
Barracuda Sentinel
製品紹介
Barracuda
Your journey, secured.

バラクーダネットワークス会社概要

2002年 Barracuda Networks Inc. 設立

- 本社：カリフォルニア州キャンベル
- 海外拠点**10カ国**、**80カ国以上**で正規代理店と提携
- **全世界16万社**のお客様にセキュリティ・バックアップソリューションを提供
- バラクーダバックアップは、バックアップ専用アプライアンスとして**シェアNo.1**
  (IDC Worldwide Quarterly Purpose Built Backup Appliance（PBBA）Tracker Q2/Q4)

2005年 バラクーダネットワークスジャパン株式会社 設立

- スパム対策アプライアンス 2005年～2011年の7年連続で**国内出荷台数No.1**
- WAF 2007年～2013年の7年連続で**国内出荷台数No.1**（富士キメラ総研調査）
- バックアップ2016年**国内出荷台数No.1**（テクノシステムリサーチ調査）
- 全数着荷検査を国内で実施

バラクーダ製品一覧

SEN クラウド型フィッシングメール対策
Sentinel

WAF クラウド型Web脆弱性対策
WAF-as-a-Service

Barracuda Essentials for Office 365
クラウド向けメールセキュリティ
Essentials for Email Security

Barracuda Essentials for Email Security
Office365向けメールセキュリティ
Essentials for Office 365

FW 次世代FW・SD-WAN
CloudGen Firewall F
Appliance VM AWS Azure Google

WSG URLフィルタ・マルウェア対策
Web Security Gateway
Appliance VM

ESG 標的型メール対策
Email Security Gateway
Appliance VM AWS Azure

メールサーバ

WAF Web脆弱性対策
Web Application Firewall
Appliance VM AWS Azure Google

Webサーバ

ADC 負荷分散
Load Balancer ADC
Appliance VM AWS Azure

MA メールアーカイブ
Message Archiver
Appliance VM AWS

BU バックアップ
Backup
Appliance VM

ファイルサーバ

DBサーバ

Appliance 物理アプライアンス
VM 仮想アプライアンス
AWS Amazon Web Service
Azure Microsoft Azure
Google Google Cloud

Barracuda **Sentinel**

詐欺メール対策とメールボックス防御

SEN

Barracuda
Sentinel

リアルタイムスピアフィッシング対策のためのAI

- 250万のメールボックスを学習済み
- 誤検知率1/1,000,000
- ゲートウェイセキュリティ製品では見抜けない攻撃を検知

侵害されたアカウントの検出と修正

- インシデント対応ワークフローをサポート
- 内部の脅威の保護も可能

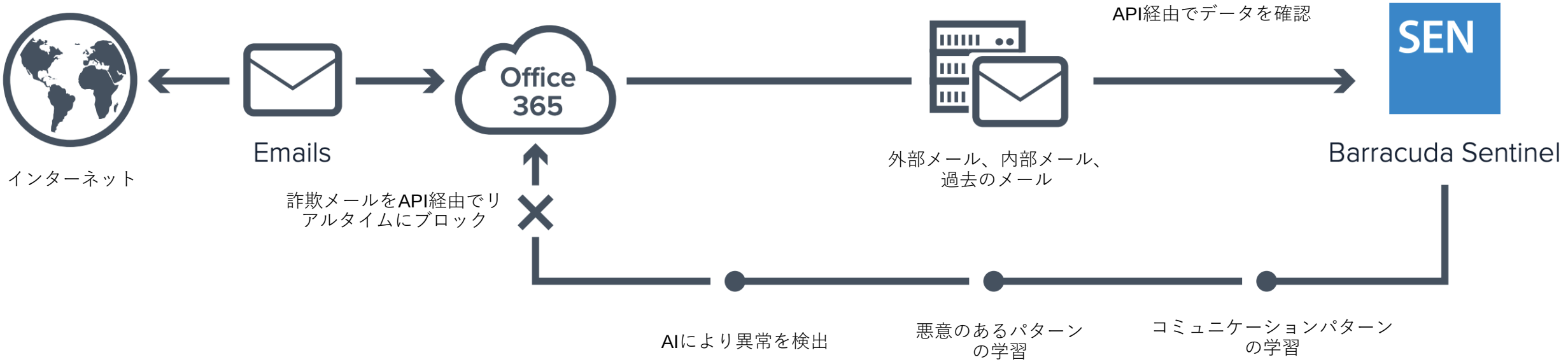
DMARCを用いたブランド詐欺防止機能

- ブランド使用状況の可視化

機能紹介：リアルタイムフィッシング防御

Barracuda Sentinel独自のAPIベースのAIエンジンが過去のメールのやり取りを研究し、ユーザーの独自のコミュニケーションパターンを学びます。 その後、メッセージのメタデータとコンテンツの異常を識別し、リアルタイムで攻撃を見つけ、ブロックすることができます。

