

Soliton®


ForeScout

CounterACT

エージェントレス型検疫／ワーム・不正アクセス防御
カウンターアクト



ForeScout

CounterACT

手軽な導入で、ポリシー違反PCを検知・修正
ワーム感染によるネットワークダウンを防止

不正接続PCの検知、通信制御から ポリシー違反PCの修正までを手軽に実現

不正なPCが簡単に接続できると、ネットワークは様々な脅威にさらされます。
CounterACTなら、最小限のネットワーク変更で、検疫を実現できます。

不正接続PCの検知や接続デバイスの精査

MACアドレスリストとの照合やWindowsドメインログオン有無などを条件に、不正接続PCを検知します。ルーターを超えた別のセグメントのPCのMACアドレスを取得する機能により、ネットワーク構成によってはCounterACT 1台で全ネットワークの不正接続PC検知が可能です。MACアドレスリストの自動生成や外部FTPサーバーを定期的に参照してMACアドレスリストを自動更新することも可能です。また、通信を監視したデバイスの種別(スマートフォン、PC、プリンター、ネットワーク機器など)を識別できるため、適切な対策が実施できます。

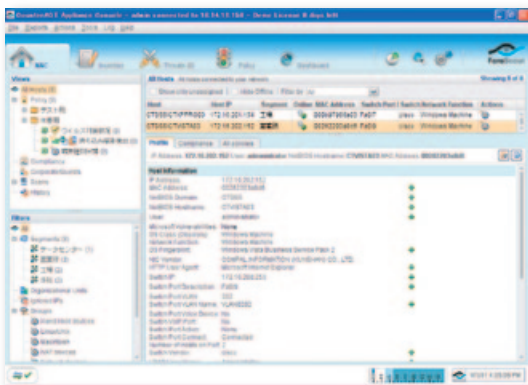
エージェント不要のポリシーチェック(検疫)

Windowsの管理者アカウントを利用するエージェントレス方式でポリシーチェックを行うことができます。エージェントを配布する必要が無いので、既存システムに影響を与えることなく簡単に導入できます。またバックグラウンドでチェック・修正することで、ユーザーの手を煩わせることのない運用が可能です。

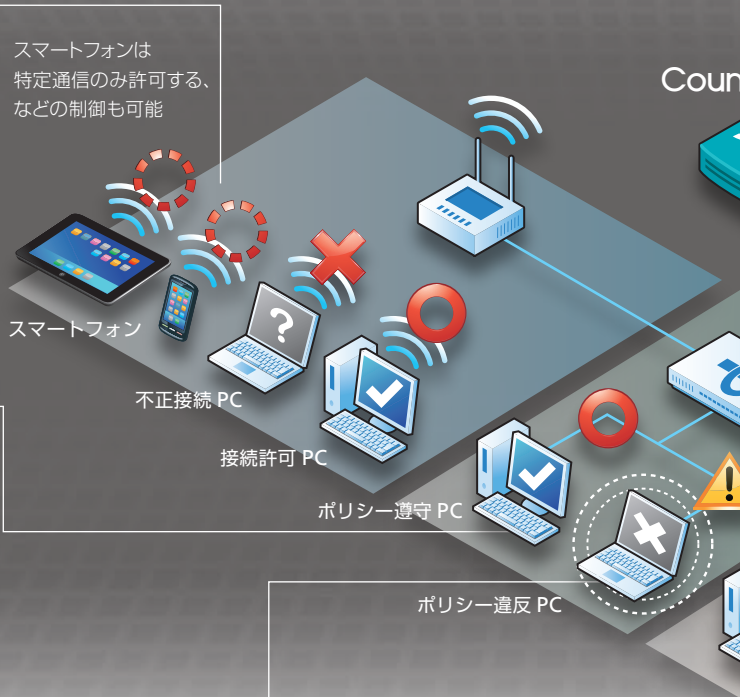
Windows、Mac、Linuxに対応したエージェントを利用すれば、持ち込みPCに対するチェック・修正も実施できます。様々なPCが接続される環境でも、ポリシーチェックを徹底することが可能です。

業務への影響を最小限にしつつ 違反を修正、セキュリティ強度を向上

カスタマイズ可能なWebメッセージ、指定IPアドレス宛通信のみのブロック、Webアクセス禁止や除外URL設定、修正アクション開始までのタイマー設定など、柔軟に検疫強度を調整できます。



CounterACT Console



ポリシーチェックの設定

トリガー (いつチェックするか?)



