

# netForensics

## Security Information Management





# Network Management and SIM



40% of  
Total  
Messages

**Security  
Information  
Management**



**Network Security  
Devices**

**Cisco, Checkpoint,  
ISS**

**Network Security  
Configuration and  
Deployment SW**

**Cisco Works, CSPM**

**Network  
Management  
Platforms**

**HP OV, Tivoli, Micro  
Muse**

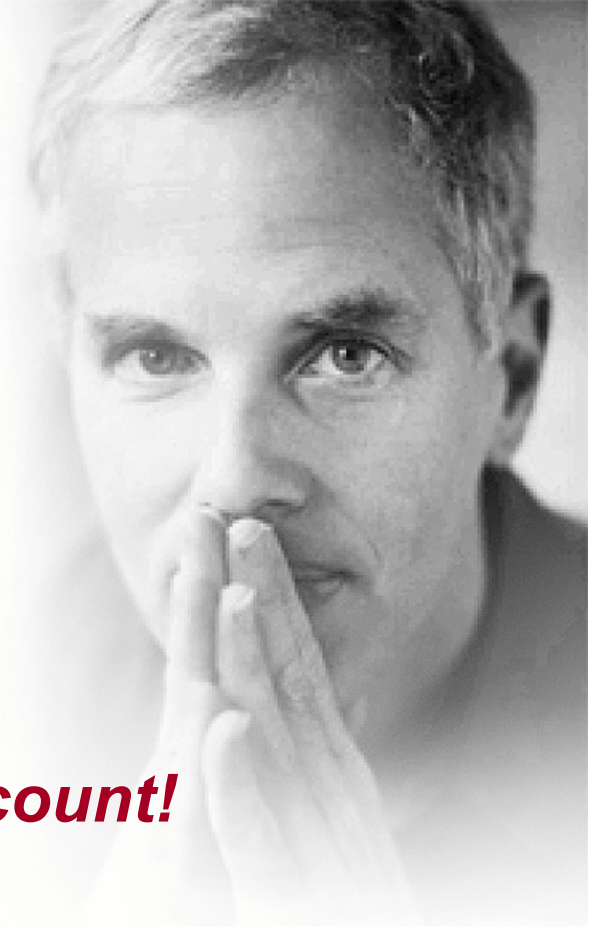


# Today's Security Challenges



- 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!*





## *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...***

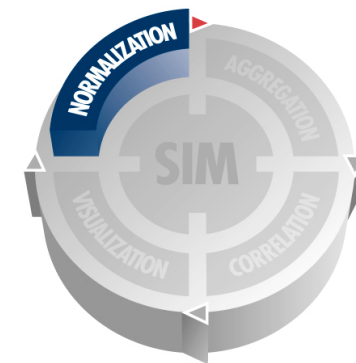
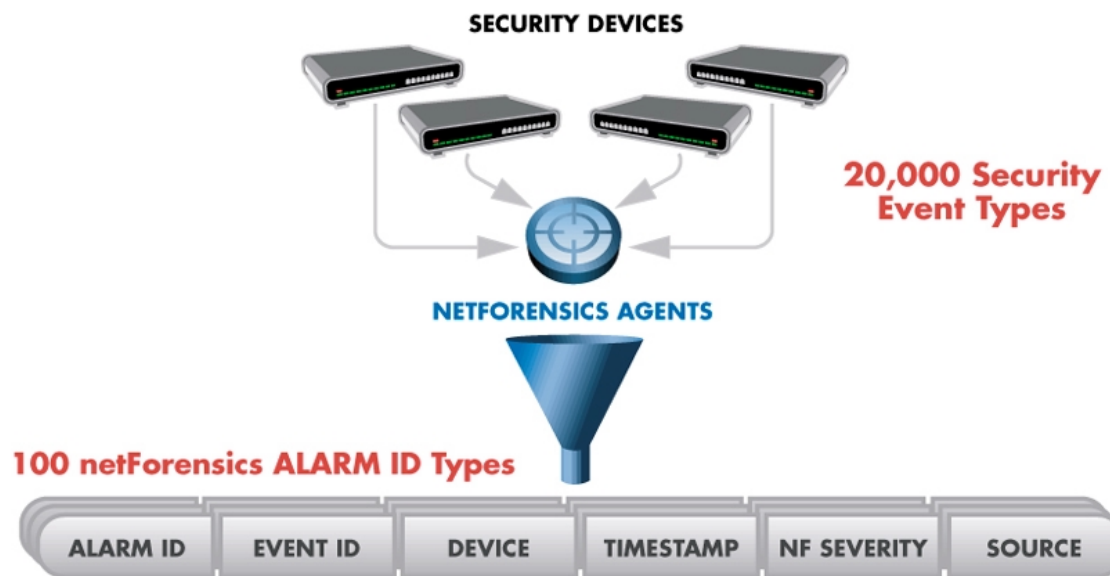


