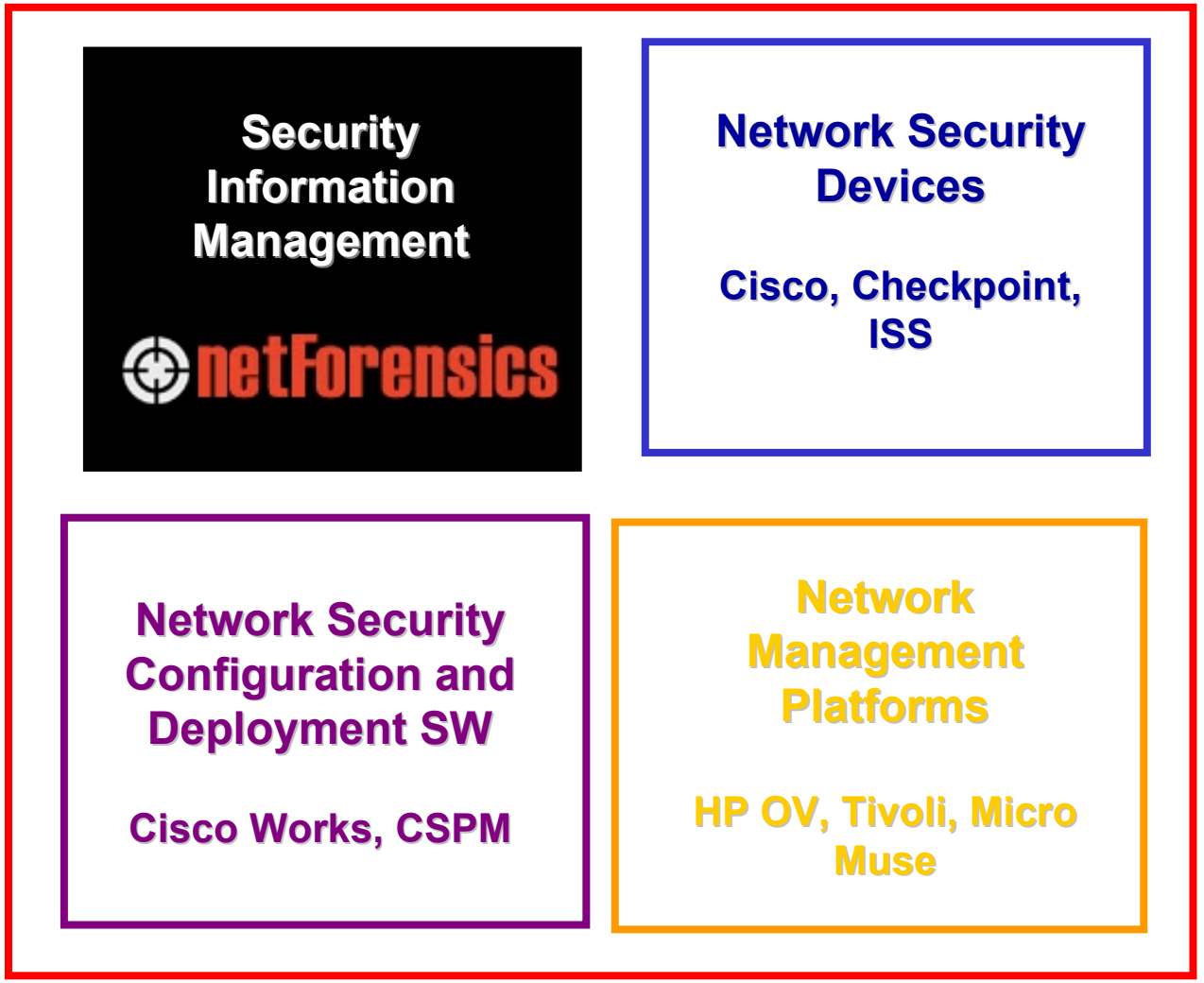
netForensics

Security Information Management

Network Management and SIM

netForensics

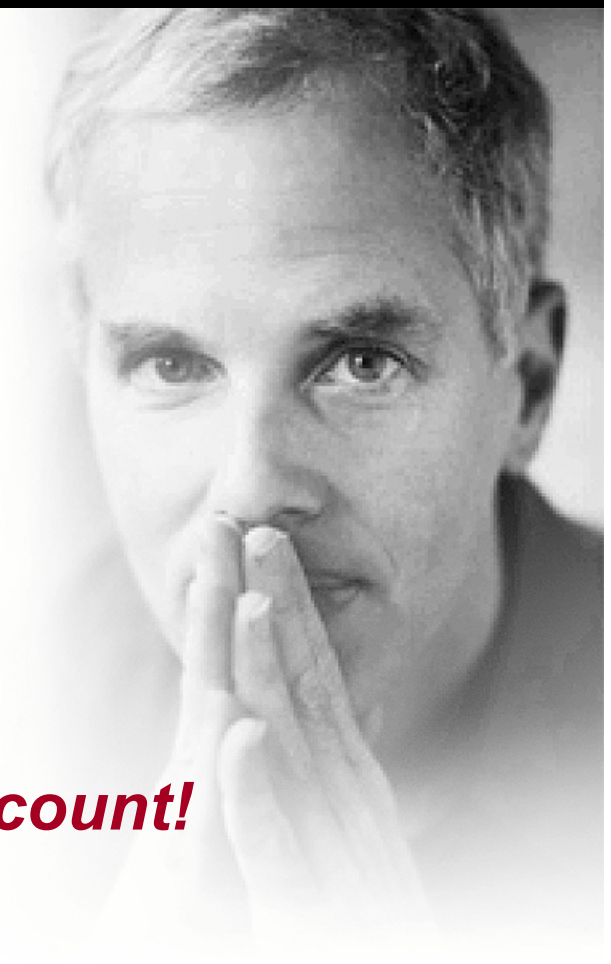
40% of Total Messages



Today's Security Challenges

netForensics

- Taking control over the **Volume & Complexity** of security alarms
- Dealing with too many **False Positives**
- **Minimizing Risk** of potential attacks
- **Accelerating Response** when attacks occur



