



ハイライト

- IBM® X-Force® の研究成果を製品に反映することにより、ゼロデイ攻撃の脅威に対する保護およびセキュリティ・インテリジェンスを提供
- 暗号化トラフィックなどのネットワーク・アクティビティに対する重要な洞察と可視性を提供
- IBM QRadar® SecurityIntelligence Platform との統合
- Web ベースと Web ベースでないアプリケーションの双方に対する、ユーザーおよびグループによるきめ細かい制御を実現
- 統合によりコストおよび複雑性を削減し、さらに帯域幅消費も削減

IBM Security Network Protection

統合化されたセキュリティ、可視性、および制御を提供し、次世代のネットワーク保護を実現

IBM Security Network Protection は、脅威防御、可視性、制御の機能を独自に組み合わせることで、ビジネスに欠くことのできないネットワーク・インフラストラクチャーを保護することを目的として設計されています。IBM は、ネットワーク上での包括的なセキュリティ、可視性、および制御を実現するためにセキュリティ・ネットワークの専門家が利用できる次世代ソリューションを提供することで、従来の侵入防御システムの機能を拡張しました。IBM Security Network Protection は、ポイント・ソリューションを拡張可能な単一のネットワーク・セキュリティ・プラットフォームに統合することによって、コストを削減し、複雑性を軽減します。また、あまり重要でない、帯域を逼迫するアクティビティを制御し、除去することで、お客様は、インフラストラクチャー内のコストをさらに節減することができます。

今日のセキュリティ事情を考慮すると、セキュリティの脅威に対応できる、さらに高度なセキュリティ手法を必要とする一方で、管理の複雑性の軽減、管理コストの削減も最優先事項です。IBM Security Network Protection は、これらすべての目的を達成するためにお客様を支援する、統合ソリューションです。このソリューションは、いくつかの高度な機能を組み合わせることによって、脅威防御、ネットワーク・アクティビティに対する重要な洞察、アプリケーションのきめ細かい制御を可能とし、新しいレベルで統合され、簡素化されたセキュリティを確立します。

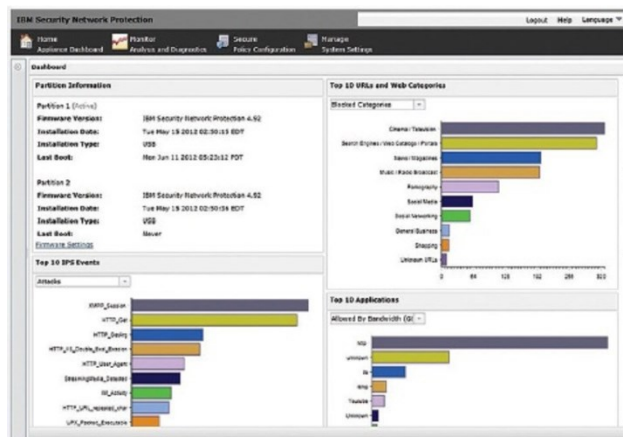


進化する脅威に対する保護

セキュリティの脅威は、ますます進化しています。先進の Web アプリケーションとファイル共有の急増によって、これまで安全性に問題はないと思われていたアクティビティが攻撃者の標的になる可能性があります。アンチマルウェア・ソフトウェアやファイアウォールなど、従来のセキュリティ手法は、容易に迂回できるようになっています。生産性やデータ・セキュリティ、コンプライアンスを確保するには、より高度でプロアクティブな脅威防御が不可欠です。つまり、Web アプリケーションの保護、埋め込みシェル・コードの脅威の検出機能、および、その他の多くの高度な機能により、新たな脅威に対する包括的なセキュリティを提供するということがです。X-Force 研究開発チームによって設計および更新された IBM Protocol Analysis Module (PAM: プロトコル解析モジュール) は、IBM Security Network Protection アプライアンスの重要な要素です。X-Force チームは GTOC (Global Threat Operations Center) からインターネットの脅威レベルを追跡しており、世界で最も包括的な脅威に関するデータベースを作成しています。セキュリティ担当者が新しい脅威に対して常に先手を打って対処できるように、PAM には、コンテンツとセキュリティの更新が継続的に組み込まれます。PAM と X-Force データベースを組み合わせることで、ゼロデイ攻撃に対して、より強固な防御を実現するとともに、マルウェア、ボットネット、ピアツーピア・アクティビティといった幅広いセキュリティ・リスクを正確に識別できます。

