルのアップロードを監視し、過度な共有など、通常とは異なる行動を検知します。OktaやSOAR（セキュリティ オーケストレーション、自動化、対応）ツールのカスタムワークフローにも対応しています。

Zen Communications Connectors は、Microsoft Teams、Zoom、Slackなど、規制対象のプラットフォームでコミュニケーションをキャプチャし、アーカイブや監視に対応します。さまざまなチャネルからのメッセージを統合型アーカイブ フォーマットに取り込み、監視ツールと統合し、HRや法務部のワークフローをサポートします。

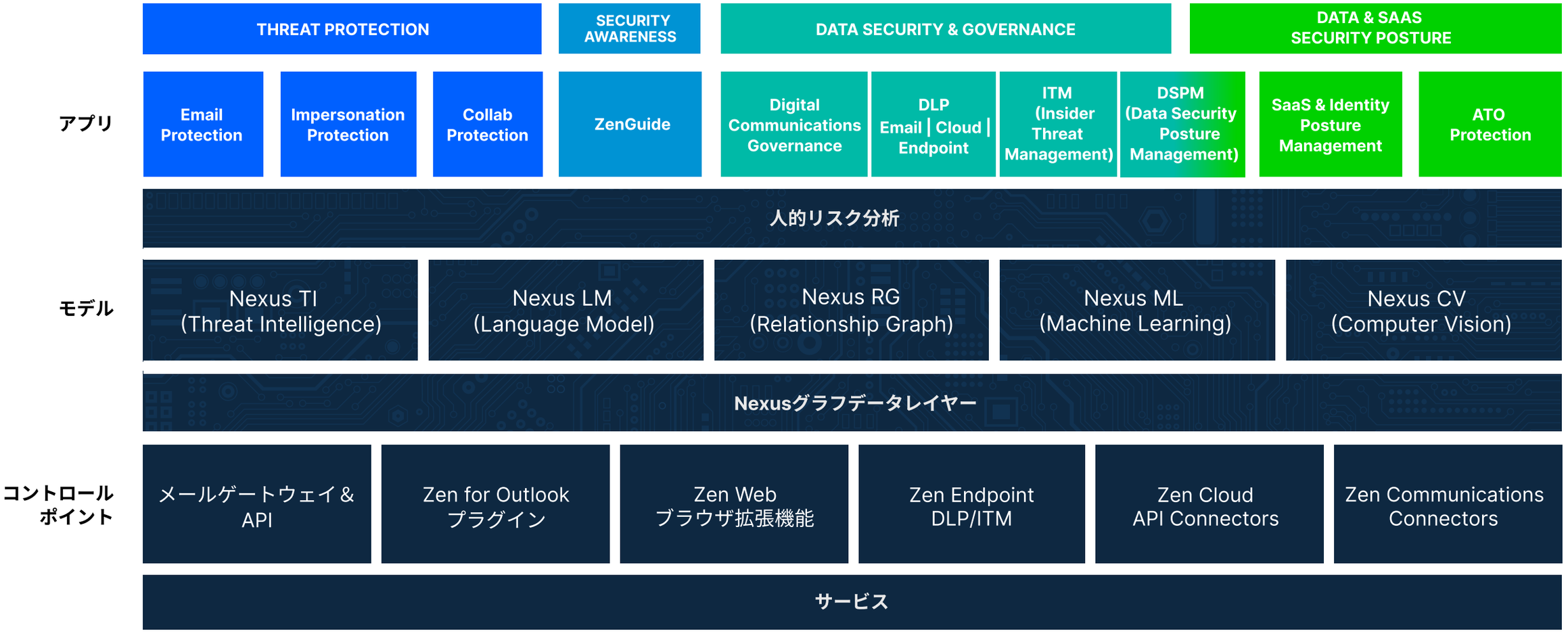


図2：プルーフポイントの Human-Centric セキュリティ プラットフォームは、マルチレイヤーのアーキテクチャを基盤としています。（脅威対策、セキュリティ意識向上、データセキュリティ＆ガバナンス、データ＆SaaSセキュリティ ポスチャの主要ソリューション エリアの）プルーフポイント製品は、NexusとZenの主要テクノロジーの機能を直接使用しています。

