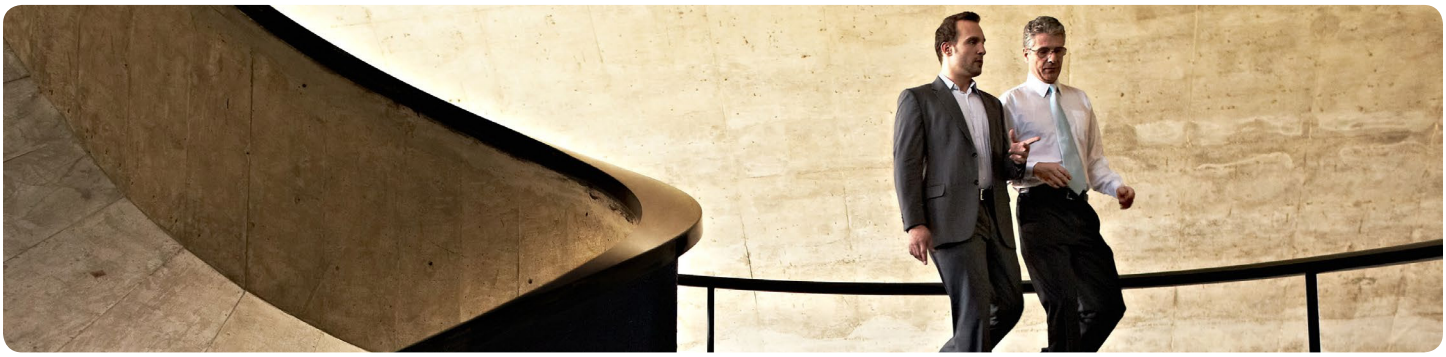
Solutionary がシスコと MapR Technologies でセキュリティを大幅に強化



概要

- **お客様名:**Solutionary
- **業種:**IT セキュリティおよびマネージド サービス
- **所在地:** ネブラスカ州オマハ
- **従業員数:**310 名
- **データ ボリューム:**1 兆メッセージ/年（ペタバイト ストレージ）

課題

- 顧客のセキュリティを強化するためにデータ分析機能を向上させる。
- 顧客数とデータ ボリュームの増加に合わせて拡張性を向上させる。
- 需要に対応するためのデータベース ソリューションの拡張にかかるコストを削減する。

ソリューション

- Cisco UCS Common Platform Architecture（CPA）for Big Data と MapR の併用

導入の効果

- セキュリティ イベントの関連性と影響を調査するために必要な時間を短縮。
- データ可用性の向上により、新規サービスおよびセキュリティ分析を促進。
- 必要に応じてキャパシティを展開できるため俊敏性が向上。

テクノロジー/アプリケーション パートナー

- MapR Technologies

マネージド サービス プロバイダーがセキュリティ ソリューションを強化し、Cisco UCS と MapR で提供する Apache Hadoop データ ソリューションのパフォーマンス向上を実現

課題

北米有数のマネージド セキュリティ サービス プロバイダー（MSSP）の Solutionary は、中堅企業やグローバル企業にマネージド セキュリティ サービスとプロフェッショナル コンサルティング サービスを提供しています。2000 年に設立された同社は、独自のセキュリティ分析テクノロジーを活かして、顧客のリスク軽減、データ セキュリティの強化、コンプライアンス イニシアティブのサポートを行っています。

顧客と緊密な連携を行い、専用のカスタマー サービスを提供している Solutionary は、業界でも常にトップクラスの顧客定着率を維持しています。

特許取得済みの Solutionary ActiveGuard セキュリティおよびコンプライアンス プラットフォームには顧客のトラフィック、具体的には、膨大な量のイベント データと詳細なユーザ アクティビティを、リアルタイムで分析する機能が含まれています。ActiveGuard は、挙動パターン、異常なアクティビティ、攻撃の兆候など、企業の全アクティビティを分析し、グローバルな脅威とトレンドすべてについてデータを相関付けます。これにより顧客は、コンテキストを把握しアラートに基づいて対策が取れるようになります。

ActiveGuard テクノロジーは、素早く正確にセキュリティ イベントを識別します。Solutionary の研究開発ディレクタであるスコット・ラスマン氏は次のように述べています。「Solutionary の MapR/Cisco UCS クラスタは ActiveGuard とともに水平拡張することが可能であり、非構造化データを分析して高度で巧みな攻撃を検出するとともに、処理された構造化データとコンテキスト データを関連付けることができます」。

