NETSCOUT

Arbor Threat Mitigation System(TMS)

実績のある包括的な脅威保護対策とサービス提供プラットフォーム

主な機能と特長

正確なミティゲーション

正規のビジネストラフィックのフローを中断することなく、攻撃トラフィックのみを自動的に駆除します。

ミティゲーションプラットフォームと能力を柔軟に選択可能

さまざまなミティゲーションプラットフォームと能力を柔軟に選択できます。

- 2Uアプライアンス(500Mbps ～ 400 Gbps)
- 6Uシャーシ(10～100Gbps)
- 仮想アプライアンス: Cisco ASR 9000 ルーター用(10～60Gbps)、KVM/Vmwareハイパーバイザー用(1～40Gbps)

8Tbpsのミティゲーション能力の一元的なコマンド＆コントロール

DDoS攻撃に対する防御をこれまでに前例のないレベルまで拡張することができます。デプロイメントあたり最大8テラビットの集約ミティゲーション能力を配備し、一元管理できます。

マネージドサービスを提供可能に

Arbor TMSを利用することで、急速に高まるDDoS攻撃防御サービスの需要に対応し、収益性の高いDDoS攻撃防御サービスをクラウド上で提供可能になります。

包括的な攻撃対策

大規模で複雑な帯域幅占有型、TCP状態枯渇型、そしてアプリケーション層へのDDoS攻撃から、自社のインフラストラクチャや顧客を保護することができます。

柔軟な導入形態

ネットワークのさまざまな領域にアプリケーション層インテリジェンス、脅威検知、そして正確なミティゲーションの機能を配備して、インフラストラクチャを保護すると同時に、より収益性の高いマネージドDDoS攻撃防御サービスの提供が可能となります。

今日のISP(インターネットサービスプロバイダー)、クラウドプロバイダー、そして大企業は、共通の問題に直面しています。分散型サービス拒否(DDoS)攻撃は、サービスの可用性の確保に大きなリスクとなります。DDoS攻撃の威力や巧妙さ、そして頻度は高まる一方です。データセンター事業者やネットワークサービスプロバイダーは今、費用対効果が高く、管理も容易で実効性のある防御対策を必要としています。Arbor Threat Mitigation System(TMS)は、優れたDDoS攻撃防御ソリューションとしてすでに広く認知されています。サービスプロバイダー、クラウドプロバイダー、そして大企業が、数あるDDoSミティゲーションソリューションの中からArbor TMSを選択しており、導入が加速しています。

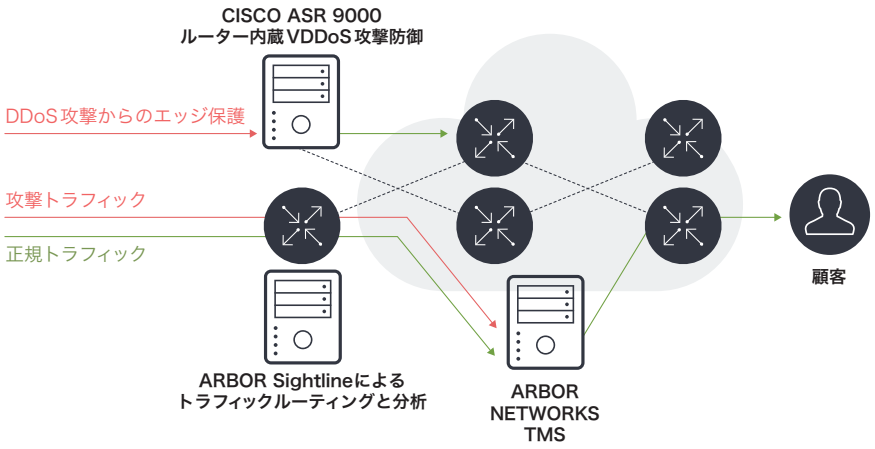
ArborのDDoS攻撃防御ソリューション

Arborのソリューションは、ネットワーク全体をカバーする脅威インテリジェンス、異常の検知能力、そしてキャリアグレードの脅威管理機能を統合することで、帯域幅占有型、TCP状態枯渇型、およびアプリケーション層に対するDDoS攻撃を特定し、阻止することができます。

