NitroSecurity, Inc.

Unifying 情報セキュリティ

企業の概要

NitroSecurity At-a-Glance

- 統合されたセキュリティマネジメント&侵入防止
- ポーツマス、NHのHQ； アイダホ・フォールズ、IDについてのR&D才能
- 2005年1月以来の130顧客

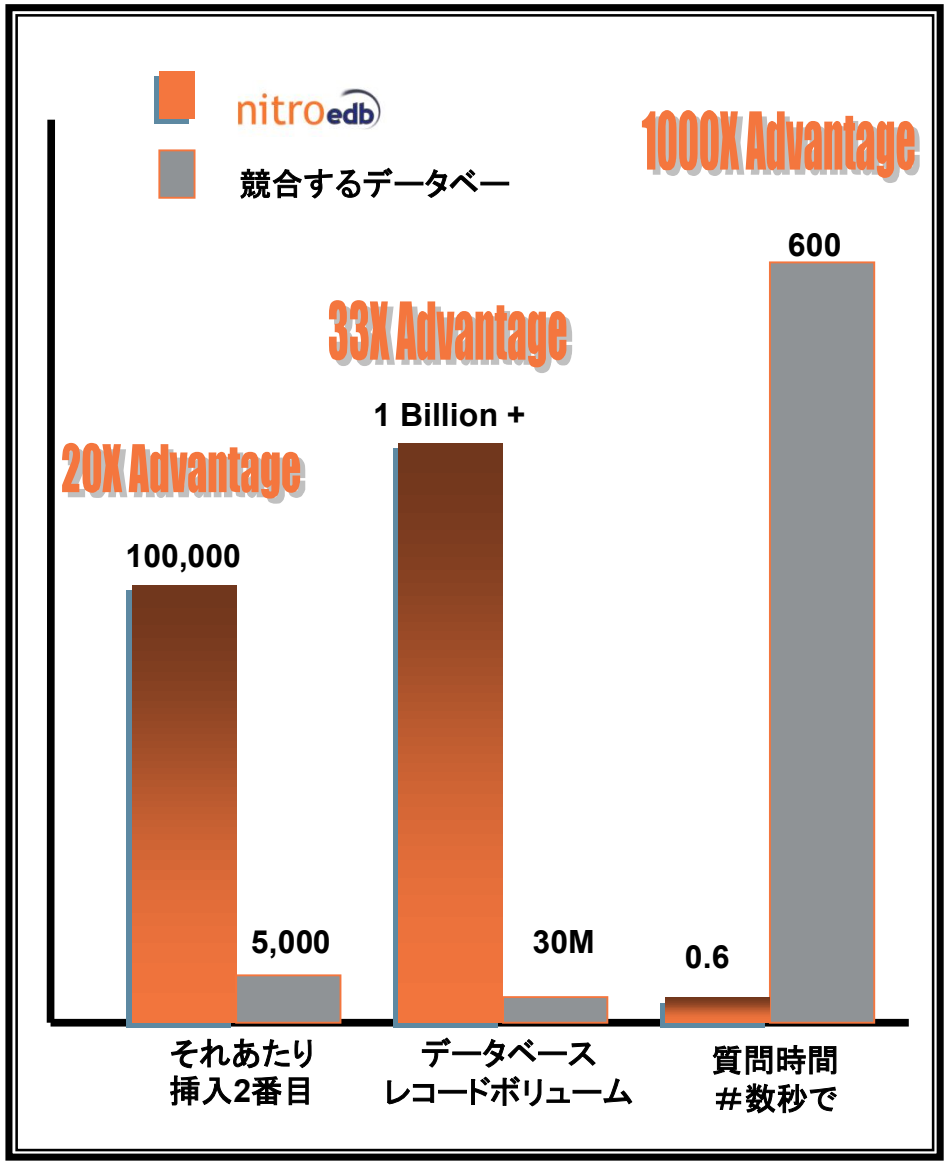
広い顧客ベース:複数の垂直線, SMB−フォーチュン500社

NitroSecurity:情報セキュリティを統合します

- 必須のネットワークセキュリティを統合することは単一の費用効果が高いシステムに機能します

  - ログ管理
  - セキュリティ情報&イベント管理（SIEM）
  - 行動分析（NBA）をネットワーク化してください
  - 変則検出（広告）
  - 侵入検出&防止（IPS）をネットワーク化してください

