金融機関向け Cisco Secure Firewall

目次

ネットワークとセキュリティの統合

世界クラスのセキュリティ制御

一貫性のあるポリシーと可視性

ネットワーク全体をセキュリティアーキテクチャの拡張として利用する

ビジネスクリティカルなアプリケーションにおいてハイブリッド環境やマルチクラウド環境の採用が広がり、従業員はどこからでも安全にリソースにアクセスできる必要がある今、従来のファイアウォールアプローチでは十分なセキュリティを確保できません。以前のネットワーク境界は単一でしたが、今や複数のマイクロ境界に分化しています。多くの金融機関にとって、アプリケーションは新しい境界であり、ファイアウォール環境も従来型のものから、物理アプライアンス、仮想アプライアンス、およびクラウドネイティブ アプライアンスが混在する環境へと進化しました。その結果、企業は最新のアプリケーション環境のサポートを運用するのに苦労していて、企業をリスクにさらす脆弱性を突かれることなく、一貫した可視性、ポリシーの適用、統一された脅威の可視性を維持するという課題に直面しています。

シスコでは、ネットワークセキュリティのビジョン「NetWORK」の構築を進めています。これは、ネットワーク（Net）が機能する（WORK）ことを目指すというビジョンであり、俊敏性に優れ、自動化された統合アプローチを可能にすることで、最新の動的アプリケーション全体、また多様化が進むネットワーク全体でポリシーを一致させ確実に適用するというものです。Cisco Secure Firewall は、コアネットワーキング機能とネットワークセキュリティを最も緊密に統合し、これまでで最も安全なアーキテクチャを構築できます。その結果、あらゆる場所でアプリケーションとユーザーを保護する完全なセキュリティポートフォリオが実現します。

メリット

- 統合されたリアルタイムのワークロードおよびネットワークセキュリティにより、動的アプリケーション環境を統合制御できます。
- ネットワークセキュリティに対するプラットフォームアプローチにより、主要なソースから得られるインテリジェンスの活用と共有が可能になり、検出、対応、修復を迅速化できます。時間や場所、使用デバイスを問わず、社内ネットワークへの安全性の高いアクセスを実現するとともに、企業、従業員、重要なアプリケーションを保護する強力な侵入防御機能を利用することで、リモートワーカーを保護できます。
- すべての Cisco® Secure Firewall に SecureX™ の利用権限が付与されているため、セキュリティに対する緊密に統合されたアプローチを取ることができ、Cisco Secure ポートフォリオ全体で脅威の関連付けが可能になり、インシデント対応を迅速化できます。

優れた可視性と制御

脅威はより高度になり、ネットワークはより複雑になっています。常に最新の状態を維持し、絶え間なく出現し進化する脅威を巧みに回避するためのリソースを備えた金融機関はほとんどありません。

脅威とネットワークがより複雑になるにつれ、データ、アプリケーション、およびネットワークを保護する適切なツールが不可欠になります。Cisco Secure Firewall は、脅威の一歩先を行くために必要な機能と柔軟性を備えています。暗号化されたトラフィックを大規模に検査する独自のハードウェアベース機能に加え、前世代のアプライアンスを 3 倍以上回るパフォーマンスを提供します。また、Snort 3 IPS は人間が読めるルールであるため、セキュリティのシンプル化に役立ちます。Cisco Secure Workload を統合することで、動的アプリケーションの可視化と制御が可能となり、ネットワークとワークロード全体で今日の最新のアプリケーションを一貫して保護できます。

自社に最適なファイアウォールを探す

シンプルで一貫性のあるポリシー管理

Cisco Secure Firewall ポートフォリオにより、将来に向けた柔軟な管理機能を備えた、強力なセキュリティ態勢が実現します。シスコは、ビジネスニーズに合わせてカスタマイズ可能な幅広い管理オプションを提供しています。

- **Cisco Secure Firewall Device Manager**：単一のファイアウォールをローカルで管理。Firewall Threat Defense のオンデバイス管理ソリューション
- **Cisco Secure Firewall Management Center**：大規模なファイアウォール環境を管理。オンプレミス、プライベートクラウド、パブリッククラウド、Software as a Service（SaaS）などのあらゆるフォームファクタで利用可能
- **Cisco Defense Orchestrator**：Cisco Secure Firewall、Meraki® MX、Cisco IOS® デバイスなど、複数のシスコ製品にわたってセキュリティポリシーとデバイス管理を合理化できる、クラウドベースの管理ソリューション

また、シスコは、拡張性の高いログ管理を可能にする Cisco Security Analytics and Logging も提供しています。これにより、脅威検出を強化できます。さらに、保持期間延長機能やふるまい分析機能も備わっているため、組織全体におけるコンプライアンス要件も満たせます。

Lake Trust Credit Union の導入事例

シスコが選ばれる理由

Cisco Secure Firewall ポートフォリオは、進化を続ける複雑な脅威からネットワークをより強力に保護します。シスコ製品を利用すれば、俊敏性と統合性の両方を兼ね備えたセキュリティ基盤に投資していることになります。これにより、現在と将来にわたって最も強力なセキュリティ態勢を構築できます。