…All With Your Existing Headcount!

Security Information Management

netForensics

What is Security Information Management?

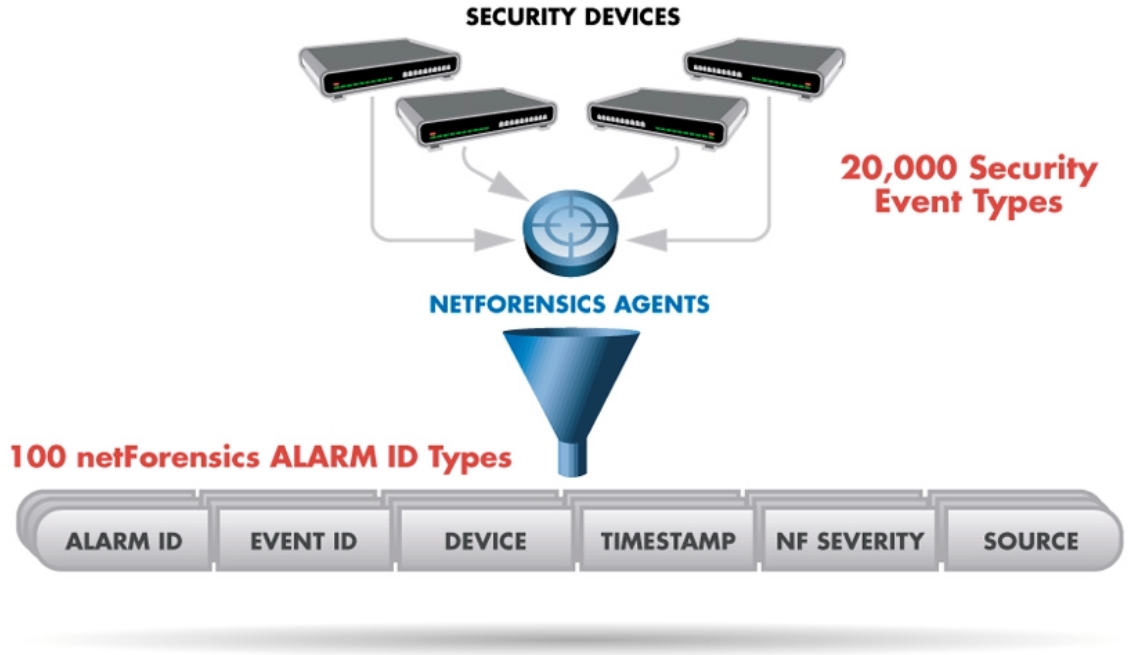
- **SIM lets you manage your growing security infrastructure with your existing team:**
  - ***Normalize & Aggregate*** security events across your enterprise
  - ***Correlate & Visualize*** to identify & respond to threats in real-time