過去メールのパターン学習に基づくこのアプローチは、高度なフィッシング攻撃、およびアカウント乗っ取り攻撃を検出する従来のポリシーベースの戦略よりはるかに正確です。



機能紹介：アカウント乗っ取りと内部リスクへの対処

アカウント乗っ取りにより、攻撃者はこっそりと自分のターゲットを調査し、攻撃を計画することができます。

ゲートウェイ型セキュリティ製品では、これらの乗っ取られたアカウントから実行される内部攻撃を見ることはできず、検出することもできません。

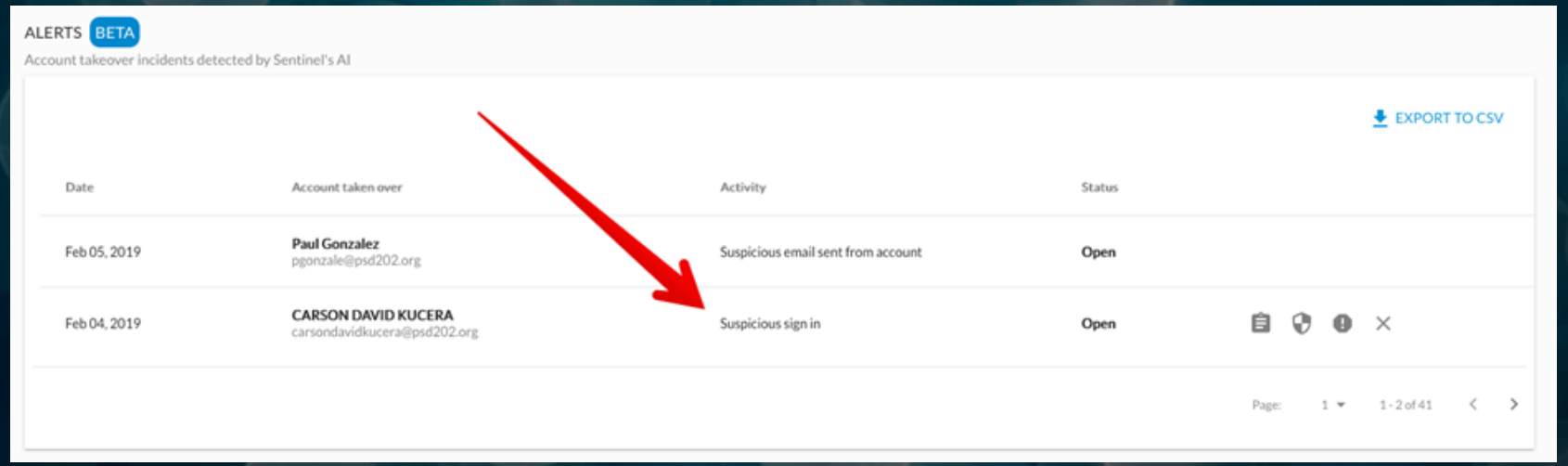
Barracuda Sentinelは異常な内部メールの振る舞いを検出して管理者に警告を送信し、その後、侵害されたアカウントから送信されたすべての詐欺メールを見つけて削除することが出来ます。

機能紹介：アカウント乗っ取りと内部リスクへの対処

1.疑わしいサインインの検出

Barracuda Sentinelのユーザ全体で、疑わしい動きを見せているIPを追跡することが可能です。Sentinelは異なる顧客に属する複数のアカウントで失敗したサインインを追跡し、アカウント間でこの情報を共有し、サインインが成功したときにIT管理者に警告します。

•Sentinelが異常なデバイスまたは地域からの異常なサインインアクティビティを監視したときに、各ユーザのアクセスパターンを追跡し、IT管理者に警告する。 Sentinelは、ユーザレベルのパターンと組織全体のレベルのパターンの両方を追跡します。