Arbor TMSネットワークアプライアンスは、Arborのソリューションに不可欠なトラフィックのスクラビングコンポーネントを提供します。Arbor TMSをインラインで配備することで、「常時稼働」の防御機能を提供することができます。また、他の製品とは異なり、「ダイバーション分析/リインジェクション(再注入)」と呼ばれるミティゲーションアーキテクチャをサポートしています。このモードでは、Arborのソリューションによって生成されるルーティング情報の更新を通じて、DDoS攻撃を実行するトラフィックストリームのみがArbor TMSにリダイレクトされます。Arbor TMSは、そのようなストリームから悪意のあるトラフィックだけを取り除き、正規のトラフィックを意図された送信先へ転送します。

このArbor独自の機能は、サービスプロバイダーや大企業、そして大規模なホスティング/クラウドプロバイダーに大きなメリットをもたらします。これにより、中央に位置する単一のArbor TMSが、複数のリンクやデータセンターを保護することが可能になります。その結果、極めて効率的なミティゲーションの実行、そして侵害を受けることのない完全なセキュリティが実現します。インラインのデバイスでは、監視先のリンクにおけるすべてのトラフィックを常に検査しなければなりません。Arbor TMSでは、特定のターゲットへの攻撃に応答してリダイレクトされるトラフィックのみを効率良く検査ことが可能です。

Arbor TMSは、2Uアプライアンス(500Mbps～400Gbps)、6Uシャーシ(10～100Gbps)、Cisco ASR 9000ルーター内蔵型(10～60Gbps)、およびKVM/Vmwareハイパーバイザーをサポートする仮想アプライアンス(1～40Gbps)など、さまざまなミティゲーションプラットフォームと能力を柔軟に選択できます。



包括的な脅威検知機能

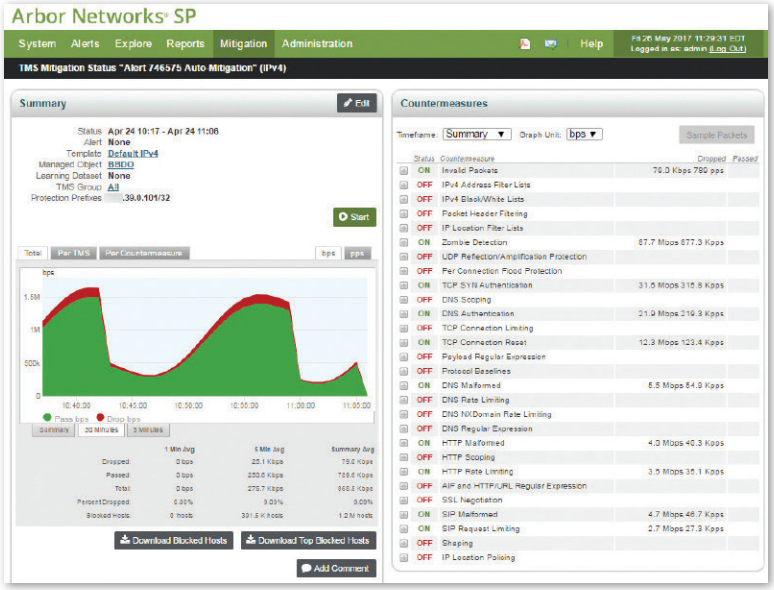
データセンターや公衆ネットワークは、常にさまざまなDDoS攻撃の標的となっています。そのような攻撃対象としては、インフラストラクチャ機器（ルーター、スイッチ、ロードバランサーなど）、ドメインネームシステム（DNS）、帯域幅、そしてWeb、eコマース、音声、ビデオなどの重要なアプリケーションが挙げられ、ファイアウォールや侵入防止システムなどのセキュリティデバイスでさえも攻撃の標的にされることがあります。Arborのソリューションは、業界で最も包括的で適応性に優れた脅威検知機能を備えており、複雑な複合型攻撃からさまざまなリソースを保護するように設計されています。脅威検知機能には、統計的異常検知、プロトコル異常検知、フィンガープリント照合、プロファイル化された異常検知などがあります。Arborのソリューションは、攻撃だけでなく需要とサービスレベルの異常な変化についても、リアルタイムで継続的にデータを収集・学習し、管理者へ警告します。