netForensics SIM is an Important Component of Enterprise Security… Let's See How it Works…

netForensics Normalization

During **Normalization,** netForensics Agents collect security data and transform it into optimized XML

- Over 20,000 security events are mapped into 100 netForensics Alarm ID's
- Multiple agents balance workloads and support your distributed enterprise
- Data is transmitted across your network via secure TCP

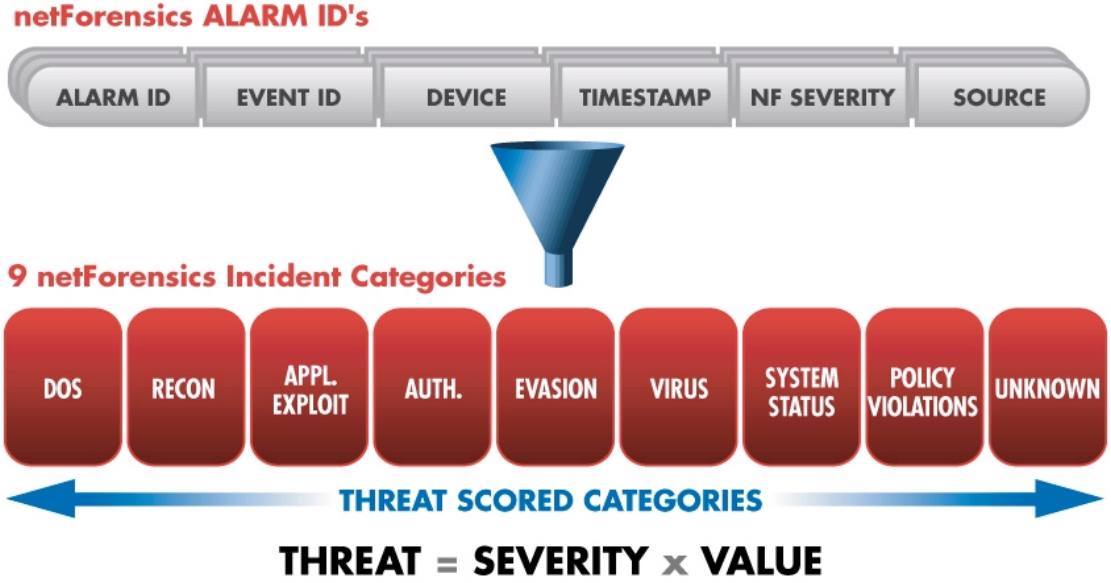


netForensics Aggregation

netForensics

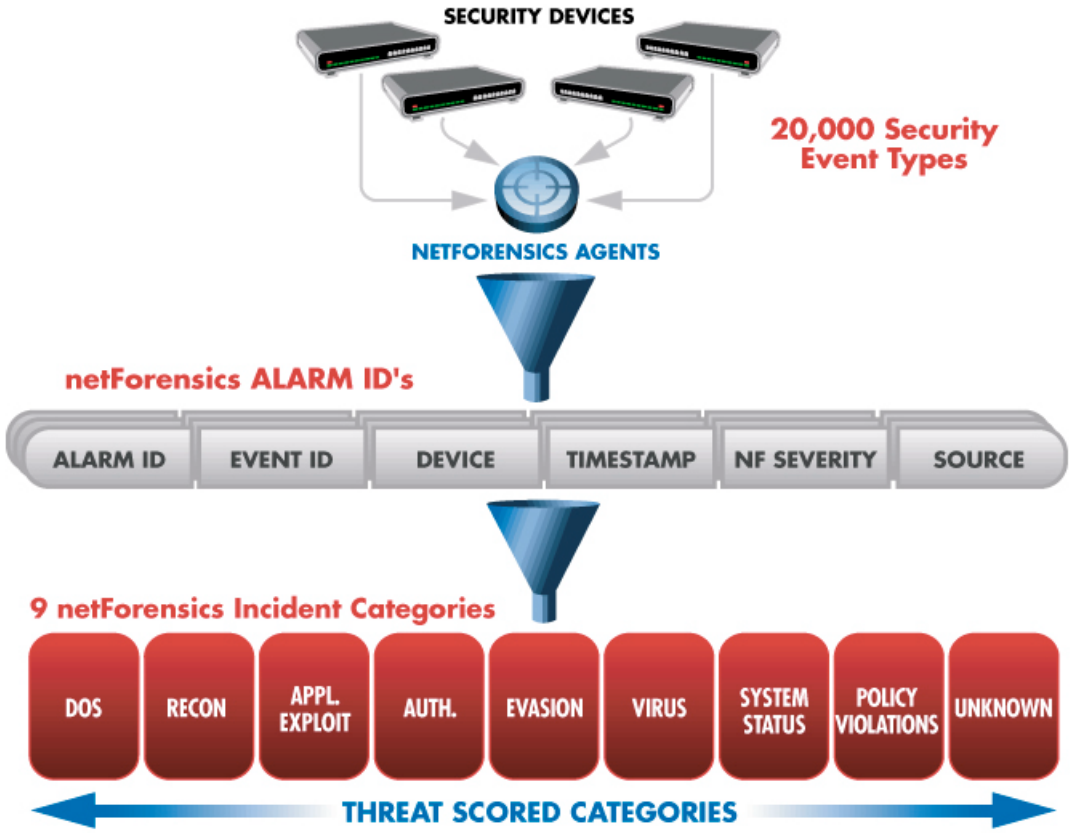
During **Aggregation,** netForensics Engines further processes event data to determine *Incident Type* and risk of occurrence

- Engines categorize Alarm ID's into 9 incident categories (users may add additional categories if necessary)
- Data is aggregated to remove duplicate events
- Resultant incident types are scored to determine threat level