増え続けるデータ量に加え、迅速なセキュリティ分析の必要性と顧客基盤の急激な拡大という面からも、環境を素早く拡張できるようにすることが Solutionary にとって急務となっていました。こうした急成長下では、従来のデータベース ソリューションを補強して、コスト効果とパフォーマンスの高い環境で動的な拡張ができるようにする必要があります。MapR

「MapR と Cisco UCS はどちらも、高パフォーマンス、効率のよい管理、使いやすさなど、多くの価値をもたらしました。両方のソリューションを併せて使用することで、セキュリティ分析サービスを拡張しながら、複雑さとコストを管理できます」

— **デイブ・キャプリンガー**
Solutionary のアーキテクチャ担当ディレクタ

Technologies の Apache Hadoop ソリューションを導入することで、Solutionary におけるビッグ データの処理方法は一新されました。構造化データが保管される従来型のデータベースとは異なり、Hadoop では 1 つのデータ インフラストラクチャ上に構造化データと非構造化データをスムーズに分散および分析することができます。

Solutionary では、MapR ソリューションと Cisco Unified Computing System™（UCS®）を組み合わせ、最適化と拡張が簡単な高パフォーマンスのプラットフォームを実現し、増え続ける需要に対応できるようにしました。Solutionary のアーキテクチャ担当ディレクタであるデイブ・カプリンガー氏は次のように述べています。「MapR と Cisco UCS を導入し、Hadoop のクラスタ インフラストラクチャが持つ非常に優れた拡張性を活かして、パフォーマンスと柔軟性を手に入れることができました。このインフラストラクチャなら、ビッグデータのリアルタイム分析を実行して、高度で組織的な国家ぐるみの攻撃に対する保護と防衛に役立てることができます」。

ソリューション

Hadoop テクノロジーをリードする MapR は、企業でも利用できるように Hadoop を変革し、業界随一の包括性を誇る Hadoop プラットフォームを提供しています。Apache Hadoop 向け MapR M7 エンタープライズ エディション（Solutionary で使用されているシスコ互換製品）は、高可用性に特化して設計されたアーキテクチャを活かし、他の Hadoop ディストリビューションにはない高度な機能を提供します。

Solutionary では、MapR Direct Access NFS 機能が提供する業界標準の NFS を利用して、パフォーマンスを損なわずに既存のシステムとスムーズに統合することができました。 データのスナップショットとミラーリングによる信頼性の高いデータ保護でデータ セキュリティが強化されるとともに、MapR Heatmap によるモニタリングでスタッフはクラスタの健全性と現在の容量を一目で確認できます。

Solutionary が特に高く評価しているのが、すべてのジョブを正常に完了させるのに役立つ MapR JobTracker HA 機能です。この機能によって、パフォーマンスが大幅に高速化したうえに、インフラストラクチャ スタッフの手動管理も減らすことができたのです。「MapR は Apache Hadoop のパフォーマンスと管理性を新たなレベルに引き上げました。社内システムにシームレスに統合でき、顧客向けデータ分析のスピードとキャパシティが大幅に向上しました」（カプリンガー氏）。

Solutionary では、16 台の Cisco UCS C240 M3 ラック サーバからなる 2 つのクラスタを含む Cisco® UCS CPA for Big Data 環境で MapR を使用しています。高密度でエンタープライズクラスの Cisco UCS C240 サーバは、データ負荷の高いアプリケーションやストレージ負荷の高いインフラストラクチャ ワークロードでも問題なく動作するように設計されており、Hadoop ソリューションに最適なハードウェアです。この Cisco UCS CPA for Big Data 環境により、総所有コスト（TCO）を削減しながら、拡張性とビジネスの俊敏性を高めることができます。

また、Cisco UCS Manager により、サーバとネットワーク リソースの統合管理を実現しています。また、すべての接続機器への統合管理ポイントとして機能する Cisco UCS 6200 シリーズ ファブリック インターコネクトにより、高帯域幅で低遅延の接続がサーバに提供され、拡張性の高いファブリック インターコネクトにより、MapR クラスタに必要な大量のノードをサポートできます。さらに、Cisco UCS 2200 シリーズ ファブリック エクステンダによって各ラックにネットワークを拡張することができます。

「MapR と Cisco UCS はどちらも、高パフォーマンス、効率的な管理、使いやすさなど、多くの価値をもたらしました。両方のソリューションを併せて使用することで、セキュリティ分析サービスを拡張しながら、複雑さとコストを管理できます」（カプリンガー氏）。

導入の効果

シスコと MapR の Hadoop 実装環境のデータ処理機能を使用することで、Solutionary はデータ モデリングとイベントの予測分析の処理を加速させるとともに、ActiveGuard プラットフォームが処理できるトラフィック量を増やすことができました。たとえば、従来のハードウェア展開とデータ構造では、ActiveGuard が分析に使用できる有益なデータの寿命が限られていました。