特許を取得した関係のデータ管理テクノロジー



Nitro EDB Logo

- 特許を取得した索引の付与テクノロジー
- 100人年を超える開発において
- 今日使用において現在のテクノロジーより速い時の100

- 真実の一体化セキュリティマネジメントをサポートするために必要なスピードで大量、マルチソース関係データ管理を使用可能にします

NitroSecurity 企業の歴史

中心的なテクノロジーに投資された100人年より多くにおいて

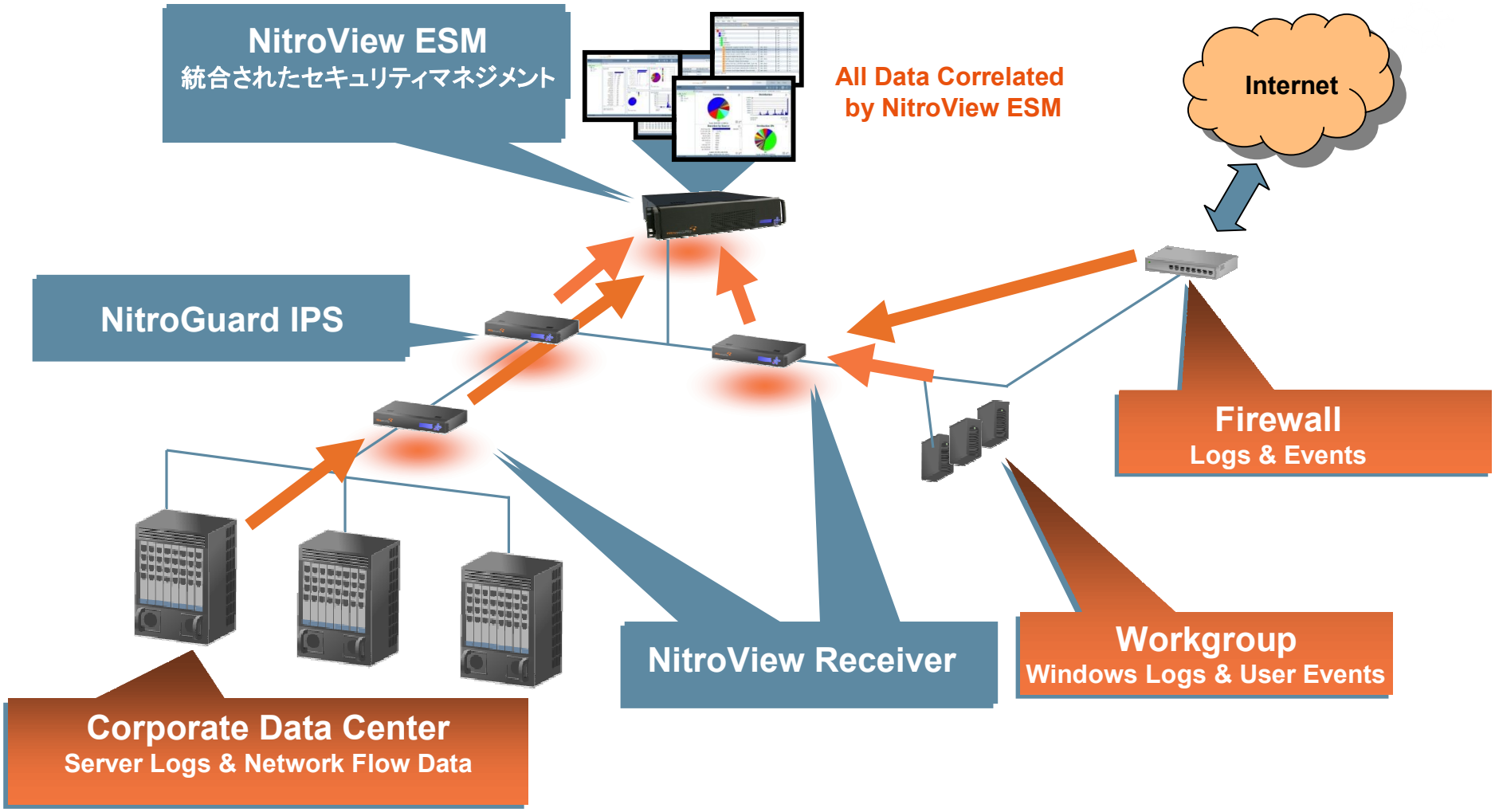
Developed &
使いこなされる
セージ&AdaSage
dbテクノロジー