netForensics Correlation

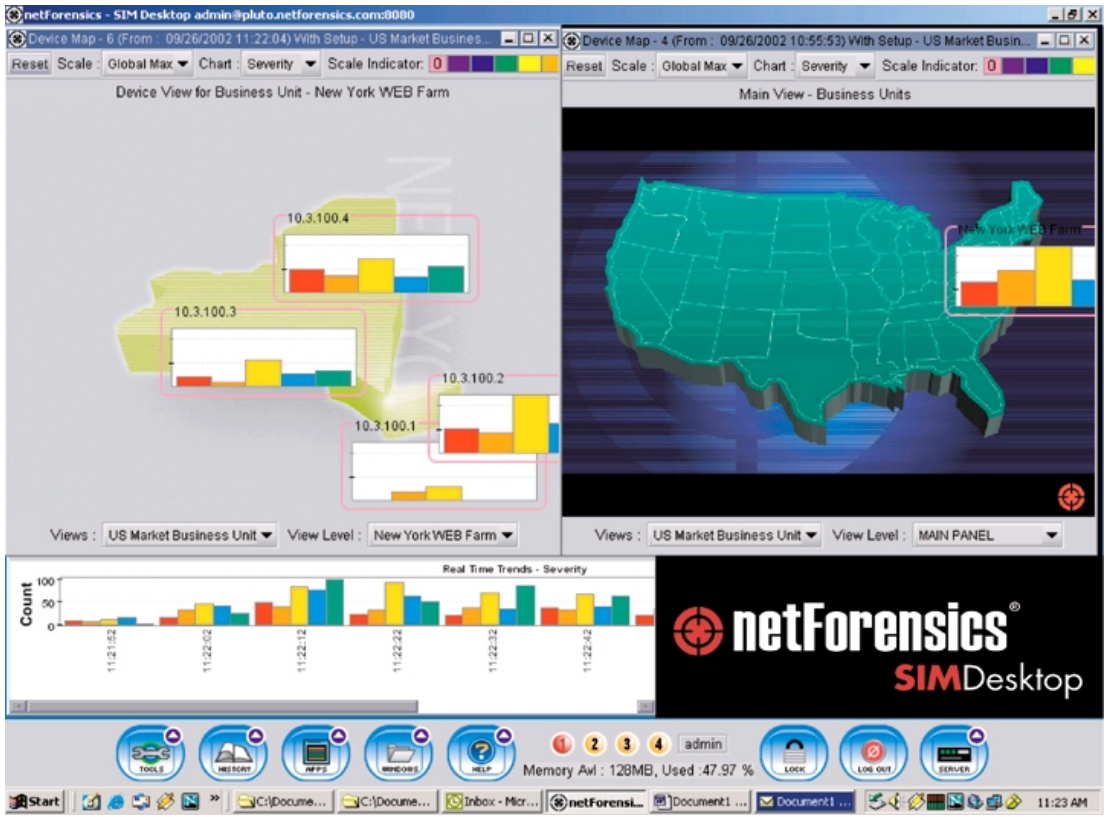
Correlation measures the relationship of two or more security events to determine Incident potential. netForensics Engines Statistically Correlate normalized and aggregated security data in real-time



netForensics Visualization

netForensics SIM Desktop - Dashboard View

- Real-time geographical view of security event trends across the enterprise
- View events by business unit, asset, or device
- Choose from Event Severity or Categorized View
- **SIM Desktop** provides intuitive dashboard interface for high-level graphical summary of enterprise security landscape