重要な洞察と可視化

主要な複数のセキュリティ機能を組み合わせることによって、IBM Security Network Protection は、基本的な脅威に対する保護だけでなく、現在使用中のアプリケーション、アクセス中の Web サイト、アクセスしているユーザーなど、ネットワーク・アクティビティに対する重要な洞察と可視化を可能とします。セキュリティを維持するためには、使用中のアプリケーション、企業内ネットワークからアクセスしている Web サイトの種類など、ネットワーク上で現在何が起きているかを正確に把握する必要があります。これらのアクティビティは攻撃の機会を生み出す可能性があり、そうした機会はデータの損失、企業ポリシーの違反、コンプライアンスの問題を引き起こす可能性があります。IBM Security Network Protection は、帯域幅使用量を可視化することで、大量の帯域幅とリソースを消費している、業務上重要でないアクティビティを識別することもできます。



IBM Security Network Protection ダッシュボードにより、ユーザーやグループによる Web やアプリケーションの使用といった、ネットワーク上のトラフィックの性質をすぐに確認できます。

ネットワーク・アクティビティのきめ細かい制御

IBM Security Network Protection には、高度な脅威防御とネットワークの可視性の構築に加えて、よりきめ細かい制御機能が備わっています。ユーザーはこの機能を使用して、ネットワークに関して新たに得た洞察に基づいて行動することができます。これらの機能は、潜在的な攻撃経路および脅威に対する脆弱性を削減するために設計され、一般的に攻撃に使用される手段（ソーシャル・メディア・サイトなど）をきめ細かく制御し、スパイ・フィッシングなど新しく登場した攻撃や、ユーザーを標的としたその他の高度な脅威を防ぎます。きめ細かい制御ポリシーが作成できるため、全体的なリスクが削減され、業務上重要でないネットワークの使用に関連した帯域幅コストが削減されます。IBM Security Network Protection は、対応可能なアプリケーションの範囲を最大限に拡大するため、2,000 を超えるアプリケーションおよび個別アクションをサポートし、200 億件を超える URL のデータベースを活用します。精度を常に最高レベルに保つために、IBM Web クローリング・テクノロジーにより URL が継続的にカテゴリー化され、変更があれば再カテゴリー化されます。これにより、IBM Security Network Protection アプライアンスは常に更新され、使用ポリシーの効率の最大化および最新のインターネット上の脅威からの保護が実現されます。



IBM Security Network Protection XGS 5100 アプライアンスには、最大 2 つのネットワーク・インターフェース・モジュールを構成できます。

シームレスなデプロイメントと統合

IBM Security Network Protection は、幅広い種類の環境にシームレスに実装可能です。この製品ファミリーには、交換可能なネットワーク・インターフェース・モジュール (NIM) などの柔軟な機能が含まれており、時間とともに変化するさまざまなネットワーク標準や構成をサポートします。また、柔軟なパフォーマンスのライセンス交付によってライセンス・アップグレードをシンプルに実行することで、ハードウェアを変更しなくてもパフォーマンスのアップグレードが可能です。事前構成済みの X-Force デフォルト・セキュリティ・ポリシーにより、即時のセキュリティ保護を追加設定なしで利用できます。また、IBM Security SiteProtector™ System を使用して、多数のサイトにアプライアンスを速やかに展開し、中央で管理することができます。IBM Threat Protection System の一部として、IBM Security Network Protection は IBM QRadar Security Intelligence Platform と密接に統合されています。例えば IBM Security Network Protection アプライアンスは、フロー・データを標準の IPFIX (Internet Protocol Flow Information Export) データ形式で送信し、より高度な分析と関連付けのためにデータ・フィードを常時提供します。IBM Security Network Protection アプライアンスはまた、QRadar SIEM によってセキュリティ・リスクが検出された際、トラフィックをブロックすることができる検疫コマンドを受信できます。これにより、QRadar ユーザーは、セキュリティの脅威が検出された場合に即時に対応できます。