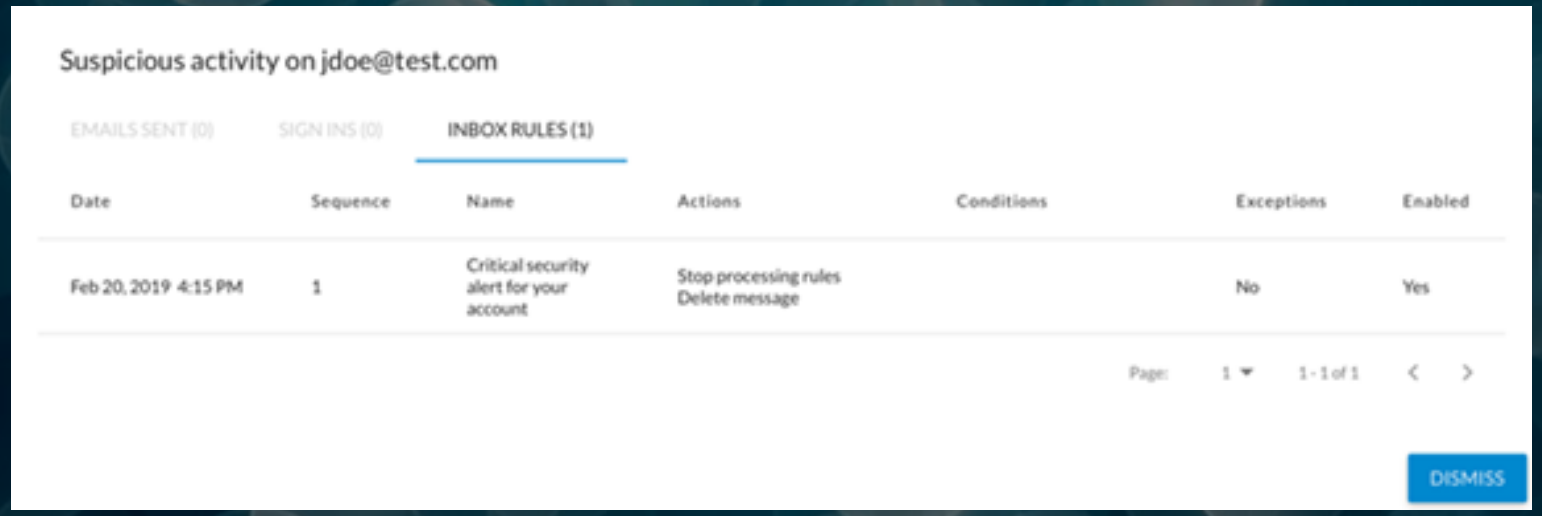


機能紹介：アカウント乗っ取りと内部リスクへの対処

2. 受信トレイルールに基づくアカウント乗っ取り検出

Barracuda Sentinelは受信トレイルールの情報に基づきアカウント乗っ取りの可能性を検知し、管理者に警告します。

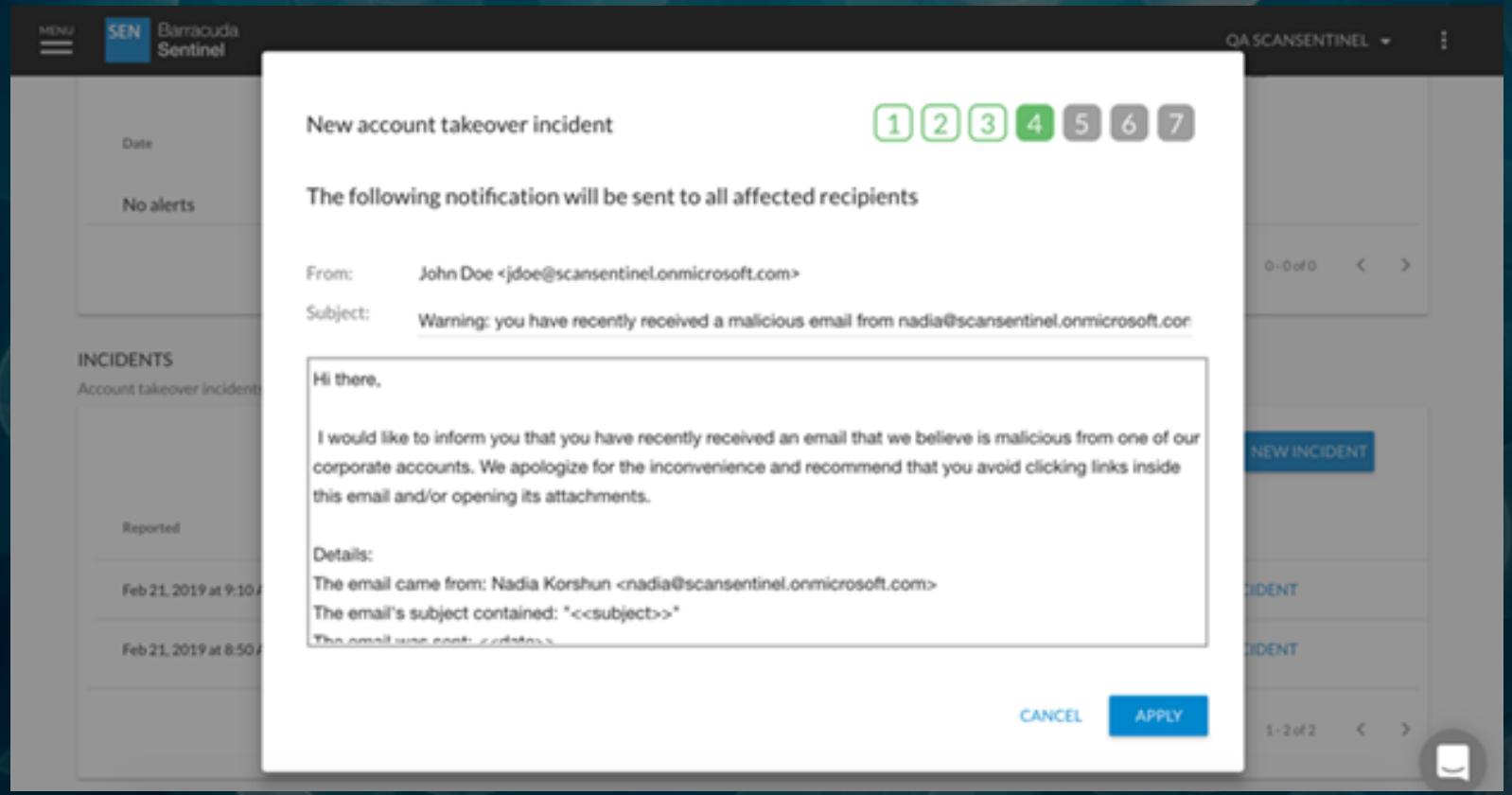
※アカウント乗っ取りが成功した後、攻撃者は偵察を行います。
この偵察の一環として、彼らは電子メールを転送したり悪意のある通信を隠したりするための受信トレイルールを設定します。Barracuda Sentinelは、被害者のアカウントに追加された受信トレイのルールを自動的に追跡し、アカウントの乗っ取りに関連するルールについて警告します（たとえば、すべてのメッセージを自動的に削除/移動するルール、配信不能および不在通知を隠すように設計されたルール）。



機能紹介：アカウント乗っ取りと内部リスクへの対処

3.アカウント乗っ取りの修復作業中に外部通知を編集およびカスタマイズする機能

Barracuda Sentinelはアカウント乗っ取り攻撃による、外部受信者への通知を編集およびカスタマイズすることができるようになりました。管理者は、カスタムメッセージ、件名、連絡先情報、その他の詳細を含めることができます。

