データシート

Content Analysis S200/S400/S500

概要

- エンタープライズクラスのマルウェアふるまい分析
- ユニークなデュアル検出アプローチにより、疑わしいファイルと URL をすばやく分析。実行されているマルウェアのすべてのふるまいを検出し、ゼロデイの脅威や未知のマルウェアの存在を検出
- アプライアンスの削減と複雑さの低減により ROI を向上
- 4 年または 5 年のサービス契約で投資を保護
- 革新的な多層型アプローチによる保護
- シマンテックのソリューションとの統合
- セキュリティとパフォーマンスのトレードオフが不要

自動化された高度な脅威防止機能により、ゲートウェイで脅威を阻止、検出、分析

企業は、ますます巧妙化する攻撃に対して脆弱になっています。脅威にさらされる可能性が高まっている今、攻撃を阻止するだけでなく、攻撃の検出と分析、攻撃への対応をより効果的に実行できる新しい防御が必要です。

Symantec Content Analysis は、既知の攻撃、未知の攻撃、標的型攻撃を強力に防御する包括的なセキュリティアプローチを採用しています。Symantec ProxySG™ または Symantec Messaging Gateway を統合した多層型のアプローチにより、Web とメールの脅威を防御します。また、シマンテックと他の主要セキュリティベンダー両方の製品を活用することで、ホワイトリストサービス、ファイルレピュテーションサービス、デュアル型マルウェア対策エンジンを提供し、静的コード分析と動的分析（オンボックス型サンドボックス）を実行します。このようにコンテンツ分析とマルウェア分析を統合することで、標的型攻撃に適切に対応するマルウェア防御機能が実現します。

企業は、ユーザーがマルウェア対策ソフトウェアをデスクトップ上で実行してないときでも、ウイルス、トロイの木馬、ワーム、スパイウェアなど、さまざまな悪質なコンテンツから保護されます。