Threat Protection Workbench

迅速な調査と自動修復

脅威が検知されたり、ポリシー違反にフラグが付けられた場合、スピードと明確さが重要となります。セキュリティ オペレーション センター（SOC）チームにとって、複数のコンソール、過度なクリック、その他のチームへの依存関係により、対応時間は遅くなり、攻撃のリスクも高まります。

Proofpoint Threat Protection Workbenchは、プルーフポイントのアーキテクチャの調査と自動化のレイヤーです。直感的かつ一元的なコンソールを提供することで、脅威の調査と修復を効率化します。セキュリティチームは、ツールの切り替えやフラグメント化されたデータによって生じる遅延に悩まされることなく、脅威のトリアージ、分析、対応を行うことができます。

セキュリティチームは、Threat Protection Workbenchを用いて不正なメールボックスのサブミッションの処理、高リスクユーザーのシグナルのエスカレーション、脅威キャンペーンの調査を行うことができます。Threat Protection Workbenchは、Nexusの脅威インテリジェンスをユーザー行動やポリシートリガーと関連付けることで、不要なノイズなく、高精度のアラートを提供します。

Threat Protection Workbench ユースケースの例

- アカウント乗っ取り調査の自動対応
- 標的となったユーザーのクリックパスの可視化
- 複雑なマルチチャネルの脅威の概要

これらすべての機能により、アナリストのワークロードを減らし、脅威の滞在時間を抑えることができます。脅威に対応するために、アナリストは、プレイブックを直接実行したり、APIを使用して、広範なセキュリティスタック内のその他のコンポーネントに任せたりできます。

まとめ

Human-Centric セキュリティを実現するために設計されたアーキテクチャ

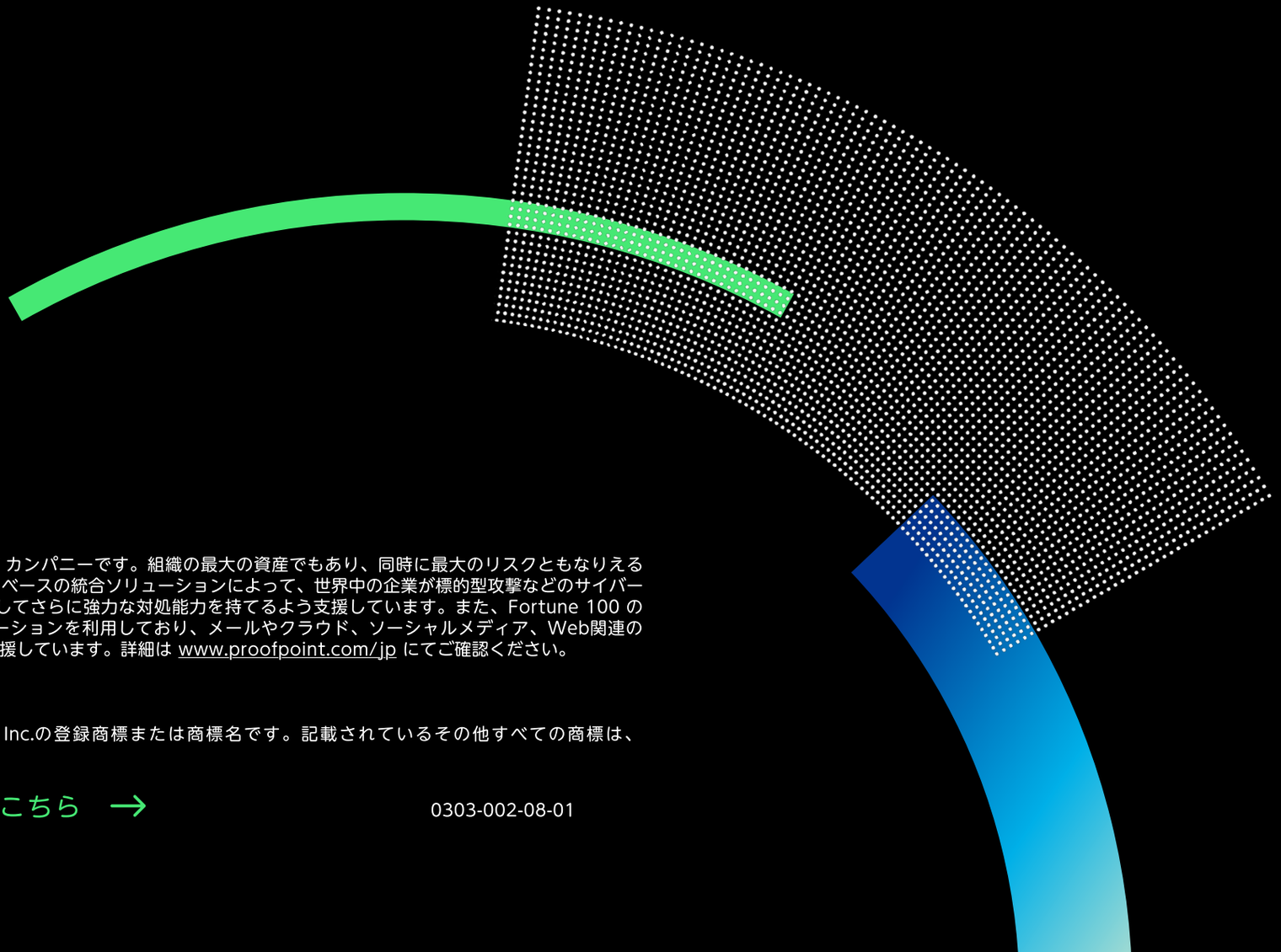
サイバーリスクの性質は変化しています。脅威の標的はシステムだけではなく、「人」そのものです。また、デジタル ワークスペースは複雑になっており、これを保護するための対策が間に合っていません。ユーザーは、メール、ブラウザ、コラボレーション ツール、クラウド アプリケーションを流動的に使用しているため、静的な境界を対象に構築された画一的なコントロールのような古いセキュリティモデルでは対応しきれません。