わずか数秒で正確なミティゲーションを実行

効果的にミティゲーションを実行する上で重要なのは、攻撃トラフィックを特定してブロックすると同時に、正規トラフィックを意図された送信先へ確実に配信することです。大規模なDDoS攻撃は、狙った標的だけでなく、同じネットワークサービスを共有している他の顧客にも影響を及ぼします。このような二次的な被害を軽減するために、サービスプロバイダーやホスティングプロバイダーが標的となったサイトへのトラフィックをすべて遮断してしまい、結果的にDDoS攻撃が成功してしまうケースもあります。Arbor TMSは、帯域幅を占有し枯渇させる大規模なフラッド攻撃、あるいはWebサイトを稼働停止に追い込む標的型攻撃のいずれの場合も、他のユーザーに影響を与えることなくわずか数秒で攻撃トラフィックを分離して駆除します。Arbor TMSでは、悪意のあるホストの特定とブラックリストへの追加、IPロケーションベースのミティゲーション、プロトコルの異常検知によるフィルタリング、不正パケットの駆除、転送レート制限（正規トラフィックに対する需要の急増を適切に管理することが目的）などのさまざまな脅威防御手法が採用されています。
ミティゲーションは、自動的あるいは管理者主導で実行できるほか、防御手法を組み合わせて複合型攻撃に対処することも可能です。

リアルタイムのミティゲーションダッシュボード

Arbor TMSが備えるミティゲーションダッシュボードでは、DDoS攻撃に関する警告の原因や、攻撃への対策が発揮している効果を、管理者が単一のスクリーンでリアルタイムに確認できます。ダッシュボードから保護対策を変更することも可能で、完全なパケットキャプチャと復号を実行し、正規および攻撃パケットストリームの両方を詳細に確認することができます。これらの情報は保存され、あとで参照したりマネジメントへのレポートに活用できます。これにより。事業者および管理者はビジネスオペレーションに対する攻撃の詳細を理解し、レポートすることが可能になります。



警告とミティゲーションの状況をリアルタイム表示するダッシュボード

複数の脅威検知およびミティゲーション手法

ホワイトリストおよびブラックリストを使用して、既知の悪質なホストをブロック

ホワイトリストには承認されたホストが含まれ、ブラックリストにはゾンビホストや侵害を受けたホストが含まれるため、それらのトラフィックはブロックされます。

フィルター複合的に使用してアプリケーション層への攻撃をブロック

Arbor TMSは、ペイロードの可視化とフィルタリング機能を提供し、隠された攻撃によって重要なサービスが停止することを確実に防止します。

HTTPに特有の攻撃を検知しミティゲーションすることで、Webベースの脅威を阻止

このメカニズムは、フラッシュクラウドのシナリオへの対応にも有効です。

重要なDNSサービスの保護

DNSサービスをキャッシュポイズニング、リソース枯渇型/増幅型攻撃から保護するとともに、DNSサービスを詳細に可視化します。

VoIPサービスの保護

VoIP/SIPに特有の攻撃を検知し、ミティゲーションすることで、毎秒のパケットおよび不正要求フラッドを悪用する自動スクリプトやボットネットからVoIPサービスを保護します。

大規模な反射型/増幅型攻撃を阻止

Arbor TMSシャーシ単体で最大400 Gbpsの攻撃ミティゲーション能力を活用し、NTP、DNS、Memcached、SNMP、SSDP、SQL RS、Chargenなどを悪用する大規模な反射型/増幅型攻撃を停止します。