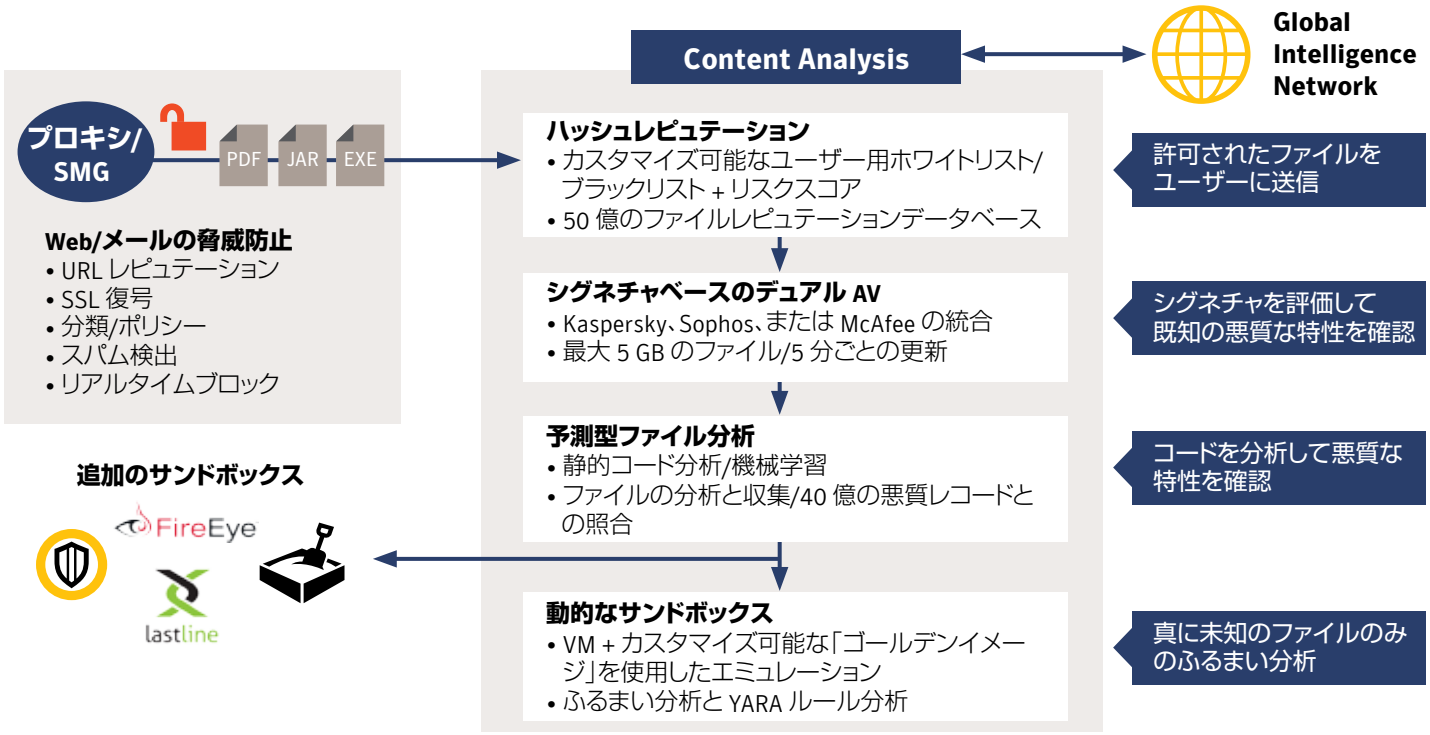
インライン型脅威分析

サイロ化された単一目的の防御ツールによる検出を回避するために、高度な攻撃はさまざまな形で行われます。したがって、単一の技術だけですべての脅威を阻止することはできません。Content Analysis は、異なるアプローチを採用することにより、多層的かつ複数ベンダーに対応した脅威の検出と阻止を実現する単一のプラットフォームを提供します。具体的には、ProxySG および Symantec Messaging Gateway と連携することで、以下の機能を実行します。

- 既知の悪質な URL をゲートウェイで阻止
- 広範なホワイトリストとブラックリストをスキャン
- デュアル型マルウェア対策エンジンでコンテンツをスキャンして、検出精度を向上
- 高度な静的コードファイル分析により、未知のファイルを分析
- オンボックス型または専用のサンドボックスで未知のファイルを実行してふるまい分析
- Symantec Endpoint Protection など、さまざまなセキュリティツールを統合することで、エンドポイントの可視性を確保し、保護および対応を実行

Symantec

Content Analysis の多層型脅威防御



Content Analysis のアーキテクチャのおかげで、シマンテックは他の技術ベンダーと連携して保護を強化できます。シマンテック、Kaspersky™、Sophos™、McAfee® の主要なマルウェアエンジンがサポートされ、分単位で更新が行われるため、デスクトップ向けマルウェア対策製品よりも効果的な防御が実現します。また、最大 2 つのマルウェア対策エンジンを同時に利用して、検出と防御を強化できます。脅威検出エンジンには、以下の機能が搭載されています。

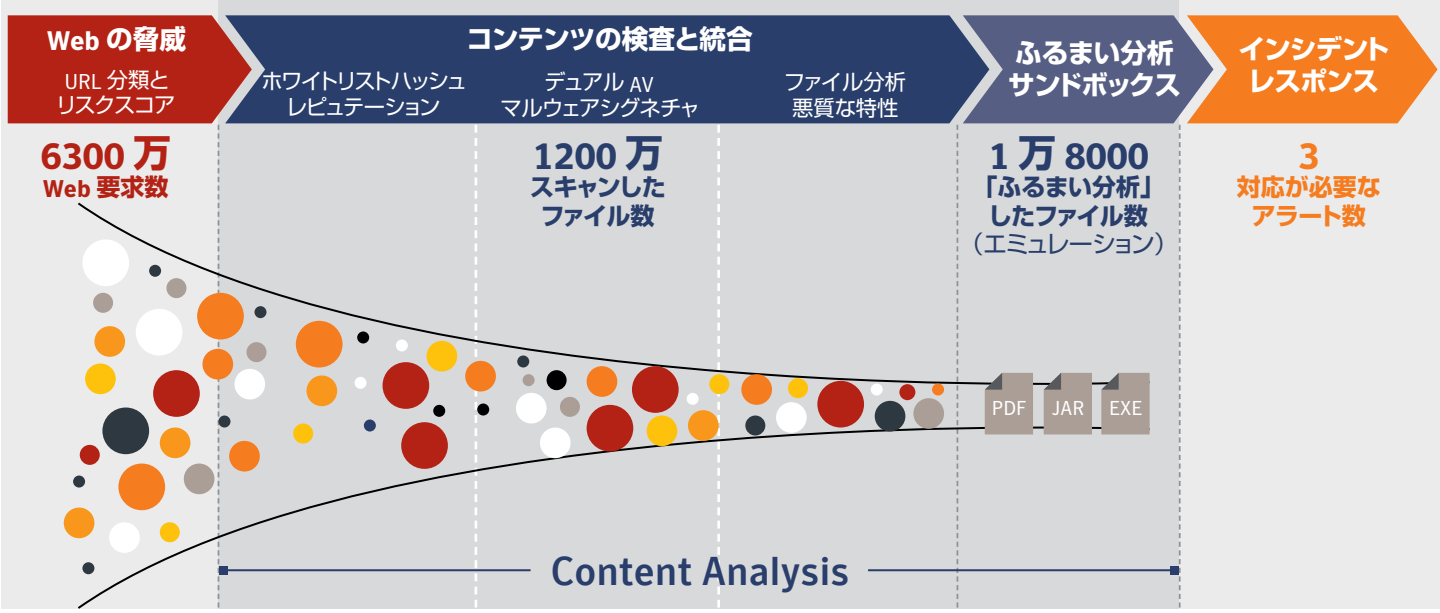
- チェックサムシグネチャによる既知の脅威との照合
- コマンドやコンテンツのふるまい分析による事前対応型の検出
- スクリプトや実行ファイルの詳細分析に適したエミュレーションモード