IBM が選ばれる理由

IBM Security Network Protection は、ネットワーク・セキュリティに対してよりスマートなアプローチを採用することにより、次世代の侵入防御システム機能を提供し、進化するセキュリティの脅威に対して高度な防御を実現します。IBM Threat Protection System の一部である IBM Security Network Protection は、攻撃を防ぐための主要なコンポーネントです。管理者はセキュリティを大幅に強化でき、それと同時にネットワークにさらなる可視性がもたらされ、ネットワークをよりきめ細かく制御できるようになるため、帯域幅効率の向上およびコストの削減が可能になります。このソリューションは、IBM X-Force の脅威に関するデータベースと膨大な数の URL

データベースを活用して、新たな脅威に対する最新のプリエンブティブな防御を確保します。IBM Security Network Protection は、複数の主要なセキュリティ機能を単一のオフリングに統合することによって、今日直面する課題に、包括的でコスト効率に優れた回答を提示します。

IBM Security Network Protection アプライアンスの概要				
	XGS 3100	XGS 4100	XGS 5100	XGS 7100
パフォーマンスの特性*				
スループット	最大 800 Mbps	最大 1.5 Gbps	最大 7 Gbps	最大 20 Gbps
フレキシブル・パフォーマンス・レベル (FPL)	最大 400 Mbps (FPL 1) 最大 800 Mbps (FPL 2)	最大 750 Mbps (FPL 1) 最大 1.5 Gbps (FPL 2)	最大 2.5 Gbps (FPL 1) 最大 4 Gbps (FPL 2) 最大 5.5 Gbps (FPL 3) 最大 7 Gbps (FPL 4)	最大 5 Gbps (FPL 1) 最大 10 Gbps (FPL 2) 最大 15 Gbps (FPL 3) 最大 20 Gbps (FPL 4)
SSL スループット (インバウンド)	最大 500 Mbps	最大 900 Mbps	最大 4.5 Gbps	最大 12 Gbps
SSL スループット (アウトバウンド)	最大 400 Mbps	最大 700 Mbps	最大 2.5 Gbps	最大 7.5 Gbps
最大スループット (UDP)	3.5 Gbps	10 Gbps	15 Gbps	45 Gbps
平均遅延時間	150 μs 未満	75 μs 未満	75 μs 未満	75 μs 未満
新規接続数 (1 秒あたり) (HTTP)	10,000	15,000	75,000	225,000
同時接続セッション数 (HTTP)	500,000	1,000,000	2,200,000	15,000,000
物理特性				
筐体サイズ	1U	1U	1U	2U
高さ	44.2 mm	44.2 mm	44.2 mm	88.4 mm
幅 (ラック)	430 mm	430 mm	430 mm	430 mm
奥行き (ラック)	540 mm	540 mm	540 mm	570 mm
重量	8.62 kg	9.36 kg	11.58 kg	18.0 kg
ラック・マウント・レール	スライド式角穴ポストをサポート			
管理インターフェース	2 x 1GbE、RJ-45 (IPv6 をサポート)			
固定モニター・インターフェース	4 x 1GbE、RJ-45 (バイパス内蔵)			利用不可
最大モニター・インターフェース (1GbE)	4	最大 12	最大 20	最大 32
最大モニター・インターフェース (10GbE)	利用不可	最大 2	最大 4	最大 8
サポート対象の物理メディア・タイプ	10/100/1000 RJ-45	10/100/1000 RJ-45 copper、1G fiber (SX/L X)、10G fiber (SR/LR)、1G SFP、10G SFP+	10/100/1000 RJ-45 copper、1G fiber (SX/L X)、10G fiber (SR/LR)、1G SFP、10G SFP+	10/100/1000 RJ-45 copper、1G fiber (SX/L X)、10G fiber (SR/LR)、1G SFP、10G SFP+
サポートされるネットワーク・インターフェース・モジュール (NIM) の数	利用不可	1	2	4
バイパス内蔵のネットワーク・インターフェース・モジュール (NIM)	利用不可	8 x 1GbE TX (100/1000) 4 x 1GbE SX 4 x 1GbE LX 2 x 10GbE SR 2 x 10GbE LR	8 x 1GbE TX (100/1000) 4 x 1GbE SX 4 x 1GbE LX 2 x 10GbE SR 2 x 10GbE LR	8 x 1GbE TX (100/1000) 4 x 1GbE SX 4 x 1GbE LX 2 x 10GbE SR 2 x 10GbE LR
ネットワーク・インターフェース・モジュール (NIM)、外付けバイパス (オプション)	利用不可	4 x 1GbE SFP 2 x 10GbE SFP+	4 x 1GbE SFP 2 x 10GbE SFP+	4 x 1GbE SFP 2 x 10GbE SFP+
予備電源機構	オプション	オプション	標準装備	標準装備
ストレージ・タイプ	HDD	MLC-SSD	EMLC-SSD	EMLC-SSD
高可用性サポート	アクティブ/アクティブおよびアクティブ/パッシブの環境をサポート			
電気および環境のパラメーター				
AC 入力要件	460 W (100 – 127 V @ 5.6A/200 – 240 V @ 2.8A)			
平均消費電力	62 W	81 W	194 W	360W
作動温度/相対湿度	0°C – 40°C/5% – 85% @ 40°C			
安全性認証基準	UL 60950-1、CAN/CSA C22.2 no. 60950-1、EN 60950-1 (CE Mark)、IEC 60950-1、GB4943、GOST、UL-AR			
EMC 認証基準	FCC Class A、Industry Canada Class A、AS/NZS CISPR 22 Class A、EN 55022 Class A (CE Mark)、EN 61000-3-2 (CE Mark)、EN 61000-3-3 (CE Mark)、EN 55024 (CE Mark)、VCCI Class A、KCC Class A、GOST Class A、GB9254 Class A、GB17625.1			
環境基準	特定有害物質使用制限 (RoHS)			