Patented &
商業化される
NitroEDBデータベース

スタートされたIPS&
セキュリティマネジメント
製品

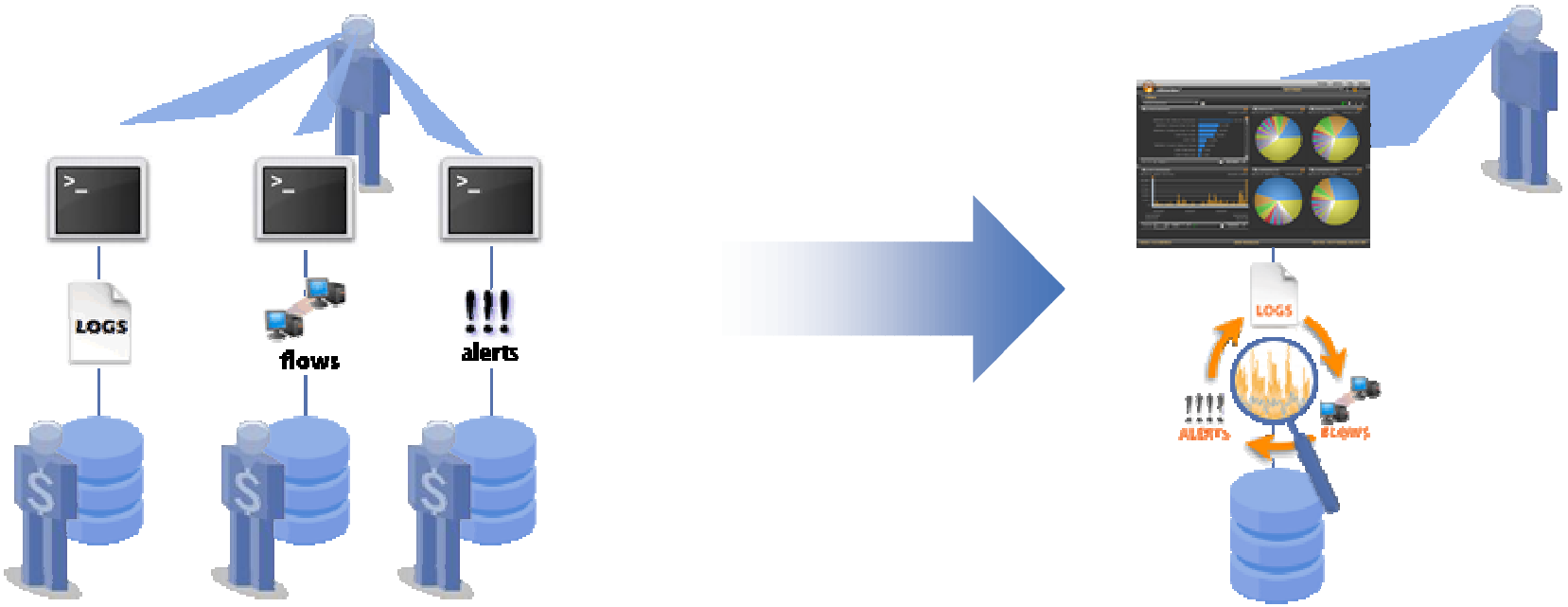
NitroSecurity 解決策

Unifying 情報セキュリティ



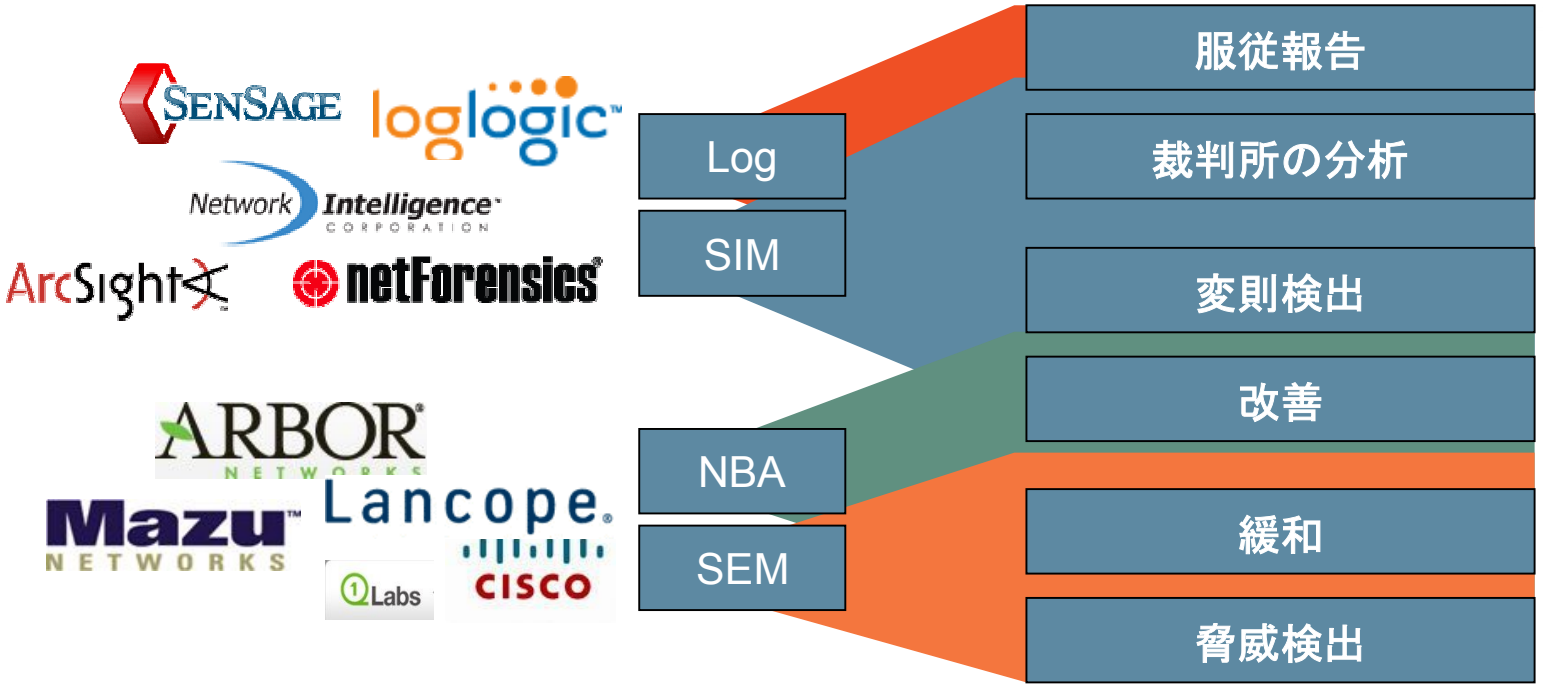
統合されたセキュリティマネジメント

- 新しい要求 = 新しい要件
  - 服従報告　→　Log Management
  - 脅威防止　→　SIEM
  - 裁判所の分析 →　変則検出／ネットワーク行動分析
- これらの機能の分離：
  - 加算は&複雑さについてコストを見積
  - “ブラインドはしみになります”というセキュリティを作成



NitroView:統合されたセキュリティマネジメント

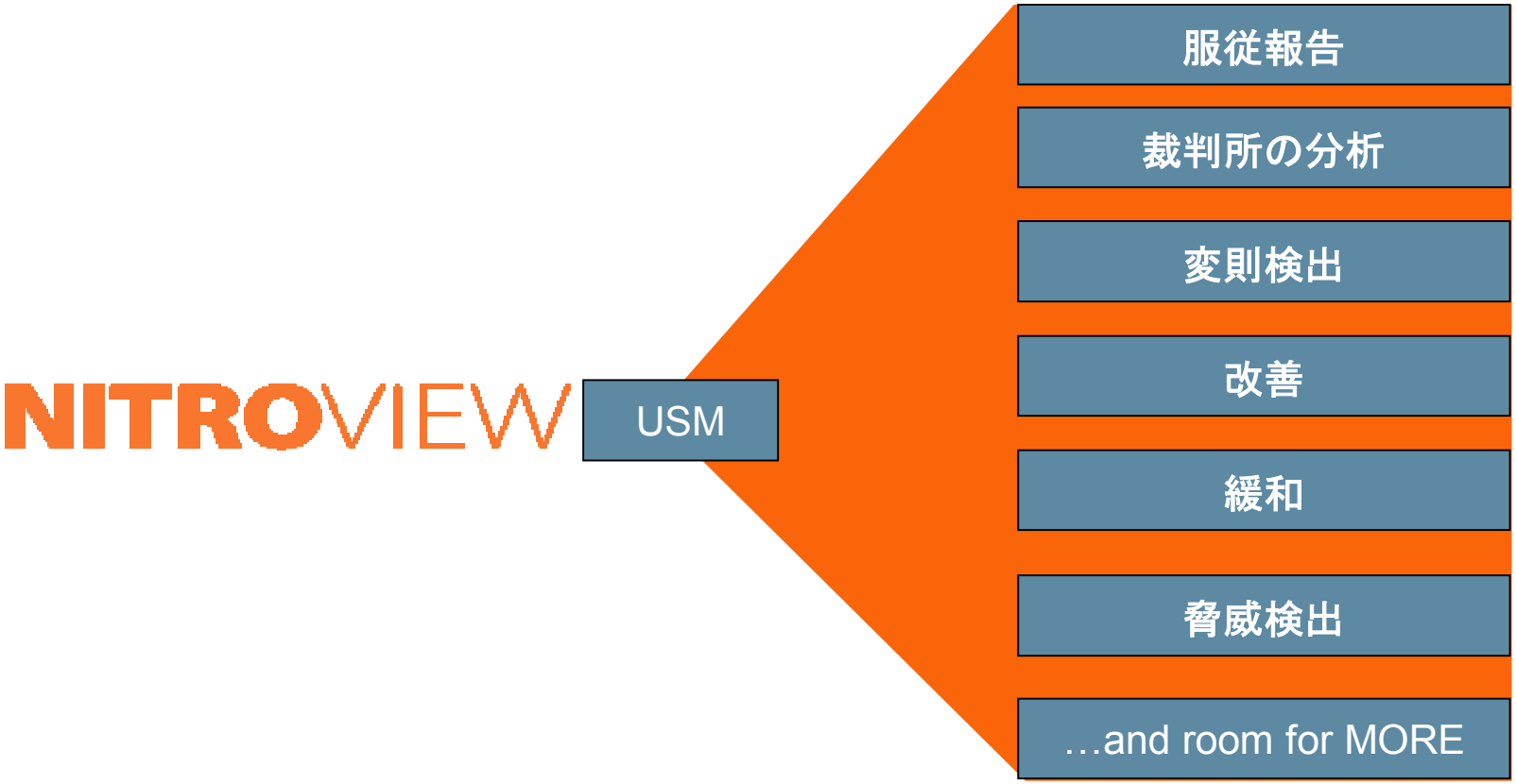
競合するSIM、SEM、NBA、およびログマネジャーは、重ねている機能を持つことができます。