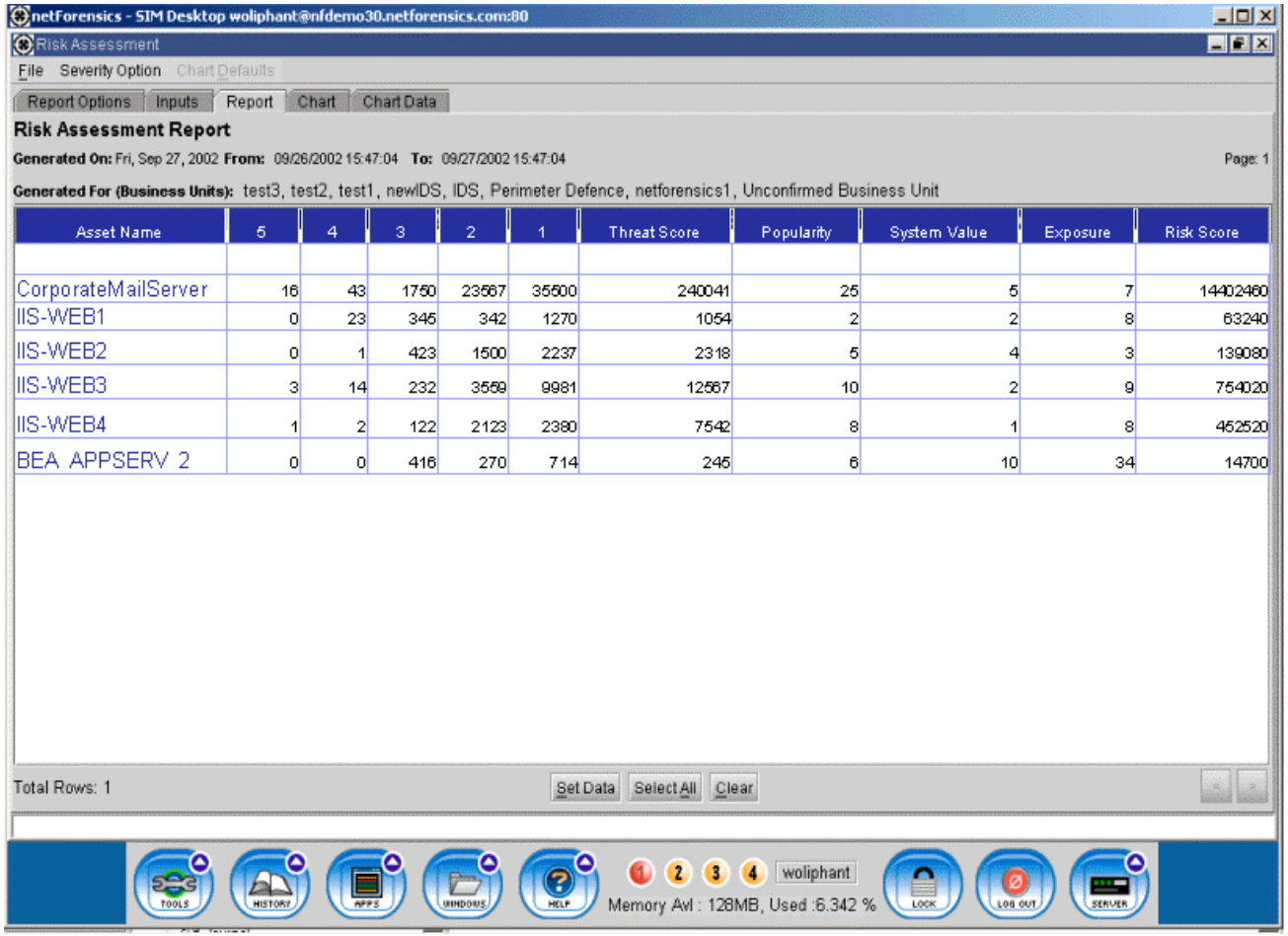
Global View Provides "Big Picture" View of Security Trends