ATLAS Intelligence Feed

Arborの研究者は、トラフィックの監視およびセンサーのグローバルネットワークを活用してATLAS® Intelligence Feedを開発しました。この脅威インテリジェンスは、対象を的確に絞った防御機能のライブラリで、ボットネットベースの攻撃のほぼすべてを自動的に阻止します。ATLAS Intelligence Feedは、Arobrの研究者が新たな脅威を発見し無効化すると、自動的にArobor TMSの情報をアップデートして新しい保護機能を追加します。

拡張性の高いDDoS攻撃検知機能とミティゲーション能力

Arbor SPは、物理/仮想インスタンスのどちらも優れた拡張性を備えており、サービスプロバイダーのネットワーク全体を網羅する、顧客側のエッジからピアリングエッジ、データセンターエッジ（またはクラウドエッジ）、モバイルエッジ、さらには中間のバックボーンネットワークに至るまで、包括的なDDoS攻撃検知機能を提供します。比類ない可視性を提供するArbor SPのワークフローにより、Arbor TMSやCisco ASR 9000のvDDoS攻撃防御機能を活用した迅速で効果的なDDoS攻撃のミティゲーションが実現します。防御対策に基づくミティゲーション能力は、TMS HD1000あたり最大400Gbps、デプロイメントあたり最大8Tbpsまで拡張できます。ブラックリストを活用すると、防御対策によるミティゲーションの前にさらなる保護レイヤーを追加できます。
Cisco ASR 9000 vDDoS攻撃防御ソリューションでは、ネットワークのあらゆるエッジにおいて最大で数十Tbpsクラスの大規模な防御能力の発揮し、OpenFlowを活用して脅威をブラックリストに登録するため、コアリンクを攻撃から保護します。

包括的な管理とレポーティング機能

Arbor TMSは、最大8テラビットのミティゲーション能力の制御を一元的に表示および管理できるため、容易で効率的な運用が実現します。これにより、複数の大規模な攻撃を阻止し、ミティゲーションプロセスを要約した顧客やマネジメント部門向けの包括的なレポートを作成することができます。

マネージドDDoS攻撃防御サービスを提供可能なプラットフォーム

Arborのソリューションによって、サービスプロバイダーやホスティング/クラウドプロバイダーは顧客向けにDDoS攻撃防御サービスを提供できるようになります。カスタマイズされたポータルへのアクセス、APIの提供、管理権限の委譲が可能であるため、マネージドサービスプロバイダー（MSP）は顧客のニーズに応じて柔軟にサービスをカスタマイズし、制御できます。Arborは、マネージドDDoS攻撃防御サービス分野で定評のあるリーダー企業で、その最先端のサービスは多くのお客様に採用されています。

Arbor TMS DDoS攻撃防御ソリューションの技術仕様

同時セッション数	制限なし	
導入モード	インラインアクティブ、インラインモニタリング、SPANポートによる監視、ダイバーション分析/リインジェクション（最注入）	
ブロックアクションの詳細	送信ソースのブロック/停止、パケット毎のブロック、送信元、ヘッダーおよび評価ベースのブロック、BGPFlowspecの送信元/宛先による自動ブロック	
防御可能な攻撃	反射型/増幅型フラッド攻撃（TCP、UDP、ICMP、DNS、mDNS、Memcached、SSDP、NTP、NetBIOS、RIPv1、rpcbind、SNMP、SQL RS、Chargen、L2TP、Microsoft SQL Resolution Service）、フラグメンテーション攻撃（Teardrop、Targa3、Jolt2、Nestea）、TCPスタック攻撃（SYN、FIN、RST、ACK、SYN-ACK、URG-PSH、その他のTCPフラグ/スローTCP攻撃の組み合わせ）、アプリケーション攻撃（HTTP GET/POSTフラッド、スローHTTP攻撃、SIP INVITEフラッド、DNS攻撃、HTTPSプロトコル攻撃）、SSL/TLS攻撃（不正SSLフラッド、SSL再ネゴシエーション、SSLセッションフラッド）、DNSキャッシュポイズニング、脆弱性攻撃、リソース枯渇型（攻撃（Slowloris、Pyloris、LOICなど）、フラッシュクラウド誤検知、ゲーム用プロトコルへの攻撃	
DDoS攻撃対策	**帯域幅占有型攻撃への対策**	**すべての攻撃への対策**
	無効パケット、IPアドレスフィルターリスト、ブラック/ホワイトフィルターリスト、パケットヘッダーによるフィルタリングIPロケーションフィルターリスト、ゾンビフラッド攻撃検知、UDP反射型/増幅型攻撃防御、コネクションフラッド攻撃別の防御、偽装TCP SYNフラッド攻撃防御、TCP SYN認証、TCPコネクション制限、TCPコネクションリセット、ペイロード正規表現フィルター、トラフィックシェーピング、IPロケーション用ポリシー設定、インラインフィルター、ブラックリストフィンガープリント、プロトコルベースライン	HTTP認証、不正HTTP検知、HTTPスコーピング、HTTP転送レート制限、HTTP/URL正規表現、DNS認証、不正DNS、DNSスコーピング、DNS転送レート制限、DNS正規表現、不正SIP、SIP要求制限、SSLネゴシエーション、ATLAS Intelligence Feed（AIF）

