

プルーフポイント ソリューション バンドル

喫緊のサイバーセキュリティ問題の解決

昨今の高度な攻撃を防ぐには、人に焦点を当ててセキュリティ コントロールを構築する必要があります。プルーフポイントでは独自の PEOPLE-CENTRIC アプローチをとっています。これはまず、誰が最も攻撃されやすい Very Attacked People (VAP) なのかを知り、彼らが組織にもたらすリスクを評価することから始めます。プルーフポイントのソリューションバンドルは、最新の脅威に対応し、人それぞれの防御力をも高め、お客様のセキュリティ戦略に合わせて進化します。

P1 ソリューションバンドル: 高度なメール セキュリティ

現在、90%以上の攻撃はメールから始まります。P1 バンドルでは、攻撃の検出から対応までの一連の攻撃フェーズにわたってメールからの脅威に対抗します。誰が攻撃されているか、どのように攻撃されているか、フィッシング リンクをクリックしたか、または不審に思っ報告したのか、そして実際に侵害されたのかを可視化できます。メール攻撃（マルウェアとマルウェアを用いない攻撃を含む）を阻止し、ユーザーを教育して脅威への耐性をつけ、修復を自動化します。また、フィッシング シミュレーション、包括的なトレーニング、Abuse メールボックスの自動管理を含むセキュリティ意識向上トレーニングを用いて脅威対策を強化します。

1 Abuse メールボックス・・・ユーザーから迷惑メールなどを報告(転送)してもらうための組織で管理するメール受信箱

P1 に含まれるソリューション

- Email Protection
メール セキュリティ ゲートウェイ
- Targeted Attack Protection (TAP)
未知の標的型攻撃に対抗するクラウド型サンドボックス
- Threat Response Auto-Pull (TRAP)
配送済の悪意あるメールを自動で隔離
- Security Awareness Training
企業向けオンライン セキュリティ意識向上トレーニング
- Basic Email Encryption (TLS)
TLSによるメール通信経路の暗号化
- Basic Email DLP (RegEx)
Eメールによる情報漏えいを未然に防止 (基本機能)

P1+ ソリューション バンドル: BEC の阻止

昨今、ビジネスメール詐欺 (BEC) のようなマルウェアを用いないメール詐欺攻撃も増加しています。こういった攻撃には、ユーザーを狙うインバウンド攻撃や、組織の従業員になりすまし、貴社の顧客やビジネス パートナーを狙うアウトバウンド攻撃などがあります。これらの BEC 攻撃ではさまざまな認証情報を窃取する手法が用いられます。DMARC 認証とメール ゲートウェイを組み合わせた多層セキュリティアプローチでマルウェアを用いないメール詐欺攻撃も阻止する必要があります。P1+ソリューションバンドルは BEC ソリューションを含むメールベースのすべての攻撃手法に対応し、メール エコシステム全体を可視化し、攻撃メールが受信箱に到達する前にブロックします。

P1+ に含まれるソリューション

- P1に含まれるソリューション に右記をプラス
- Email Fraud Defense (EFD)
DMARCを用いたなりすましメール対策、類似ドメインの可視化

P2 ソリューション バンドル: BEC と EAC の阻止

P2 では、メールアカウント侵害 (EAC) の兆候を検出し、それにも対応します。これには侵害されたアカウントから送信される悪意ある内部メールへの対応も含まれます。どのアカウントが侵害され、誰が攻撃され、どのような脅威が送信されているのかをリアルタイムに可視化し、悪意のあるメールの除去、パスワード リセット、アカウントの停止などといった脅威への対応を自動化します。さらに、個人の Web メールへの攻撃や、会社メールに送信された危険な Web サイトを阻止します。

P2 には、P1+のソリューションに加えて以下が含まれます:

P1+ に含まれるソリューションに以下をプラス

- Internal Mail Defense (IMD)
内部メールに対する防御
- Cloud Account Defense (CAD)
SaaSアカウント侵害対策
- Proofpoint Email Isolation
従業員によるWebメールのアクセスを分離
- Email Encryption
SaaS型ポリシーベースのメール自動暗号化
- Email DLP
Eメールによる情報漏えいを未然に防止

P2+ ソリューションバンドル: クラウド アプリの保護

Microsoft 365 (Office 365)、Google G Suite、その他のクラウドアプリケーションを使用するユーザーとそのデータを保護しましょう。人を中心としたセキュリティ戦略に CASB ソリューションを追加することで、クラウド環境を集中管理できるようになります。これはまた、クラウド上の脅威やアカウント侵害を防ぎ、危険なサードパーティ クラウド アプリを可視化し、ユーザーが作成しアクセスする情報を保護します。