…しかし、完全な統合はデータストレージと管理制限のため不可能です

NitroView:統合されたセキュリティマネジメント

NitroSecurityは、データストレージおよびより速く時の100である分析テクノロジーの特許を取得しました。



…成長する多くの余地によってこれらの機能の完全なユニフィケーションを可能にします。

NitroView: USMのセキュリティ情報／イベント管理

- 伝統的 SIM/SEM
  - 方針、役割、および財産を中心に行ってください
  - それらが起こることとしてのイベントの分析
  - イベントの相互関係は要約または他のデータ整理テクニックを含みます
  - データ整理による、制限された歴史の分析
  - 服従リポート世代
  - 操作上の弁論術に適当ではありません

- 低い性能
- 相互関係規則&分類学の「信頼」を必要とします
- High Cost

- SIM/SEM in NitroView
  - フォーカスはデータにあります
  - 方針、役割、アイデンティティ、財産は、本当のデータと関連します
  - 索引を完全に付けられて、関係のデータベースを経たすべてのイベントデータの相互関係
  - アイデンティティによってイベントを検索してください
  - 歴史およびライブのデータはシームレスに管理されます
  - 服従リポート世代
  - 操作上の弁論術のための理想

- より高い性能
- 内蔵の規則に加えてリアルタイムおよび特別の相互関係を許します
- Lower Cost

NitroView: USMの管理を記録

- 伝統的なログマネジャー
  - Storage of raw logs
  - Logs from most any source
  - ログの暗号化／保護
  - ログ は検索可能に、服従／監査使用のために第一に
  - ログ は標準化されない
  - ログ は操作上の弁論術のために使われない

- リアルタイムの弁論術のために使用できないデータを記録
- High Cost
- 完全なログ検索は、イベントを見つけるために必要です

- NitroViewの管理を記録
  - ストレージ of 標準化されるログ
  - ほとんどのネットワーク&セキュリティログソース（WMI、ファイヤーウォール、syslogなど）
  - ログは構文解析し、標準化
  - 構文解析されたログは、操作上の弁論術のために使用（速い質問、データピボットなど）

- リアルタイムの弁論術のために使用可能です
- Low Cost
- 構文解析されたログデータは、イベントをピンポイントで狙うために容易に検索されます

NitroView: USMでの行動分析をネットワーク化してください

- 伝統的 NBAD
  - モニタネットワークフローデータとユーザー活動
  - 急速なフロー処理
  - 歴史のフロー解析
  - ネットワーク活動&変則検出におけるフォーカス
  - Alert-based 変則の通知

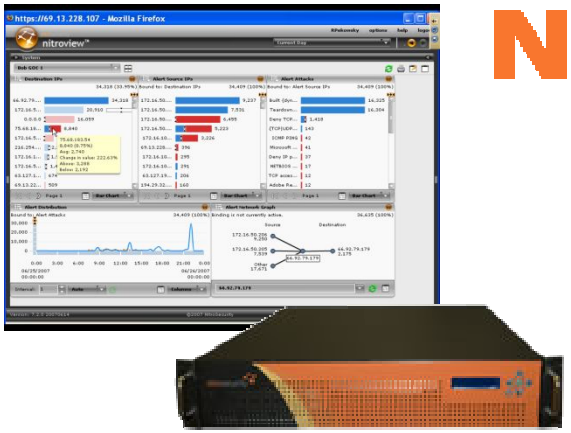
- 有益けれども近視ネットワーク化／操作上ツール
- イベントまたは裁判所のデータへの無リアルタイムの相互関係

- NitroViewのネットワーク分析
  - モニタネットワークフローデータとユーザー活動
  - また、ログデータ、セキュリティイベントデータを監視
  - 急速なフロー処理は相互関係を他のデータソースに含む
  - 活動と変則検出は、また、他のデータソースにあてはまります
  - イベント／フローオーバーレイを持つトポロジー眺め*(future, v7.3)*
  - トポロジーは改善のためにコントロール*(future, v7.3)*

- 高視界ネットワーク操作上ツール
- 加算がネットワーク化すること、およびUSMのSIM、SEM、およびログ管理機能へのユーザー活動&分析

NitroView 企業保障マネジャー

- **USM Appliance**
  - パワフル: セキュリティマネジメント機能の完全なユニフィケーションを提供します。
  - スケーラブル: 必要であるように、単一の器具または配布されたニトロ見方レシーバーを使用
  - 高い価値: 個々のSIEMより効果的なので効果的なより多くのコスト、NBA、ログマネジャー
  - 認められています: 数百人の顧客によりグローバルに使いこなされた賞を受けたシステム



NITROVIEW

GCN "Value: A" Government Computer News (06, 06, 2007)

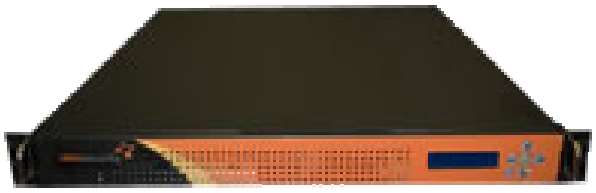
EAL 3 certified

SC MAGAZINE LAB APPROVED

NitroGuard IPS

- Signature based IDS / IPS
  - 業界標準サインフォーマットを使い、容易に拡張可能
  - 検出のタイプ:
    - 基づくサイン
    - 基づく変則
    - 発見的学習
  - 0日保護のための高性能ソフトウェアアーキテクチャ柔軟性
  - 高性能で頑強なサインセットによって評価
  - どのようなネットワークでも適応させるバーチャルIDS/IPS機能を持つIDSまたはIPSモード

NITROGUARD



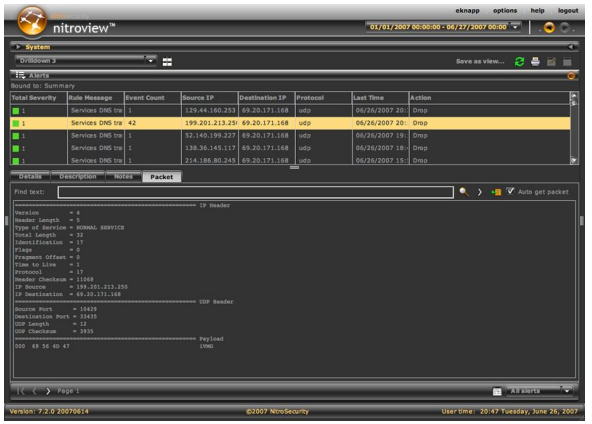
EAL 3 certified

SC MAGAZINE RECOMMENDED

SC MAGAZINE INNOVATOR 2007

NitroGuardは “IPS” より多くです

- …Network Flow Analysis
  - 継続的なフロー解析（引き起こされないか、またはサンプリングされます）
  - 変則検出をネットワーク化してください
- …Flow / Event Correlation
  - イベントとフローの間の関係を見てください
  - 攻撃のソースを見つけてください
  - どんな他の宛先が攻撃されたかもしれないかをわかってください
  - 異例のまたは変則的なネットワーク行動と関連するすべてのイベントを見てください
- …Event & packet capture for historical / forensic analysis
  - 収集されたイベントデータの粒状性は、時間の間失われません
  - インテリジェントな圧縮により粒状の詳細が維持されます