1. 定期的にチェック
2. 新しい端末からの通信を検知した時にチェック(新規IPアドレス、MACアドレスからの通信監視など) など

コンディション (何をチェックするか?)



1. 接続許可端末かどうか
2. 端末種別 (Windows/Mac/Linux、スマートフォン、プリンター、スイッチ等)
3. OSバージョン、セキュリティパッチ適用状況
4. アンチウイルス稼働・パターン更新有無
5. 特定アプリケーションの稼働 など

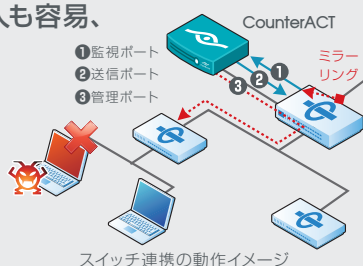
アクション (何を行うか?)



1. 端末にアラート・修復方法を通知
2. 強制的な修正 (ウイルスパターン更新、パッチ適用)
3. 特定通信を禁止 (TCP RST) や端末隔離 (スイッチ連携)
4. パッチスクリプトの実行 など

インライン型ではないので導入も容易、 万一の障害時も安心

インライン設置ではなく、スイッチのミラーポートからトラフィックを監視する仕組みなので設置が簡単です。障害発生時にもネットワークに影響を与えません。



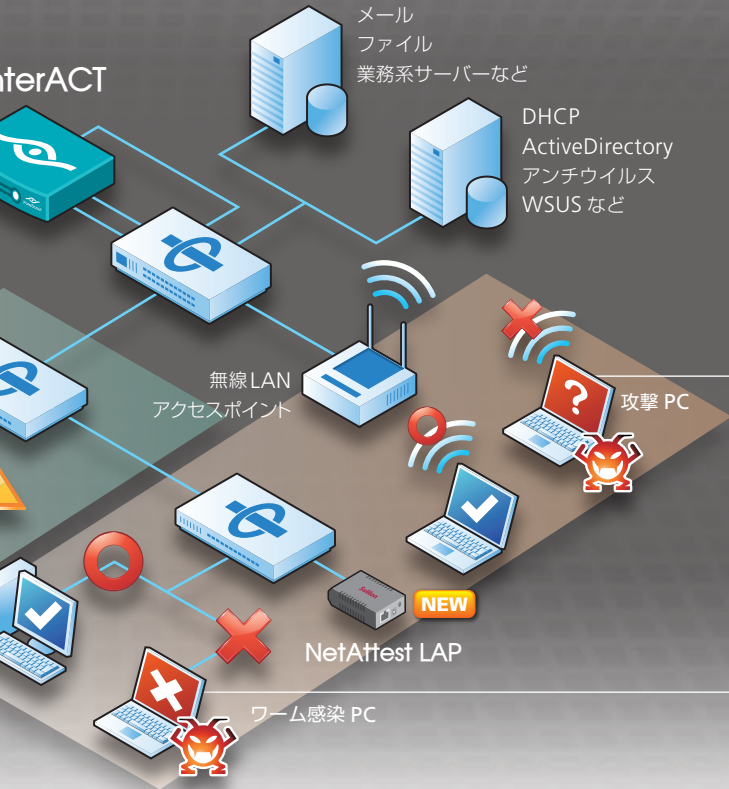
スイッチ連携の動作イメージ

ネットワークデバイスとの連携

NetAttest LAPと連携し、CounterACTが通信を監視できない端末の接続検知やブロックを実現できます。また、SNMPやTelnetなどで各種スイッチと連携し、通信を制御したり(ポートのリンクダウン、VLAN変更、ACL設定)、端末接続先スイッチのポート情報やARPテーブル参照を行い、ネットワークを可視化することができます。無線LANコントローラやVPNゲートウェイ等との連携も可能です。

パッチ適用では間に合わない未知の攻撃や ゼロデイワームの感染を検知、防御

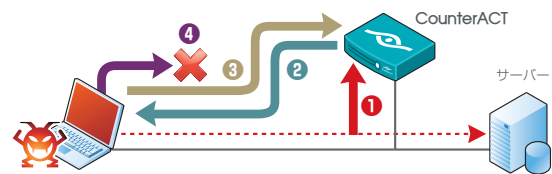
運用の手間をかけず、確実に攻撃だけを自動ブロック。
CounterACTなら、攻撃やワーム感染によるネットワークダウンを防止できます。