データセンター、支社、企業オフィス、クラウド環境など、あらゆる場所からシスコの力を活用して、既存のネットワーク インフラストラクチャをファイアウォール ソリューションの拡張機能に変換し、必要なあらゆる場所で世界トップレベルのセキュリティ制御を実現できます。

Cisco Secure Firewall アプライアンスに投資することで、暗号化されたトラフィックを検査する際のパフォーマンス低下を起こすことなく、最も高度な脅威からも確実に保護できます。さらに、他のシスコソリューションや他社製のソリューションと統合することで、セキュリティ製品の幅広い豊富なポートフォリオを活用できます。こうした製品を連携させれば、これまでばらばらだったイベントを相互に関連付け、ノイズを除去し、脅威を迅速に阻止できます。

Cisco Secure Firewall の先進的な機能

先進的な機能	詳細
Cisco Secure Workload 統合	• Cisco Secure Workload（旧 Tetration）を統合することで、ネットワークとワークロード全体で最新の分散アプリケーションや動的アプリケーションを包括的に可視化し、拡張可能な方法で一貫してポリシーを適用できます。
Cisco Secure Firewall Cloud Native	• Kubernetes で構築され、AWS で初めて利用可能になった Cisco Secure Firewall Cloud Native は、開発者向けの使いやすいアプリケーション アクセス ソリューションであり、柔軟性の高いクラウドネイティブなインフラストラクチャを構築できます。
動的ポリシーのサポート	• 動的属性は、静的 IP アドレスを利用できない場合に VMware、AWS、Azure タグをサポートします。 • シスコはタグベースのポリシーにおけるパイオニアであり、セキュリティグループタグ（SGT）と Cisco Identity Services Engine（ISE）の属性サポートを提供しています。
Snort 3 侵入防御システム	• 脅威に対して一段階上の保護を提供し、業界をリードするオープンソースの Snort 3 は、検出精度の向上、カスタマイズの簡素化、パフォーマンスの向上に役立ちます。
Transport Layer Security（TLS）サーバーアイデンティティ検出	• 暗号化された TLS 1.3 トラフィックに対し、レイヤ 7 のポリシーを維持できます。すべてのトラフィックフローを復号して検査することが現実的ではない、暗号化された環境でも可視性と制御を維持します。競合他社のファイアウォールは、暗号化された TLS 1.3 トラフィックではレイヤ 7 のポリシーを無効にします。
Cisco Secure Firewall Management Center	• ファイアウォール、アプリケーション制御、侵入防御、URL フィルタリング、マルウェア防御のポリシーを包括的に管理します。 • Cisco Secure Workload（旧 Tetration）と統合することで、ネットワークとワークロード全体で、動的アプリケーションに対する一貫した可視化とポリシー適用を実現できます。
Cisco Defense Orchestrator	• Cisco Secure Firewall 全体でポリシー管理を一貫して簡単に行えるようにするクラウドベースのファイアウォール管理ツールです。
Cisco Security Analytics and Logging	• 拡張性に優れたオンプレミスベースおよびクラウドベースのファイアウォールのログ管理機能とふるまい分析機能により、リアルタイムの脅威検出が可能になり、対応時間が短縮されます。さらに、継続的に分析することで、セキュリティ態勢の見直しを進め、将来の脅威に対する備えを強化することができます。 • すべての Cisco Secure Firewall からのログを集約することで、コンプライアンスのニーズに対応できます。 • ファイアウォールマネージャとの緊密な統合によって、ロギングと分析を拡張し、ファイアウォールログデータを単一の直観的なビューに集約します。
Cisco SecureX	• SecureX プラットフォームを活用すれば、脅威検出と修復を迅速化できます。すべての Cisco Secure Firewall には Cisco SecureX の利用権限が付与されています。Firewall Management Center に新しく追加された SecureX リボンにより、セキュリティチームは即座に SecureX のオープンなプラットフォームに切り替えられるようになったため、インシデント対応を迅速化できます。
Cisco Talos® 脅威インテリジェンス	• Cisco Talos インテリジェンスグループは、民間の脅威インテリジェンスチームとしては世界で最大の組織の 1 つです。シスコのお客様、製品、サービスを保護するための正確かつ実用的な脅威インテリジェンスを迅速に作成します。また、Talos は、Snort.org、ClamAV、SpamCop の公式ルールセットの保守も行っています。

次のステップ

Cisco Secure Firewall の詳細や金融サービス向けの他のセキュリティソリューションについては、ポートフォリオエクスプローラをご覧ください。シスコのセールス担当者への問い合わせや、購入オプションの確認はこちらからお願いいたします。

シスコ コンタクトセンター

自社導入をご検討されているお客様へのお問い合わせ窓口です。
製品に関して | サービスに関して | 各種キャンペーンに関して | お見積依頼 | 一般的なご質問

お問い合わせ先
お電話での問い合わせ
平日 9:00 - 17:00
0120-092-255

お問い合わせウェブフォーム
cisco.com/jp/go/vdc_callback

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
cisco.com/jp

0415-2024-000-X