…ニトロガードは完全です。
それのためのデータを
収集するために精査してください。
統合されたセキュリティマネジメント

NitroGuard –より大きい解決策の一部

- Traditional IDS, IPS & UTM devices
  - 脅威を検出するために、交通をサイン／規則のセットと比較
  - 警告を生成します (IDS)
  - ブロック交通 (IPS, UTM)
  - 内容濾過、または他のセキュリティ機能というファイアウォールを含むかもしれません (IPS, UTM)

"IPSがまだ君臨している所にさえ、より大きい写真の一部であるかもしれないIPSだけが残存します。"

~ Dr. Peter Stephenson
SC Magazine

- NitroGuard IPS
  - Deep packet inspection:
    - 脅威を検出するために、交通をサインの大きいセットと比較
    - イベント変則を検出する時間の上のイベントを分析
  - Collects flow data:
    - 脅威&変則を検出するために、フローサインに比較
    - 脅威&変則を検出する時間の上のフローを分析
    - フローをより一層の分析のためのイベントと関係づける
  - 警告および／またはブロック交通
  - インタフェースまたはVLANあたりサポートユニーク方針
  - 統合されたセキュリティマネジメントの一部:
    - リアルタイムにおいて、関連したフローとイベントデータを収集し、格納します
    - フローとイベントデータをより高レベル分析に利用可能

SC MAGAZINE RECOMMENDED
SC MAGAZINE INNOVATOR 2007

"... IPS、ESMおよびレシーバーすべては、その高性能系図事 that 無他のシステム缶 をすることができるシステムに発展しています。"

~ Dr. Peter Stephenson
SC Magazine

例：複雑な攻撃を防止するために、ニトロ見方&ニトロガードを使用

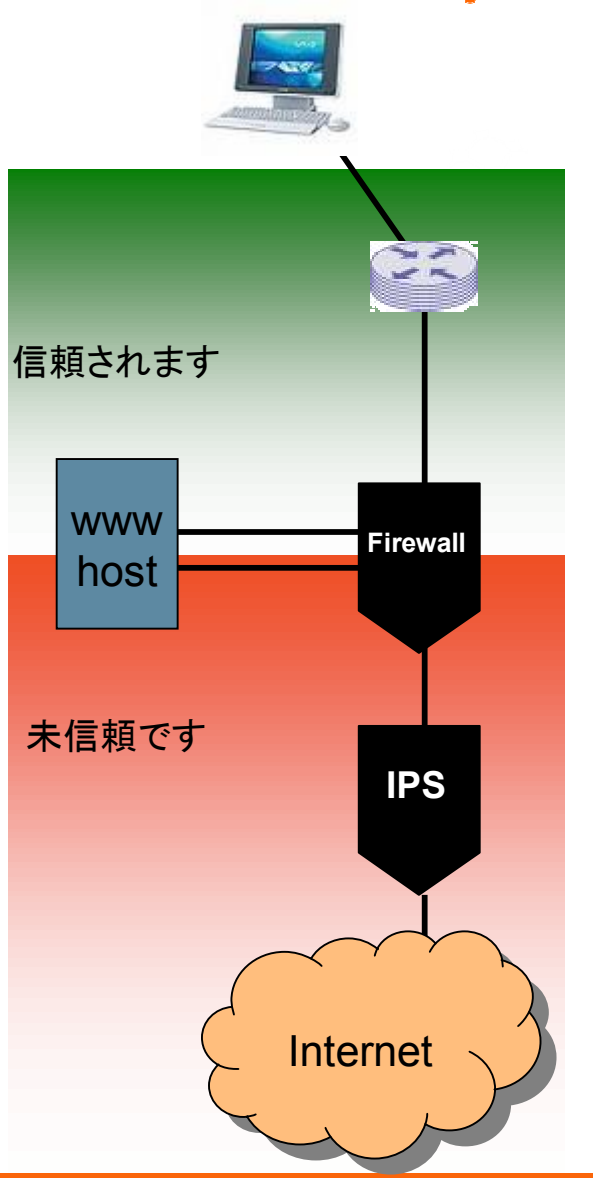
例：ネットワーク

- 以下を含むネットワーク持ち典型的防御：
  - An IPS
  - A Firewall
  - A Routed Internal Network

- ファイヤーウォールは、DMZに取り付けられたホストのシステムを持つ(e.g., web server)
  - ウェブサーバーは、また、内部 ならば 特権を与えられたユーザーとadminのための『裏口』で接続される

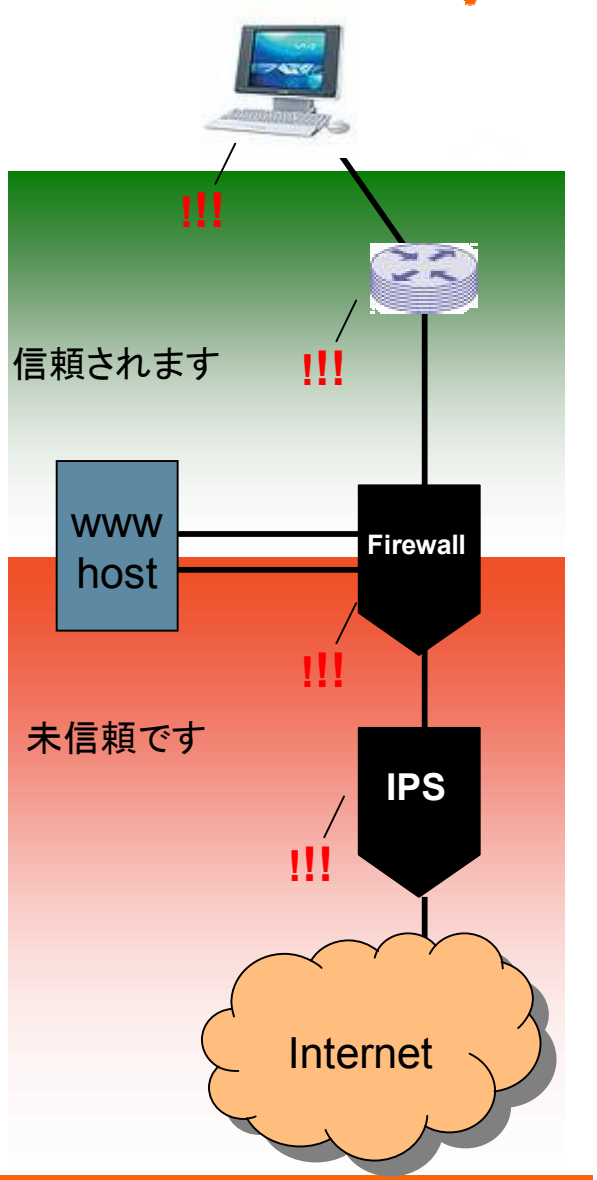
- 安全なデータはデータベース、ネットワークの中の金庫において格納される。

…金庫はどれほどですか?



