AvePoint

AvePointで実現する
Microsoft 365 セキュリティ

クラウド利用時のセキュリティリスクを専門知識なしで解決！

ランサムウェア

情報漏洩

内部不正

「クラウドだから安心」と思っていませんか？
Microsoft 365 セキュリティの落とし穴

攻撃手法の進化

- M365に特化したフィッシング
- 管理者アカウントの窃取
- 多要素認証を突破するマルウェア

Microsoft 365に特化した
攻撃集団・手法の登場

クラウドの設定ミス

- チームの公開範囲が全員になっている
- 社外ユーザーに与える権限が強すぎる

設定ミスによって機密情報が公開！
内部での情報漏洩も

インシデント発生を前提とした
クラウドセキュリティが重要！

インシデントの
“検知”

—

データの
“復旧”

—

影響範囲の
“監査”

➡ AvePointで解決！

リスクの“検知”

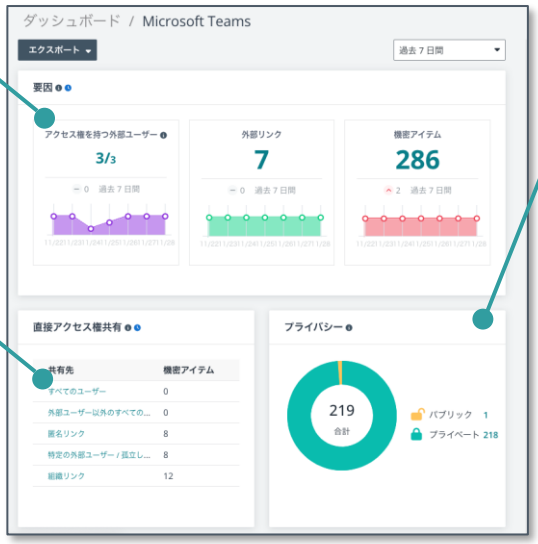
クラウドの設定ミスや潜在的な情報漏洩リスクを検知

主要なリスク要因

- チームにいる外部ユーザー
- 外部に共有されているファイル
- 機密ファイル

共有リンクの分析

- 作成されている共有リンクを共有先ごとに集計



チームのプライバシー設定

- チームの「パブリック」「プライベート」の設定状況を可視化

AvePoint Policies & Insights For Microsoft 365

データと設定の“復旧”

被害を受けたデータを迅速に復旧

AvePoint Cloud Backup

バックアップ対象

SharePoint	Teams	OneDrive	Exchange
サイト	チャネル会話	ドキュメント	メールアイテム
ライブラリ / リスト	個人チャット	権限	連絡先
ドキュメント	ドキュメント		カレンダー
権限	メンバーシップ/権限		パブリックフォルダー

影響範囲の“監査”

AvePoint Cloud Governance

インシデントの影響範囲を正確に監査

M365標準機能

過去180日 しか保持されない

→

AvePoint

期間無制限 でログを保存

AvePoint

AvePoint 製品・サービスに関するお問い合わせ
03-6853-6300 | ContactJP@AvePoint.com | お問い合わせはこちらから:
https://www.avepoint.com/jp/about/contact AvePoint Japan 株式会社 | 〒108-0074 | 東京都港区高輪 4-10-18 | 京急第一ビル 11F