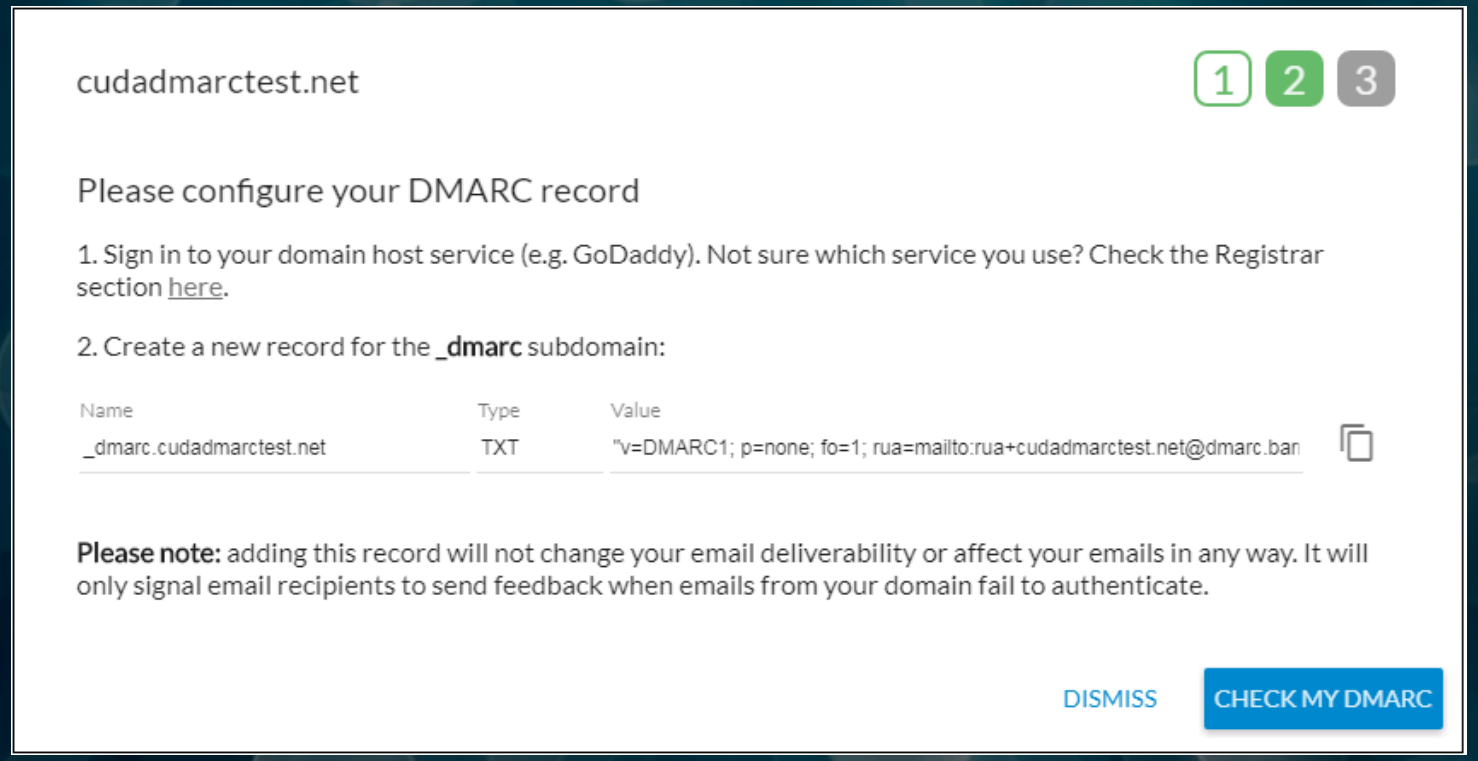


機能紹介：ブランド保護とドメイン詐欺の可視性

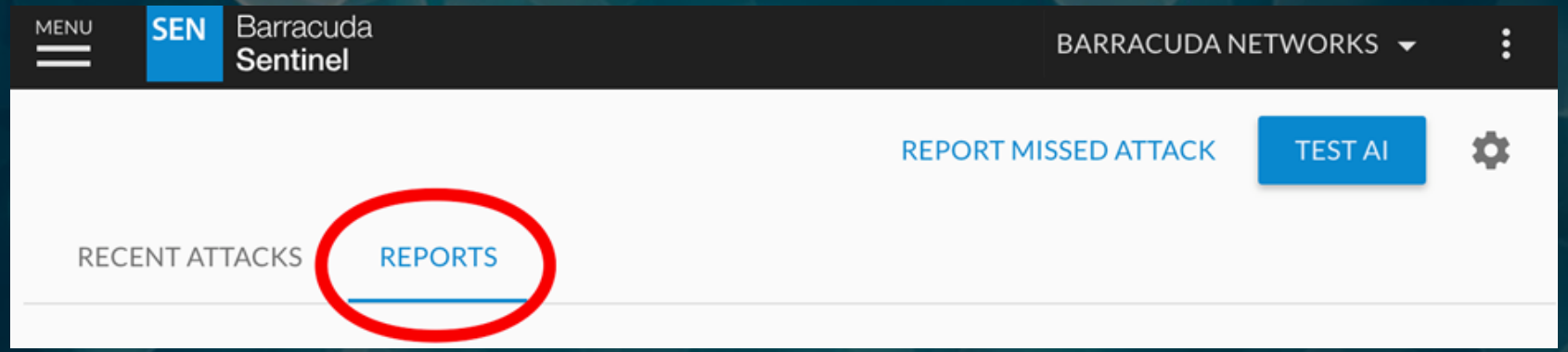
ドメイン詐称は、従業員、顧客、およびパートナーを標的とした一般的な攻撃です。

Barracuda Sentinelは、DMARC（Domain-based Message Authentication Reporting and Conformance）分析によって、電子メールドメインの不正使用を防止します。

Barracuda SentinelはDMARC認証の設定をサポートします。



機能紹介：レポート機能



Barracuda Sentinelには、脅威環境とリスクの発生源に関する詳細なレポートと分析が含まれています
ダッシュボードよりこれらのレポートへアクセスできます。

- Sentinelによって検出された攻撃
- 詐欺メールの上位受信者
- 偽装メール上位送信者
- サービス偽装
- 詐欺メールでよく使われる件名


Thank You
Barracuda
Your journey, secured.