第13版年次『ワールドワイドインフラストラクチャセキュリティレポート』

Arborの第13版年次『ワールドワイドインフラストラクチャセキュリティレポート』（WISR）は、2016年11月から2017年10月までの1年間をカバーしています。Arborは、本レポート用に世界中のTier 1、Tier 2、Tier 3のサービスプロバイダー、ホスティング、モバイル、エンタープライズ、そしてその他のネットワーク事業者から、390件のアンケート回答を得ています。このアンケートは、事業者のセキュリティに関するコミュニティにおける経験や所見、懸念事項に関する情報を収集するために実施されています。過去と同様に、今回のアンケート調査で対象としたトピックには、インフラストラクチャと顧客に対する脅威、インフラストラクチャの保護に使用している技法やテクノロジー、セキュリティインシデントの管理、検知、対処の手段やメカニズムなどが含まれています。

DDoS攻撃に関する13年目のレポート

- 2017年に報告された最大のDDoS攻撃の規模は800Gbpsで、昨年に比べ60倍に増加しています。2018年3月には、1.7TbpsのMemcached攻撃が確認されました。ATLASのデータでも、2018年には極めて大規模な攻撃の頻度が劇的に増加していることが明らかになっており、今回のアンケート回答者の3分の1が、ピーク攻撃の規模が100Gbpsを超えていたと報告しています。エンタープライズおよびデータセンターの57%以上が、インターネットへの接続を完全に飽和させた攻撃を経験したと回答しており、2016年の42%からさらに増加しています。
- 回答者は、DDoS攻撃の頻度が引き続き増加していることを認識しています。サービスプロバイダーの回答者の45%が毎月21回以上の攻撃を受け、エンタープライズの回答者の29%は毎月20回以上の攻撃を受けたと回答しています。
- DDoS攻撃は多様化が続いており、サービスプロバイダーの59%、エンタープライズ、政府/教育機関（EGE）の48%が、自社ネットワークにおいてマルチベクトル攻撃（帯域幅占有型、TCP状態枯渇型、アプリケーション層への各攻撃など）を確認したと報告しています。