Minimizing Risk

netForensics

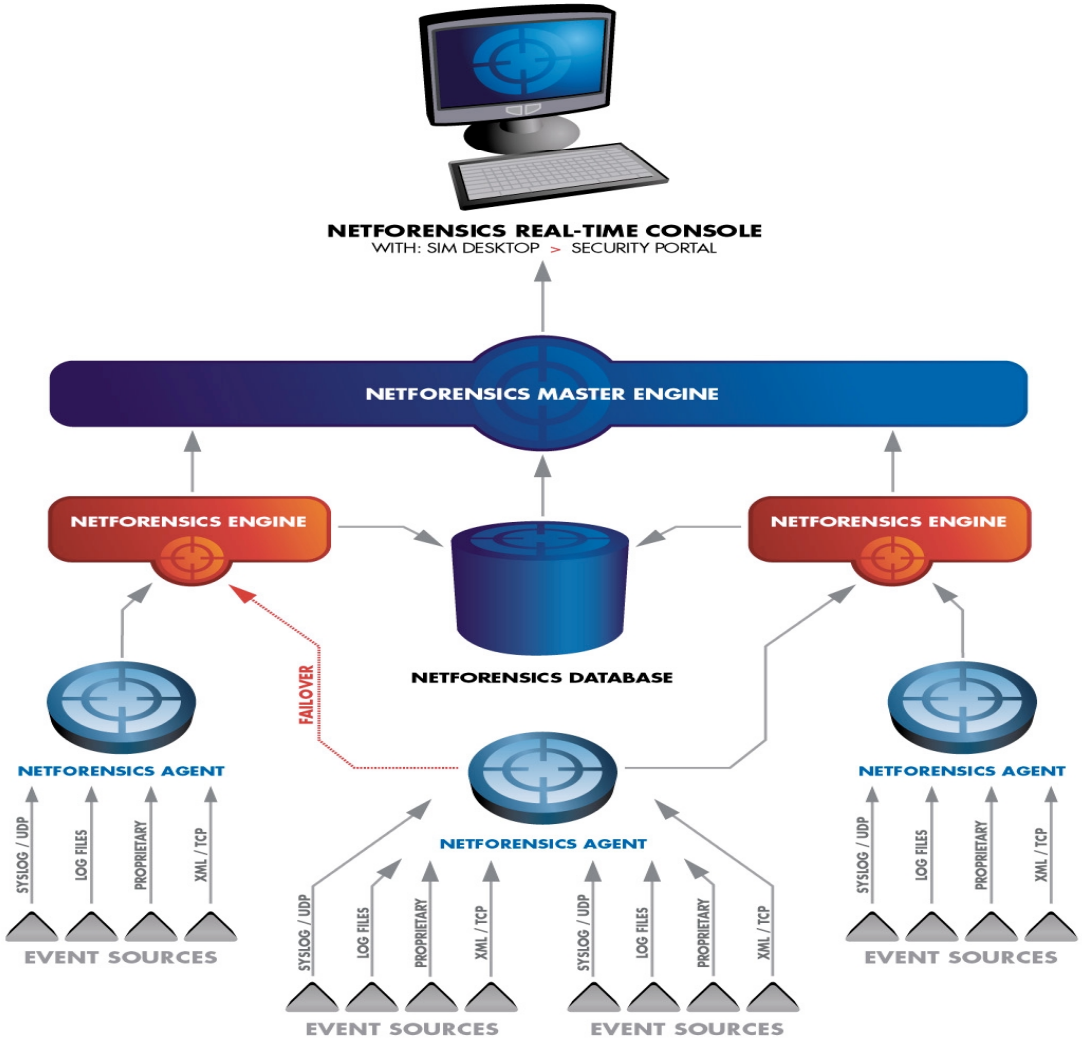
netForensics Risk Assessment Report

- netForensics combines Risk Scoring and Categorization for a comprehensive threat picture
- Provides correlated view of all assets



netForensics Provides Quantitative Risk Assessment

netForensics Architecture



Agent Supported Products

netForensics

- Cisco Secure PIX
- Cisco Secure IDS
- Cisco Secure ACS
- Cisco IOS Firewall / IDS / ACL
- Cisco VPN Concentrators
- Cisco-OKENA – Host based IDS
- Entercept – Host based IDS
- ISS Real Secure - Host/NW IDS
- Microsoft Windows Events
- Check Point Firewall-1
- UNIX Log Data
- NT Log Data
- Netscreen
- Enterasys Dragon
- Snort
- Tripwire
- Symantec Raptor
- Sidewinder
- CyberGuard
- Manhunt
- Other devices via Universal Agent

Cisco OEM's netForensics Platform

netForensics

CiscoWorks Security Information Management Solution v3.1
Available 5/1/03

SOFTWARE

CWSIM-3.1-SS-K9	Starter Kit - Solaris
CWSIM-3.1-SL-K9	Starter Kit - Linux
CWSIM-3.1-EN-K9	Additional Distributed Engine
CWSIM-3.1-DS-K9	Additional Database Solaris
CWSIM-3.1-DL-K9	Additional Database Linux
CWSIM-3.1-ADD20-K9	Additional 20 Devices
CWSIME-1160-K9	Appliance (available 7/1/03)

Summary - Why netForensics?

- **netForensics Increases Your Team's Capacity by…**
  - Eliminating manual device monitoring
  - Automatically correlating security alerts in real-time
  - Resolving security events in real-time from a single console
- **netForensics Gives You Quantifiable Results…**
  - Monitor more devices and alerts with your existing staff
  - Provide better security protection for your enterprise
  - Lower your security TCO

netForensics

International Sales

Rafael Samper
Sales
rafael@netforensics.com
1 508 904 5923

David Avezov
Engineer
Davezov@netforensics.com
1 732 393 6027

Amy McCoy
Inside Support
amccoy@netforensics.com
1 732 393 6040

Fiaz Khan
Sales
fkhan@netforensics.com
44 7764 163 310

John Stiley
Engineer
Johns@netforensics.com
44 7764 163 310