プルーフポイントのプラットフォームなら、従業員の働き方に合わせたセキュリティアーキテクチャを構築しているため、この課題を解決できます。Nexusにより、比類のない脅威インテリジェンスと振る舞い分析に基づいて、Human-Centric 脅威に対し、AIを活用した可視性を手に入れることができます。Zenにより、プルーフポイントのプラットフォームはユーザーをスムーズに保護し、その場で適切なガイダンスを提供します。また、Threat Protection Workbenchを活用することで、セキュリティチームは迅速な対応が可能となり、明確なインサイトのもとで運用負荷を低減できます。

これは理論上の話ではなく、実践で証明されているものです。プルーフポイントのプラットフォームは、リスクを低減し、長きにわたりレジリエンスを築く、実証済みのプロダクション規模のアーキテクチャです。組織は、現在のワークフローを保護しながらも、Human-Centric な新たな進化にも備えることができます。

世界クラスの検知、内蔵の振る舞い制御と迅速な統合対応を組み合わせることで、プルーフポイントは、組織にとって最も重要な場所である、人、データ、脅威が交わる所で、リスクを低減できるようサポートします。

proofpoint.



proofpoint.

Proofpoint, Inc.は、サイバーセキュリティのグローバル リーディング カンパニーです。組織の最大の資産でもあり、同時に最大のリスクともなりえる「人」を守ることに焦点をあてています。プルーフポイントは、クラウドベースの統合ソリューションによって、世界中の企業が標的型攻撃などのサイバー攻撃からデータを守り、そしてそれぞれのユーザーがサイバー攻撃に対してさらに強力な対処能力を持てるよう支援しています。また、Fortune 100 の 85% の企業などさまざまな規模の企業が、プルーフポイントのソリューションを利用しており、メールやクラウド、ソーシャルメディア、Web関連のセキュリティのリスクおよびコンプライアンスのリスクを低減するよう支援しています。詳細は www.proofpoint.com/jp にてご確認ください。

プルーフポイントとつながる: LinkedIn

プルーフポイント プラットフォームの詳細はこちら →

0303-002-08-01