詳細情報

最新のレポートは、次のURLからダウンロードいただけます。
jp.arbornetworks.com

Arbor TMS 2600、2800、5000、HD1000の仕様

	Arbor TMS 2600	Arbor TMS 2800	Arbor TMS 5000	Arbor TMS HD1000
スループットおよびミティゲーション *2600/2800シリーズはソフトウェアライセンスが必要*	1Gbps、2Gbps、5Gbps、10Gbps（20Gbpsへのアドオン）の各ライセンス、最大15Mpps	10Gbps、20Gbps、30Gbps、40Gbpsの各ライセンス、最大30Mpps	**1xAPMe：**最大25Gbps、10Mpps **2xAPMe：**最大50Gbps、20Mpps **3xAPMe：**最大75Gbps、30Mpps **4xAPMe：**最大100Gbps、40Mpps	最大8個のパケットプロセッシングモジュール（PPM）、20Gbps（14Mpps）または50Gbps（25Mpps）の組み合わせによるミティゲーションスループットを追加、最大400Gbps、198Mpps
電源要件	冗長電源 **AC：**100～240VAC、50/60Hz、12/6A、**DC：**-40～-72V、**最大**28/14A	冗長電源 **AC：**100～240VAC、50/60Hz、12/6A、**DC：**-40～-72V、**最大**28/14A	冗長電源（4個）**AC：**100～120VAC/200～240VAC、50～60Hz、15A、**DC：**-48～-60VDC、最大90A	**AC：**2個の1,500W冗長電源、100～240VAC、15～10A、50～60Hz（x2）、**DC：**2個の1,500W冗長電源、-48～-60VDC、44A（x2）
電力要件および放熱	325W（最大）、280W（標準）、955BTU/時（280W）	325W（最大）、280W（標準）、955BTU/時（280W）	**1 x APMe：**1,090W（最大）、610W（標準）、2,081BTU/時 **2 x APMe：**1,125W（最大）、800W（標準）、2,730BTU/時 **3 x APMe：**1,440W（最大）、980W（標準）、3,344BTU/時 **4 x APMe：**1,595W（最大）、1,160W（標準）、3,958BTU/時	（1）MM、（5）ファン、（2）QSFP+、（4）QSFP28、（x1）PPM：327W、1,116BTU/時、（x4）PPM：569W、1,940BTU/時、（x8）PPM：932W、3,180BTU/時
サイズ	**シャーシ：**高さ2Uラックサイズ **重量：**17.76kg **高さ：**8.76cm **幅：**43.53cm **奥行：**50.8cm	**シャーシ：**高さ2Uラックサイズ **重量：**17.76kg **高さ：**8.76cm **幅：**43.53cm **奥行：**50.8cm	**シャーシ：**高さ6Uラックサイズ **重量：**34.99kg（AC電源含む）、26.54kg（DC電源含む）、APM-Eブレードあたり2.72kg追加されます **高さ：**265.76mm **幅：**482.6mm **奥行：**462.00mm（ハンドル含む）	**シャーシ：**高さ2Uラックサイズ **重量：**20.5kg（PPM 1台）、追加のMMPあたり0.73kg追加されます（最大8台） **高さ：**88.1mm **幅：**449mm **奥行：**50.8mm
ネットワークインタフェース	4x10G（SFP+）+ 8x1G（SFP）ポート	8x10GigE（SR/LR/混合ファイバー用SFP+）	32x10GigE（ブレイクアウトケーブル付属QSFP+、SR4/4LR）、8x40GigE（QSFP+ SR4/LR4）、4x100GigE（LR4）	**4x100G + 8x10G：**1～4つの100GbE QSFP28（LR）光トランシーバー +1 ～ 4つの4x10GbE QSFP+（SR/LR Lite）光トランシーバー、各トランシーバーに1つの4x10GbEブレイクアウトケーブル付属 **16x10G：**1～8つの10GbE SFP+（SR/LR）光トランシーバー +1 ～ 2の4x10GbE QSFP+（SR/LR Lite）光トランシーバー、各トランシーバーに1つの4x10GbEブレイクアウトケーブル付属
ストレージ	2x150GB SSD（RAID 1構成）	2x240GB SSD（RAID 1構成）	2x128GB SSD（RAID 1構成）	2x480GB SSD（RAID 1構成）
環境	**温度（動作時）：** 41°～104°F（5°～40°C） **相対湿度（動作時）：** 5～85%（結露しないこと）	**温度（動作時）：** 41°～104°F（5°～40°C） **相対湿度（動作時）：** 5～85%（結露しないこと）、73°～104°F（23°～40°C）の場合95%	**温度（動作時）：** 23°～104°F（-5°～40°C） **相対湿度（動作時）：** 5～85%（結露しないこと）	**温度（動作時）：** 39.2°～104°F（4°～40°C）