トラフィック分析では、受信トラフィックと送信トラフィックの両方を分析対象に設定でき、タイムアウト時間の設定、検出エラー発生時のファイル削除、リアルタイムのサンドボックス作成による初期感染の阻止、信頼できるサイトの定義などの各種オプションを利用できます。ポリシーの許可/拒否リストでは、拡張子やファイルサイズ、コンテンツタイプによる制限を設定できます。また、アラートやログファイルのカスタマイズも可能です。

高度な脅威に効果的に対抗

Content Analysis は、複数のソースから得た脅威インテリジェンスを活用して、標的型攻撃を阻止するとともに、主要なプロキシアーキテクチャと連携して、悪質な Web セッションをブロックします。また、トラフィックを複数の段階で検査およびフィルタリングし、マルウェアが企業に侵入するのを阻止します。高速なネットワークであっても、より多くの攻撃を検出して阻止でき、脅威分析の負担が軽減され、誤検知が減少します。強力な保護を実現するために欠かせない、多層化された統合技術を提供しているのはシマンテックだけです。

高度な脅威に効果的に対抗



多層型の脅威分析と脅威検出により、従来よりも多くの脅威が発見、阻止される一方で、詳細なサンドボックス分析を必要とするファイルの数は減少します。その結果、対応が必要なインシデントの数が削減されます（上の例は、ある実際のお客様の 1 日の Web トラフィックの処理結果です）。

	CAS S200-A1	CAS S400-A1	CAS S400-A2	CAS S400-A3	CAS S400-A4	CAS S500-A1
パフォーマンス						
スループット	25 Mbps	50 Mbps	100 Mbps	250 Mbps	500 Mbps	1000 Mbps
システム						
ディスクドライブ	500 GB（1 x 500 GB）	1 TB（2 x 500 GB）	1 TB（2 x 500 GB）	1 TB（2 x 500 GB）	1 TB（2 x 500 GB）	6 x 1 TB
RAM	6 GB	16 GB	16 GB	32 GB	32 GB	128 GB
オンボードポート	2 x 1000Base-T カッパーポート（バイパス付き） 2 x 1000Base-T カッパーポート（バイパスなし） 1 x 1000Base-T カッパー、システム管理ポート 1 x 1000Base-T カッパー、BMC 管理ポート	2 x 1000Base-T カッパーポート（バイパス付き） 1 x 1000Base-T カッパーポート（ICAP） 1 x 1000Base-T カッパー、システム管理ポート 1 x 1000Base-T カッパー、BMC 管理ポート				2 x 10GBase-T カッパーポート（バイパスなし） 1 x 1000Base-T カッパー、システム管理ポート 1 x 1000Base-T カッパー、BMC 管理ポート
オプション NIC	4 x 10/100/1000Base-T（カッパー、バイパス対応） 4 x 1GbE Fiber-SR（バイパス対応、フルハイトスロットのみ）	4 x 10/100/1000Base-T（カッパー、バイパス対応） 4 x 1GbE Fiber-SR（バイパス対応、フルハイトスロットのみ） 2 x 10Gb Base-T（カッパー、バイパス対応） 2 x 10Gb Base-T（カッパー、バイパス非対応） 2 x 10Gb Fiber（SR、バイパス対応） 2 x 10Gb Fiber（LR、バイパス対応）				
利用可能なスロット数	1 x フルハイト	1 x フルハイト/1 x ハーフハイト				2 x フルハイト/ 4 x ハーフハイト
電源	1	2				2