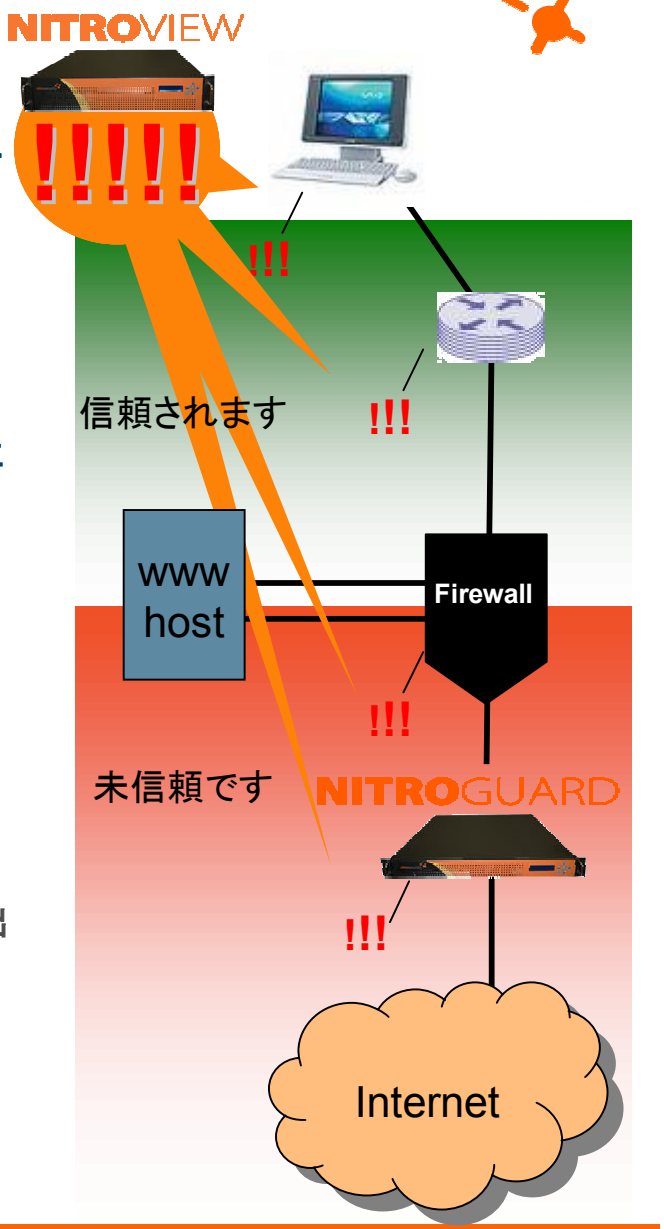
例：攻撃

1. ハッカーポートはウェブサーバーを走査し、ポート69が開いていると気付きます。
   - IPSはportscan警告を送ります。
   - ファイヤーウォールはportscan警告を送ります。
   - 両方の警告は同様な警告の高いボリュームのため気づかれず行きそうです。
2. tftpは、/など／passwdをダウンロードしてウェブサーバーのポート69に開始されます。
   - IPSはTFTP違反警告を送ります。
   - また、これは、逃された量 生成された 反対 と交通が未信頼であった警告の大規模な量 でありそうです。
3. ログインは安全なデータベースで試みられます。
   - データベースサーバーはLOGIN故障警告を送ります。
4. 交通行動は変わります。
   - NBADシステムは、目標サーバーから用心深い示している変則的なトラフィックをインターネットに送ります。データは盗まれました！



例：視界にUSMを提供します。

- 攻撃は見られえて、停止しました ならば：
  - IPS, Firewall, Server, and Network information情報は一緒に見られえました。
    - 変化を増大させて、攻撃はそれが遅すぎる前に見分けられます！
  - IPSとファイヤーウォールとサーバーとネットワーク情報は一緒に関係づけられているかもしれません。
    - するために様々な攻撃ベクトルに沿って単一の徴候が前と後ろに追跡されることを可能にします：
      - 根原因を決定
      - 追加の目標／違反を決定
  - Logs from IPS, Firewall, Server, and Network information時間の間一緒に分析できました。
    - 歴史を通る攻撃の段階への許可視界
      - 遅い攻撃を検出
      - より遠くに視界を増大させるために、全体観の変則検出を提供

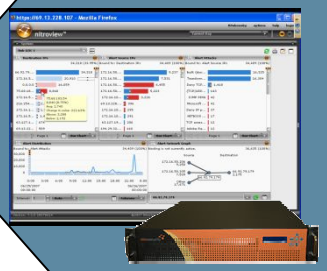


NitroSecurity 製品

NitroSecurity Products

NITROVIEW

NITROVIEW ESM



分析、相互関係、および報告

- 統合されたセキュリティマネジメント
  - SIEM
  - Log Management
  - Network分析
- 服従報告
- リアルタイム操作上弁論術
- 企業業績&スケーラビリティ

NITROVIEW Receiver

ログ、イベント、&フローのコレクション

- Net flow, S-Flow, WMI data
- Firewalls, IDS, Log Data, SYSLOG data
- Real-time相互関係と集合体