Hadoop によって、ActiveGuard がアクセスできるデータ分析とコンテキスト データの量は大幅に増加しました。その結果、攻撃の兆候を認識しやすくなり、幅広くグローバルな相関を見ることで攻撃者の狙いや技法を正しく把握できるようになりました。この機能により、顧客間で共通して現れるグローバルなパターンもコスト効率よく迅速に識別できます。

パフォーマンスが大幅に向上し、Solutionary の ActiveGuard プラットフォームでより複雑なプロセスを実行できるようになりました。新しい脅威が発見された場合には、数ミリ秒以内で全顧客を対象にアクティビティをグローバルに検出し、分析できます。以前の環境では、こうした一見単純なタスクが非常に困難でコスト高になり、事前に計画して最適化された環境でさえ 30 分もかかることがありました。

「今日の攻撃のスピードや巧みさ、エンタープライズ環境で生成されるデータの膨大な量を考えると、Solutionary には、顧客への増え続ける攻撃に素早く対応できる高パフォーマンスで拡張性の高いインフラストラクチャが必要でした。その解決策となったのが、MapR と Cisco UCS CPA for Big Data 環境です。パフォーマンスとビッグデータ分析機能が大幅に向上し、顧客への攻撃を防衛し、影響を最小限に抑えることができるのです」（ラスマン氏）。

合理化されたシスコ環境によって、Solutionary スタッフの管理作業は簡素化されました。機器と接続はすべて Cisco UCS Manager を使用してプロビジョニングし、管理できます。Cisco UCS ファブリック インターコネクトがシスコ インフラストラクチャの集中管理ポイントとして機能するため、環境内の各要素を別々に管理する必要はなくなりました。

Cisco UCS Manager の自動プロビジョニングと構成により、環境の変更に必要な時間が短縮され、管理の合理化が進み、拡張性が向上しました。「以前のインフラストラクチャでは、新しい機器の追加は時間とリソースのかかるプロセスでした。Cisco UCS では、必要に応じてインフラストラクチャを拡張でき、増え続ける動的なビジネス ニーズに即応できるようになりました」（カプリンガー氏）。

次のステップ

Solutionary では、Cisco UCS CPA for Big Data および MapR 環境の Hadoop テクノロジーを使用して分析機能を強化し、機械学習、予測型モデリング、および分析を拡張して、ゼロデイ脆弱性を悪用した高度な技法が含まれる Advanced Persistent Threat（APT）の検出性能を向上させることを計画しています。「Cisco UCS と MapR によって、グローバルなセキュリティ インテリジェンスを強化し、現在のサービスを拡張できました。また、ほぼリアルタイムの高度な挙動分析と機械学習も可能になりました。これは従来のプラットフォームでは考えられなかったことです。なぜなら、精度が高く素早い攻撃はペタバイトものデータの中に埋もれていたからです」（ラスマン氏）。

製品リスト

データセンター ソリューション

- Cisco Unified Computing System (UCS)
- Cisco UCS C240 M3 ラック サーバ

ルーティング/スイッチング

- Cisco Catalyst 6500 シリーズ スイッチ

ファブリック インターコネクト

- Cisco UCS 6200 シリーズ ファブリック インターコネクト
- Cisco UCS 2200 シリーズ ファブリック エクステンダ

ネットワーク管理

- Cisco UCS Manager

アプリケーション

- Apache Hadoop 向け MapR M7 エンタープライズ エディション

cisco Compatible

関連情報

シスコ ユニファイド データセンターの詳細については、
www.cisco.com/web/JP/solution/datacenter/products.html をご覧ください。
Cisco UCS ビッグデータ ソリューションの詳細については、
http://www.cisco.com/jp/go/bigdata/をご覧ください。
Cisco UCS ビッグ データ ソリューションと MapR の併用の詳細については、
www.cisco.com/en/US/docs/unified_computing/ucs/UCS_CVDs/Cisco_UCS_CPA_for_Big_Data_with_MapR.html [英語] をご覧ください。
MapR Technologies の詳細については、
https://marketplace.cisco.com/catalog/companies/2032 [英語] をご覧ください。
MapR M7 エンタープライズ エディションの詳細については、
http://www.mapr.com/jp/products/mapr-m7-editionをご覧ください。

cisco Available in the Cisco Developer Network Marketplace

お問い合せ先

cisco

シスコシステムズ合同会社
〒107 - 6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp

COO-XXXXXX-00JA 16.02