詳細情報

このオフラインの詳細については、IBM の営業担当員またはビジネス・パートナーにお問い合わせいただくか、次の Web サイトをご覧ください。 ibm.com/security/jp

* IBM Security Network Protection で引用されたパフォーマンス・データは、通常、使用時のトラフィックを反映するために、混合 TCP/UDP トラフィックでのテストに基づいています。プロトコル混合および平均パケット・サイズなどの環境要因は、ネットワークごとに異なります。また、測定されるパフォーマンス結果もそれに伴って変化します。IBM Security Network Protection のスループットは、未圧縮の混合プロトコル・トラフィックをこのアプライアンス経由で送信して、パケット損失なしで達成されたスループットを測定して決定しています。ベンチマーク・テストでは、「Trust X-Force」ポリシーを使用したデフォルトのインライン保護モードで入力されたフル装備のネットワーク・インターフェース・モジュールを使用して、XGS シリーズのアプライアンスを Drop Unanalyzed モードで実装しました。ファームウェア v4.03 以降を実行している Spirent Avalanche および Spirent TestCenter テスト機器を使用。トラフィック混合の比率: HTTP=69%、HTTPS=20%、SMTP=5%、FTP=5%、DNS=1%。ここで HTTP/HTTPS トラフィックは未圧縮で、標準の HTTP/S 1.1 GET 要求で 44 Kb オブジェクトを使用。オブジェクト転送を伴わない単純な SMTP 接続、15,000 バイト/2 ミリ秒でバースト転送する FTP GET 要求、および DNS 標準の A レコード・ルックアップを使用。SSL 検査レートは、SSL Decryption Policy を有効にして計測しました。最大スループットは 1518 バイト・フレーム・サイズの UDP トラフィックを使用して生成されました。



© Copyright IBM Corporation 2014

日本アイ・ビー・エム株式会社
〒103-8510 東京都中央区日本橋箱崎町 19 番 21 号

Produced in Japan
October 2014

IBM、IBM ロゴおよび ibm.com は、世界の多くの国で登録された International Business Machines Corporation の商標です。他の製品名およびサービス名等は、それぞれ IBM または各社の商標である場合があります。現時点での IBM の商標リストについては、ibm.com/legal/copytrade.shtml をご覧ください。

本書の情報は最初の発行日の時点で得られるものであり、予告なしに変更される場合があります。すべての製品が、IBM が営業を行っているすべての国において利用可能なものではありません。

本書に含まれるパフォーマンス・データは、特定の動作および環境条件下で得られたものです。実際の結果は、異なる可能性があります。

IBM 以外の製品とプログラムの操作またはサービスの評価および検証は、お客様の責任で行っていただきます。

本書に掲載されている情報は特定物として現存するままの状態提供され、第三者の権利の不侵害の保証、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任なしで提供されています。IBM 製品は、IBM 所定の契約書の条項に基づき保証されます。



Please Recycle