5K – 15K events per second

NITROGUARD

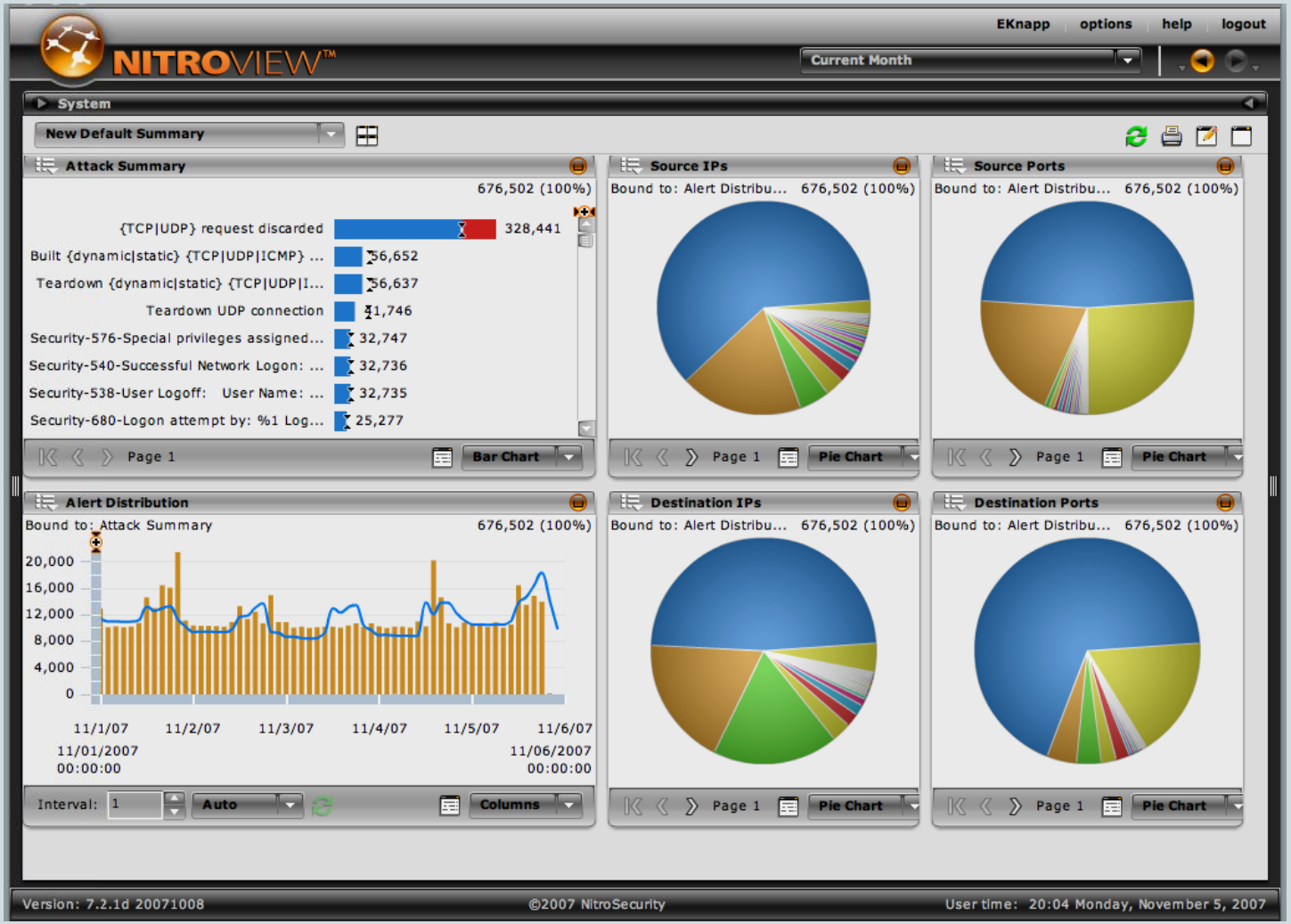
NITROGUARD IPS

侵入検出&防止

- 証明された企業スケール
- 統合されたサイン&変則検出
- 流れ／イベント相互関係
- バーチャルなIPS機能
- お忍び管理モード
- 存在&0日脅威検出

250 Mbps – 1.5 Gbps throughput

NitroView:視覚化するパワー



Industry 認識

EAL 3 certified

- “真実のネットワーク脅威分析は、SIEM ...forget簡単SIM/SEM製品または伝統的なログ相関計を越えます。ニトロ眺めは3つのエリアで向こうにそれらをすべて吹きつけます: 包括的なログ管理、反応スピード、および分析深さ。”
  - Dr. Peter Stephenson, SC Magazine

- “すべての他のセキュリティゲートウェイ器具に絶えず注意し、1つの中心的で、使いやすいインタフェースからそれらをコントロールする器具は、時間が来た機器です。”
  - Greg Crowe, Government Computer News

- “... IPS、ESMおよびレシーバーすべては、その高性能系図 事 that 無他のシステム缶 をすることができるシステムに発展しています。”
  - Dr. Peter Stephenson, SC Magazine

NitroView 機能詳細 -アイデンティティ管理

- ユーザーによってイベントを追跡
  - whoに追加の文脈を提供し、それについて責任があるか、またはイベントにより影響されます。
- WMIログからエンドユーザーアイデンティティ（ユーザーネーム）を知ります。
  - 未来のリリースにおいて追加される他のソース（RADIUSなど）
- ローカルにキャッシュされたDNSルックアップを使ってネットワークアイデンティティ（ドメインネーム）を学びます。
- いったんアイデンティティが知られたら、それはそのユーザーから他のイベントに補外できるでしょう。
  - E.g.,もしWMIメッセージがユーザーネームを含み、そのユーザーネームがそのユーザーのためのIP、MACなどと関連するならば
  - ユーザーネームデータを明示的に含まないユーザーベースの報告使用データソースを許します（フロー、イベントログなど）。

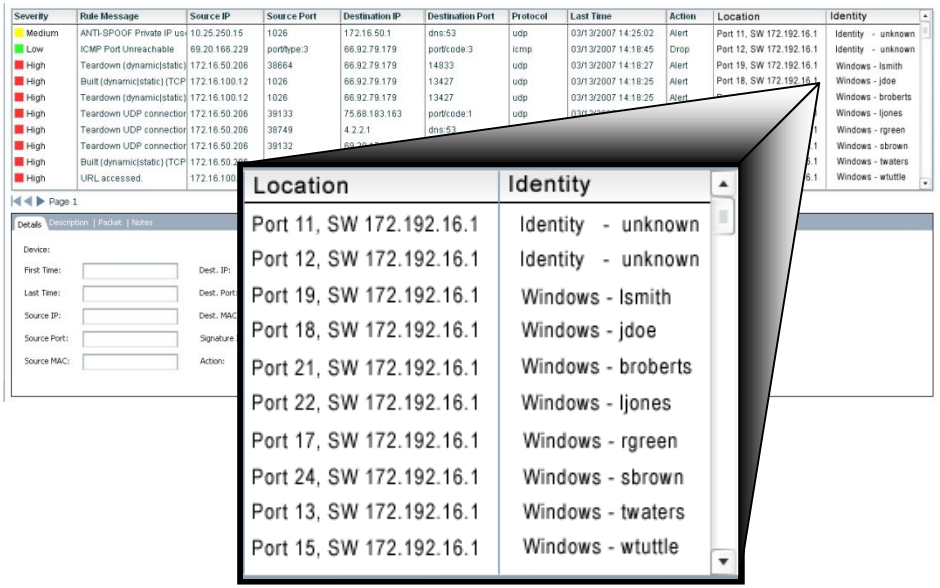
NitroView機能詳細 -アイデンティティ管理

- アイデンティティ情報は索引を完全に付けられます:
  - 検索、データ回転というフィルタのために使われえます。
  - 容易に、フロー、イベント、および他の収集されたデータと関係づけられています。