Arbor TMS 2600、2800、5000、HD1000の仕様

	Arbor TMS 2600	Arbor TMS 2800	Arbor TMS 5000	Arbor TMS HD1000
準拠規格	UL60950-1/CSA 60950-1（米国／カナダ）、EN60950-1（欧州）、IEC60950（インターナショナル）、CB証明書／テストレポート（あらゆる国際的な規格差異を含む）、GS証明書（ドイツ）、EAC-R認証（ロシア）、CE低電圧指令73/23/EEE（欧州）、BSMI CNS 13436（台湾）、KCC（韓国）、RoHS指令2002/95/EC（欧州）	UL 60950-1第2版/CSA C22.2 No. 60950-1-07第2版、低電圧指令2006/95/EC、安全指令2001/95/EC、CB証明書／テストレポート（IEC60950-1第2版、およびあらゆる国際的な規格差異を含む）、FCC 47CFR Parts 15、Verified Class A Limit、ICES-003 Class A Limit、EMC指令、2004/108/EC、EN55022、EN55024、EN61000-4-2、EN61000-4-3、EN61000-4-4、EN61000-4-5、EN61000-4-6、EN61000-4-8、EN61000-4-11、EN61000-3-2、EN61000-3-3、VCCI Class A ITE（CISPR 22、Class A Limit）、BSMI承認、CNS 13438、Class AおよびCNS 13436安全、KCC認証、Gost認証、CISPR 22 Class A Limit、CISPR 24 Immunity、改正RoHS指令2011/65/EU	RoHS 6/6、IEC/EN/UL 60950-1、FCC Part 15 Subpart B Class A、ETSI EN 300 386、ULマーク、CEマーク	RoHS 6/6、IEC/EN/UL/CSA 60950-1、FCC Part 15 Subpart B Class A、EN 55022、EN55024、ETSI EN 300 386、cCSAusマーク、CEマーク、KN22、KN24、RCMマーク、KCC、EAC、BIS、CCCマーク（申請中）
ハードウェアバイパス	外部			

仮想 TMS（vTMS）

サポートされるハイパーバイザー	x86_64アーキテクチャ、最近のLinuxディストリビューション上で動作するVMwareまたはKVM
仮想マシンの仕様	**コア数：**3～32、RAM：9.5～56GB、**ミティゲーションインタフェース：**1～8、管理インタフェース：1～2
ミティゲーションスループット構成	**3コア、ハードウェアパススルーなし：**3 vCPU、9.5GB RAM、100Gbのディスク容量、2x Virtio管理インタフェース、2x Virtioミティゲーションインタフェース：1Gbps **3コア、ハードウェアパススルーあり：**3 vCPU、9.5GB RAM、100Gbのディスク容量、2x Virtio管理インタフェース、8x Intel 82599 PCIパススルーミティゲーションインタフェース：6Gbps **16コア、ハードウェアパススルーあり：**16 vCPU、29GB RAM、100Gbのディスク容量、2x Virtio管理インタフェース、8x Intel 82599 PCIパススルーミティゲーションインタフェース：40Gbps
サポートするNFV管理およびオーケストレーション	Openstack（Heat、Tracker、Ansible、Cisco NSO/ESC、Nokia CloudBand、AWS CloudFormation

NETSCOUT

米国本社
NETSCOUT Systems, Inc.
Westford, MA 01886-4105
TEL：+1 978-614-4000
www.netscout.com

アーバーネットワークス株式会社
101-0063　東京都千代田区神田淡路町2-105
ワテラスアネックス13階
TEL：03-3525-8040
EMAIL：japan@arbor.net
WEB：jp.arbornetworks.com

NETSCOUTは、世界32カ国以上の国々で製品、サポート、サービスを提供しています。各国の事業拠点所在地、電話番号などのお問い合わせ先は、NETSCOUTのWebサイトでご参照ください。
www.netscout.com/company/contact-us

SECPDS_004_JP-1804 12/2018