P2+ には、P2のソリューションに加えて以下が含まれます:

P2 に含まれるソリューションに以下をプラス

- Cloud App Security Broker (CASB)
クラウドアプリケーションの保護、シャドー ITの可視化、サードパーティ製アプリのリスク分析

P3 ソリューション バンドル: 人を中心とした完全なセキュリティ

攻撃対象となる人とエコシステム全体をカバーする戦略的セキュリティ体制を構築します。これには、ドメイン、ソーシャルメディアアカウント、エグゼクティブ、ロケーション、環境内のその他のテクノロジー インフラストラクチャ、Web へのアクセスの保護が含まれます。分離可能でアダプティブな統合制御でVAPを保護します。また、専任の脅威アナリストが、組織向けにカスタマイズした脅威調査を提供します。

P3 には、P2+のソリューションに加えて以下が含まれます:

P2+ に含まれるソリューションに以下をプラス

- Browser Isolation
Web 分離
- Threat Response
インシデント レスポンスの自動化、オーケストレーションによる脅威の封じ込め
- Digital Risk Protection
デジタル リスク プロテクション
- Premium Threat Information Service (PTIS)
脅威情報提供サービス

ソリューションバンドル

		高度なメールセキュリティ	+BEC 対策	+EAC 対策	+CASB	PEOPLE CENTRIC
		P1	P1+	P2	P2+	P3
脅威対策	フィッシング攻撃、なりすましメールおよびマルウェアから受信メールを保護 Email Protection、Targeted Attack Protection (TAP)	✓	✓	✓	✓	✓
	Very Attacked People (VAP) と、VAP を狙う脅威を可視化 Targeted Attack Protection (TAP)、CASB	✓	✓	✓	✓	✓
	配信後に脅威が判明した場合、またはエンドユーザーから報告があった場合に悪意のあるメールをユーザーの受信箱から自動的に削除 Threat Response Auto-Pull (TRAP)、CLEAR	✓	✓	✓	✓	✓
	メール認証により、信頼できるドメインから送られてくる詐欺メールを阻止 Email Fraud Defense (EFD)		✓	✓	✓	✓
	会社支給のデバイスで個人 Web メールを使用するリスクから保護 Email Isolation			✓	✓	✓
	クラウドアカウントの侵害リスクを調査して対応 (これらのアカウントから送信される内部脅威を含む) Threat Response Auto-Pull (TRAP)、Cloud Account Defense (CAD)、Internal Mail Defense (IMD)			✓	✓	✓
	悪意のあるコンテンツによる会社支給デバイスの被害を防ぎユーザーが安全にインターネットを使用できる環境を提供 Browser Isolation					✓
不審な Web ドメイン及びソーシャルメディア アカウントからの詐欺を検出 Digital Risk Protection					✓	
特定組織向けの脅威分析で、インテリジェンスと推奨事項を提供 Premium Threat Information Service (PTIS)					✓	
ユーザー保護	ユーザーのフィッシング攻撃への対応をテストする脅威シミュレーション (35 以上の言語及び 13 のカテゴリーにわたる数千のテンプレート) ThreatSim	✓	✓	✓	✓	✓
	インタラクティブなセキュリティ意識向上トレーニング Security Awareness Training	✓	✓	✓	✓	✓
	セキュリティリスクを認識して回避できるよう従業員をトレーニング CyberStrength	✓	✓	✓	✓	✓
データ保護	メール DLP のための正規表現、TLS メール暗号化 Email Protection(RegEx)	✓	✓	✓	✓	✓
	ポリシーベースのメール自動暗号化および E メールによる情報漏えいを未然に防止 Email DLP & Email Encryption			✓	✓	✓
	クラウドアプリケーションの保護 機密情報の過度な共有、サードパーティアプリの管理、およびシャドールー IT などを対象とする DLP Cloud App Security Broker (CASB)				✓	✓

詳細

proofpoint.com/jp でご確認ください。

ブルーポイントについて

Proofpoint, Inc. (NASDAQ:PFPT) 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。Proofpoint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 1000の過半数を超える企業などさまざまな規模の企業が、ブルー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。

©Proofpoint, Inc. Proofpointは、米国およびその他の国におけるProofpoint, Inc.の商標です。記載されているその他すべての商標は、それぞれの所有者に帰属します。