

FORTUNE 100 企業がデータセキュリティインシデントを 80% 削減



保険

製品

- Vontu Network Monitor および Vontu Network Prevent
- Vontu Enforce Platform

主な利点

- 6 カ月間、擬陽性インシデント誤認識ゼロを達成
- データセキュリティインシデントを 80% 削減
- CEO は四半期レポートからデータセキュリティをさらに正確に把握可能
- 通常業務時間の 20% 未満で DLP イニシアティブを管理
- 米国および州のプライバシー規制のコンプライアンスを実証

Vontu ソリューションが選ばれた理由

- すぐに使える包括的なレポート機能
- セキュリティチームがインシデントの詳細情報を迅速に入手可能
- わかりやすいユーザーインターフェース
- 精度の高い検出機能

500 万人を超える米国人が、彼らを保護してくれる米国のある大手生命保険会社に信頼を置いている。この会社には、「信頼」というブランドがあるため、顧客の個人データの安全を維持することに関しては余念を許さない。

このブランドの公約を維持するために同社では、Vontu Network Monitor と Vontu Network Prevent を含むシマンテックの Vontu データ漏えい対策 (DLP) ソリューションを利用している。同社は、Vontu ソリューションを導入以来、データセキュリティインシデントを 80% 削減し、擬陽性インシデントの検出をほぼゼロにした。Vontu DLP ソリューションにより CEO は全社のデータセキュリティをより正確に把握できるようになり、データ保護ポリシーに関する社員の認知度を大幅に向上させた。また、HIPAA (医療保険の相互運用性と説明責任に関する法律) やデータプライバシーに関する米国州法の遵守を実証できるようになった。

正確な検出により所有コストを削減

ビジネスの性質上、生命保険会社では機密データを 1 万店の代理店や数百に上る取引先との間で機密データをやり取りする必要がある。最近起こっている企業のデータ漏えい事件やコンプライアンス規制の強化を受けて、同社は機密情報の漏えい防止にプロアクティブな対策を取ることに決めた。セキュリティチームでは、データ漏えいのリスク評価を実施し、電子メール、FTP、HTTP を経由して企業ネットワークの外部に顧客データが転送される危険性のある機会を特定できた。

「われわれは、潜在的なデータへの脅威の特定、違反している社員への通知、ビジネスプロセスのセキュリティ最適化の支援が可能なテクノロジーソリューションを評価した」と同社のセキュリティアーキテクトは説明する。「Vontu DLP ソリューションを選んだのは、精度の高い検出技術、卓越したレポート機能、矯正機能、およびインシデントレビュー機能があったからだ」。

Vontu DLP ソリューションが導入され、組織のポリシーが見直された結果、同社では 6 カ月連続で擬陽性インシデントの検出率がゼロになり、データセキュリティインシデントは 80% 削減された。さらに、CEO と事業部門に運用レポートが配信されるようになった。これらすべてが 0.2 人/月で管理されている。

「今では、様々なシステムを超えて、あらゆる詳細レベルまで個人情報特定できるようになった」と、このセキュリティアーキテクトは言う。

通知およびレポート機能がデータ漏えいインシデントの削減に寄与

同社では Vontu Network Monitor を使用し、SMTP、HTTP、FTP、NNTP、UTCP、およびインスタントメッセージ経由で送信されるアウトバウンドのネットワークトラフィックを検査し、顧客の機密データやポリシー違反を調査している。Vontu ソリューションは、ポリシー違反のあるアウトバウンドのトラフィックにフラグを立て、自動的に送信者にポリシー違反であることを通知する。この通知機能は社員の教育とデータ保護ポリシーの強化に役立ち、データセキュリティインシデントの発生リスクを約 80% 削減した。

「Vontu DLP ソリューションは、社員の行動を改めることができることを実証した、数少ないセキュリティ強化策の 1 つだ」。同社の副社長兼最高セキュリティ責任者はこのように語っている。「弊社では、一度違反の通知を受けた送信者の 90% 以上は、再び違反の通知を受けることがないと判断した。繰り返し違反する者を特定できた場合には、データにリスクが生じているビジネスプロセスを切り分けて、修正することができる」。

また、Vontu DLP ソリューションのレポート機能によってセキュリティチームは、直ちに対処する必要があるセキュリティインシデントをより効果的に特定し、優先的に対応することができる。さらに、社内で顧客データの移動パターンについて理解が深まり、長期的にリスクの評価と削減が可能になる。顧客の個人情報を守るプロアクティブな手順を講じることで、この会社では自社のブランドを守りながら、罰金や訴訟が発生するのを回避している。

同社のテクニカルアーキテクトは次のように話している。「Vontu DLP ソリューションでは、われわれが必要とするレポートがすぐに使える状態で提供される。他社のソリューションで同じレポートを作成しようとすれば、最大で 30 万ドルはかかるだろう」。

Vontu Network Monitor がセキュリティの心配を無用に

顧客データが Vontu Network Monitor で保護されるようになった今、この企業では HIPAA やデータプライバシーに関する米国州法などの規制遵守をより簡単に実証できるようになった。また、Vontu Enforce Platform は、社内のセキュリティ担当者が発生したポリシー違反を迅速に解決して報告できるように支援する。追加のセキュリティ対策として、Vontu Network Prevent も導入された。Vontu Network Prevent では、条件に応じて機密データを含むトラフィックにタグが付けられ、安全に配信できるように暗号化ゲートウェイに転送される。

「弊社のリスク漏えい対策および削減の取り組みにおいて、Vontu は重要なパートナーである」と、テクニカルアーキテクトは結論付ける。「われわれは、Vontu の統計資料をデータ漏えい対策の成功を示す書類として会長の四半期決算報告書にも添付している」。

株式会社シマンテック

〒107-0052 東京都港区赤坂 1-11-44 赤坂インターシティ

www.symantec.com/jp/vontu

「Vontu DLP ソリューションは、社員の行動を改めることができることを示した、数少ないセキュリティ強化策の 1 つだ」。

副社長兼最高セキュリティ責任者

稼働中の Vontu ソリューション

1. **Vontu Network Monitor** : SMTP、HTTP、FTP、NNTP、UTCP、インスタントメッセージングなどを含むネットワークを常時スキャンし、機密データがないか調査する。
2. **Vontu Network Prevent** : 社外に送信されるメッセージをブロックする。
3. **Vontu Enforce Platform** : ポリシー違反があった場合に直ちに社員と管理者にアラートを送信する。それにより、すべての社員にデータポリシーの遵守と責任を認識させることができる。