シグネチャ不要で新種の攻撃にも自動対応

シグネチャやパターンファイルに依存しない、独自の検知手法 (US Patent#6,363,489) により、新しい攻撃や新種のワームも即座に検知します。シグネチャの更新やチューニングなどの煩わしい作業は一切不要です。

- 1 不正なスキャン活動を検知
- 2 CounterACT がサーバーからの応答を擬装
- 3 擬装情報へのアクセスから該当 PC を攻撃者として検知
- 4 保護対象のサーバーや PC にアクセスすると攻撃セッション確立前にブロック



誤検知のない安全な自動防御

シグネチャ型ではないため、IPSで懸念される誤検知の心配はありません。擬装情報への通信確立という確実な証拠を根拠にするため、攻撃を検知したらすぐにアクションを起こす自動防御設定を行っても、安心してご利用いただけます。

攻撃通信のブロック・感染スピードの抑制

攻撃通信のブロック (TCP RSTでの通信制御、スイッチ連携での端末隔離など) のほか、ワーム感染スピードの抑制、メールワーム検知も可能。攻撃端末への Web メッセージだけではなく、さまざまな対応アクションが可能です。

知らないうちに攻撃されている？ 「ゼロディアタック」とは

脆弱性が発見され、セキュリティパッチが提供されるまでの間に行なわれる攻撃をゼロディアタックと呼びます。アンチウイルスやシグネチャ型 IPS を導入していても、パターンやシグネチャが作成されるまでは、ネットワークは無防備なままです。

シグネチャ方式では無防備期間が発生！



CounterACTならゼロディアタックにも対応可能！



CounterACT Edgeとの組み合わせで ネットワークをトータルに保護

内部ネットワークではなく、インターネットとの境界を保護するのが CounterACT Edge です。どの地域から攻撃を受けているかを世界地図上に可視化するなど、セキュリティを高めるための情報も得られます。



不正接続端末の 検知・防止を強化



NetAttest LAP NEW

CounterACTと連携する小型アプリケーション (別売)。CounterACTの端末検知・ブロック範囲を広げることができます。

利用形態に応じて アラートを選べます

検疫や侵入検知の結果を知らせるアラートにはメール送信、Syslogへの出力、SNMPトラップなど数種類の方法から、環境に応じて選べます。

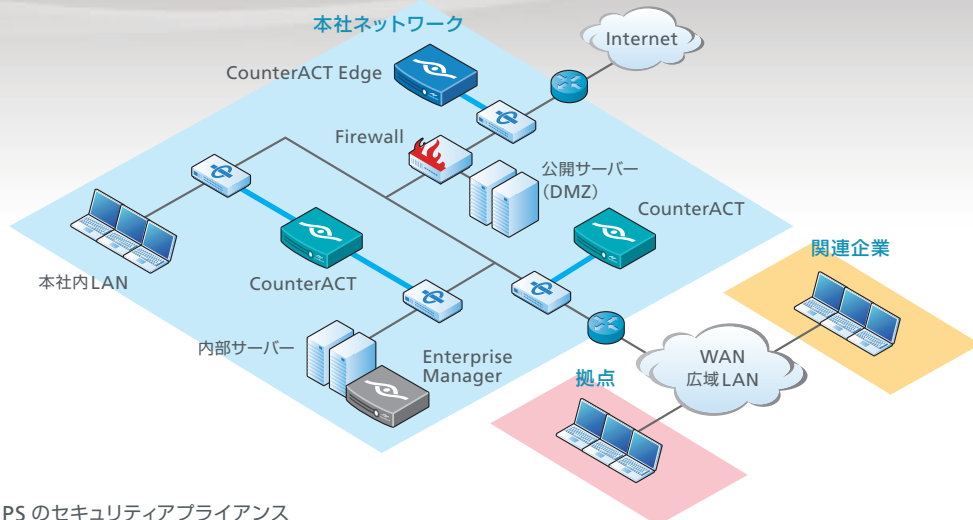
レポート機能で利用履歴も インシデント情報も一目瞭然

セキュリティ状態のチェックや社内の報告に活用できるレポート機能を搭載しています。見やすいレイアウトの PDF 形式のほか、加工が容易な CSV 形式でも出力できます。