アイデンティティ
および
認証データ

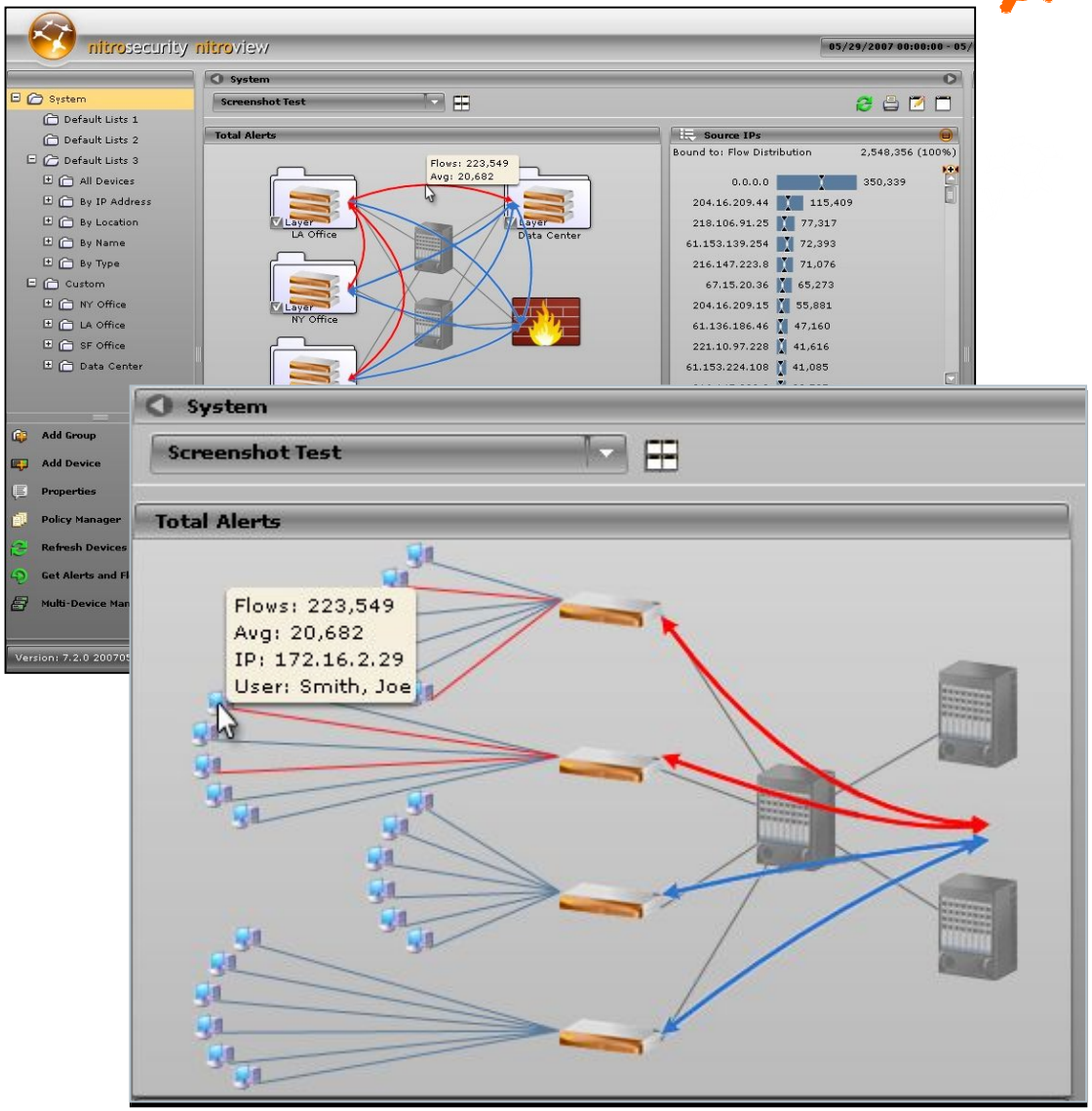
ネットワーク
トポロジー
データ

関係づけられた
イベント



NitroView 機能詳細 -トポロジー文脈をネットワーク化

- 物質的な位置に関連してイベントとフローを提供
- 物質的なアーキテクチャの上のオーバーレイアイデンティティと財産
- スピードは改善をネットワーク化
- 活動のリアルタイムベースライン
- ネットワークとクライアント発見にトポロジーを提供



NitroView機能詳細 – 服従報告

- あらかじめフォーマットされた服従リポートを提供
  - PCI
  - SOX
  - HIPAA
  - GBLA
  - Etc.
- リポートは要求に応じて実行されるか、またはスケジューリング
- リポートは、ユーザー、IP、機器により、フィルタをかける
- リポートは自動的に配布できて、ユーザー・ポリシーを尊敬
  - MSSPsのための理想　-すべてのクライアントに1つのリポートをスケジューリングし、配布してください：それぞれは、それらに関連したデータだけを見ます。

NitroView機能詳細 –服従報告

- Near Real-Time 服従報告
  - 他のニトロ眺め機能と同じエンジンを使用

- 高く粒状のデータ
  - ニトロ眺めが要約しないことまたは“時間サンプル”データ
  - リポートはより粒状で、より貴重

NitroView 機能詳細 – イベント相互関係

- 「複雑なイベント」は、より大きい脅威を識別するために支配
  - “A + B + C =脅威”
  - 助けはイベントノイズの間の本当の脅威を識別
  - もみ殻から小麦を分離

- コンポーネントイベントは完全に守られる
  - 基本のイベント（A、B、C）は、蓄えられた長期
  - 相互関係の結果としての粒状性の無縮小

- Supplements NitroView’s existing Ad-Hoc data correlation capability
  - 関係づけられているイベントおよび／またはそれらのコンポーネントは、まだ下記であるかもしれません:
    - 手動で、他のフローと関係づけられています イベントまたはログデータ
    - 傾向／変則／操作上の弁論術のために分析

ありがとうございます。