モデル	CA S200	CA S400	CA S500
寸法と重量			
寸法 （長さ x 幅 x 高さ）	446.3 x 440.0 x 43.5（mm）（筐体部分のみ） 454.5 x 482.6 x 43.5（mm）（筐体 + 拡張部分） 注: オプションのスライドレールを取り付けた場合の幅は 640 mm	572 x 432.5 x 42.9（mm） （筐体部分のみ） 643 x 485.4 x 42.9（mm） （筐体 + 拡張部分）	710 x 433.3 x 87.2（mm） （筐体部分のみ） 812.8 x 433.4 x 87.2（mm） （筐体 + 拡張部分）
フォームファクタ	1 RU の高さ	1 RU の高さ	2 RU の高さ
重量（最大）	約7.4 kg +/- 5%	約12.8 kg +/- 5%	約30 kg +/- 5%
稼働環境			
AC 電源	100-127 V (6 A) 200-240 V (3 A), 47-63 Hz	デュアル冗長ホットスワップ対応電源、 100-127 V (8 A) 200-240V (4 A), 47-63 Hz	デュアル冗長ホットスワップ対応電源、 100-240 V, 50-60 Hz, 12-5 A
最大消費電力	350 ワット	450 ワット	1100 ワット
発熱量	通常時: 785 BTU/時、最大: 1195 BTU/時	通常時: 1086 BTU/時、最大: 1381 BTU/時	通常時: 2598.42 BTU/時、最大: 3751 BTU/時
オプションの DC 電源	利用不可	入力電圧範囲: 40.5 - 57 V 入力最大電流: 22 A 合計出力電力: 770 ワット	入力電圧範囲: 40 - 72 V 入力最大電流: 30 A 合計出力電力: 1100 ワット
温度	5˚ C から 40˚ C（海抜 0 m）		
湿度	相対湿度 20% から 80%、結露しないこと		
高度	最大 3048 m		

すべての Content Analysis モデル		
法規制	**安全基準**	**電磁適合性（EMC）**
国際	CB – IEC60950-1, Second Edition	CISPR22, Class A、CISPR24
米国	NRTL – UL60950-1, Second Edition	FCC part 15, Class A
カナダ	SCC – CSA-22.2, No.60950-1, Second Edition	ICES-003, Class A
欧州連合（CE）	CE – EN60950-1, Second Edition	EN55022, Class A、EN55024、EN61000-3-2、EN61000-3-3
日本	---	VCCI V-3, Class A
メキシコ	NOM-019-SCFI by NRTL Declaration	---
アルゼンチン	S Mark – IEC 60950-1	---
台湾	BSMI – CNS-14336-1	BSMI – CNS13438, Class A
中国	CCC – GB4943.1	CCC – GB9254、GB17625
オーストラリア/ニュージーランド	AS/NZS 60950-1, Second Edition	AS/ZNS-CISPR22
韓国	---	KC – RRA, Class A
ロシア	TP TC 004/2011	TP TC 020/2011
環境	RoHS-Directive 2011/65/EU、REACH-Regulation No 1907/2006	
製品保証	出荷日から 1 年間有効で譲渡不可のハードウェア限定保証。 BlueTouch サポート契約では、24 時間 365 日対応のソフトウェアサポートを提供。さらに、ハードウェアサポートのオプションを用意。	
政府機関の認定	政府機関の認定について詳しくは、Federal_Certifications@bluecoat.com までお問い合わせください	
詳細	法規制遵守の認定に関する質問やサポートについては、regulatoryinfo@bluecoat.com までお問い合わせください。	

シマンテックについて

シマンテックコーポレーション（NASDAQ: SYMC）はサイバーセキュリティ業界をリードする世界的企業です。さまざまな場所に保管されている大切なデータを守るため、企業や政府機関、個人のお客様を支援しています。エンドポイントからクラウド、インフラまでを高度な攻撃から守るため、世界中の企業がシマンテックの戦略的統合ソリューションを選択しています。また、世界中で 5 千万以上の個人やご家庭が、自宅などで使用するデバイスそしてデジタルライフを守るために、ノートンと LifeLock 社の製品を使用しています。シマンテックのサイバーインテリジェンスネットワークは民間が運営するネットワークとしては世界最大規模を誇ります。このネットワークが、先進的な脅威をいち早く発見し、お客様を守ります。詳しくは www.symantec.com/ja/jp/ をご覧ください。

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