導入例

CounterACT、CounterACT Edgeを社内に効果的に配置することで、様々なセキュリティ課題を解決します。Enterprise Managerを設置すれば、分散設置されたCounterACTを統合管理し、攻撃情報や検疫情報をCounterACT同士で共有できるようになり、より効果的なセキュリティ対策を実施できます。



CounterACT ■ エージェントレス検疫+IPSのセキュリティプライアンス

モデル	CT-100/A	CT-1000/A	CT-2000/A	CT-4000/A	CT-4000/AF10G
監視帯域	500Mbps	1Gbps	2Gbps	4Gbps	4Gbps
検疫対象ホスト数	500	1000	2500	4000	4000
連携対象デバイス数	25	50	100	200	200
ハードウェア					
筐体	19インチラック、1U			19インチラック、2U	
サイズ	43.2 (H) × 430 (W) × 665.5 (D) mm			87.30 (H) × 430 (W) × 704.8 (D) mm	
CPU	Dual-core Intel Xeon ×1	Quad-core Intel Xeon ×1		Quad-core Intel Xeon ×2	
ハードディスク	3 HDD (RAID1+HotSpare)				
ネットワークインターフェイス	10/100/1000Base-T ×6	10/100/1000Base-T ×8			10G Fiber ×2 10/100/1000Base-T ×6
重量	約25kg			約32kg	
電源	100-127/200-240VAC、50/60Hz				
消費電力	650W	650W (電源冗長化)		750W (電源冗長化)	
発熱量	2550 BTU/hour				
適合規格	VCCI Class A、FCC Class A、CE、UL、RoHS				

Enterprise Manager ■ 複数のCounterACTを統合管理するアプライアンス

モデル	CEM-05/A	CEM-10/A	CEM-25/A	CEM-50/A	CEM-100/A
管理するCounterACT数	5	10	25	50	100
ハードウェア					
筐体	19インチラック、1U			19インチラック、2U	
サイズ	43.2 (H) × 430 (W) × 665.5 (D) mm			87.30 (H) × 430 (W) × 704.8 (D) mm	
CPU	Quad-core Intel Xeon ×1				Quad-core Intel Xeon ×2
ハードディスク	3 HDD (RAID1+HotSpare)				
ネットワークインターフェイス	10/100/1000Base-T ×8				
重量	約25kg			約32kg	
電源	100-127/200-240VAC、50/60Hz				
消費電力	650W (電源冗長化)			750W (電源冗長化)	
発熱量	2550 BTU/hour				
適合規格	VCCI Class A、FCC Class A、CE、UL、RoHS				

※ CT-4000/AF10GのFiber NICは、10GBASE-SR (LCコネクタ) です。 ※ 同一ネットワークで2台以上のCounterACTを利用する場合は、CounterACT台数に応じたEnterprise Managerが必須です。
 ※ CounterACT Edgeのスペックはお問い合わせください。 ※ ハードウェアスペックは予告なく変更する場合がございます。

CounterACT Console システム要件

- CPU : Pentium3 1GHz以上
- メモリ : 512MB以上 (1GB以上推奨)
- ハードディスク : 100MB以上の空き容量
- NIC : 1ポート
- ドライブ : CD-ROM
- OS : Microsoft Windows 2000/XP/2003/Vista/2008/7

※ 記載の製品名は、各社の商標または登録商標です。

安全に関するご注意

正しく安全にお使いいただくために、ご使用前に必ず「取扱説明書」をお読みください。

販売元:

Soliton

株式会社ソリトンシステムズ

〒160-0022 東京都新宿区新宿2-4-3 TEL 03-5360-3811 FAX 03-3356-6354
<http://www.soliton.co.jp/> netsales@soliton.co.jp

大阪営業所 06-6821-6777 福岡営業所 092-263-0400 名古屋営業所 052-963-9700
 東北営業所 022-716-0766 札幌営業所 011-242-6111

開発元:

ForeScout

ForeScout Technologies, Inc.

<http://www.forescout.com/>

このカタログは、2011年9月現在のものです。仕様、デザインは予告なく変更することがあります。

FS-1109D