# netForensics Normalization



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





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

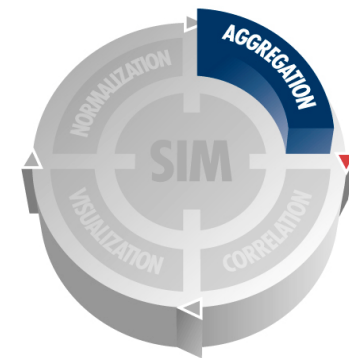
### netForensics ALARM ID's



### 9 netForensics Incident Categories



$$\text{THREAT} = \text{SEVERITY} \times \text{VALUE}$$

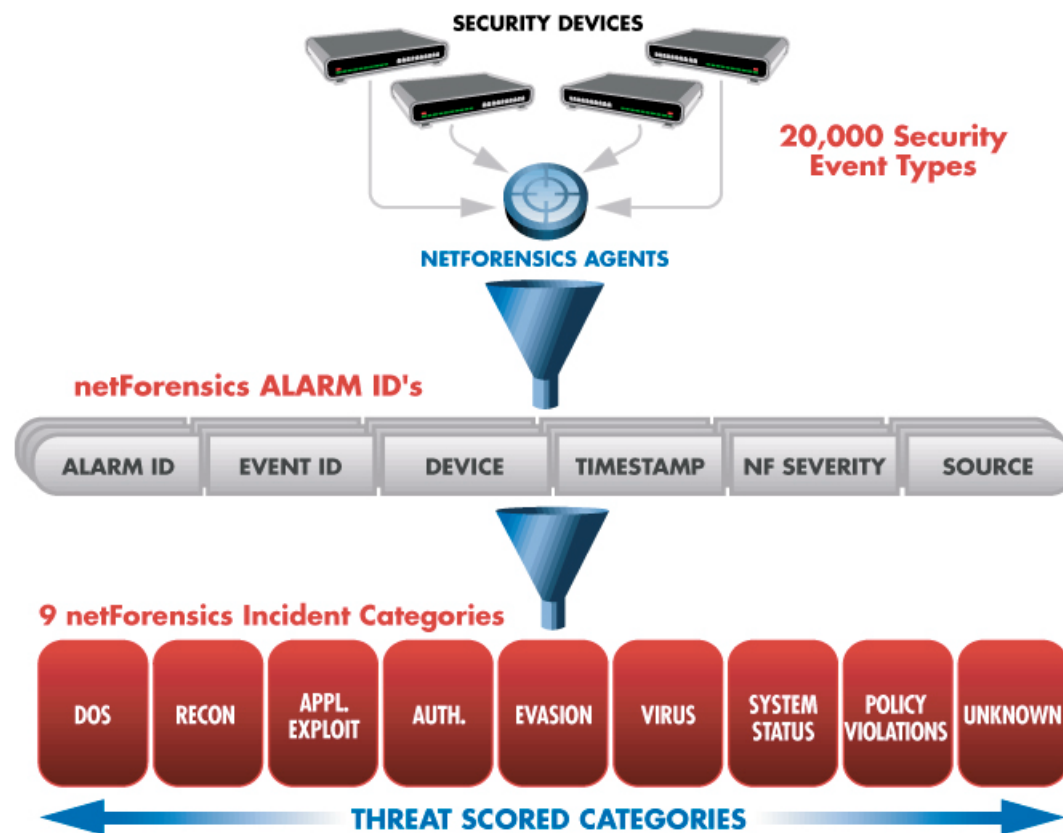




# netForensics Correlation



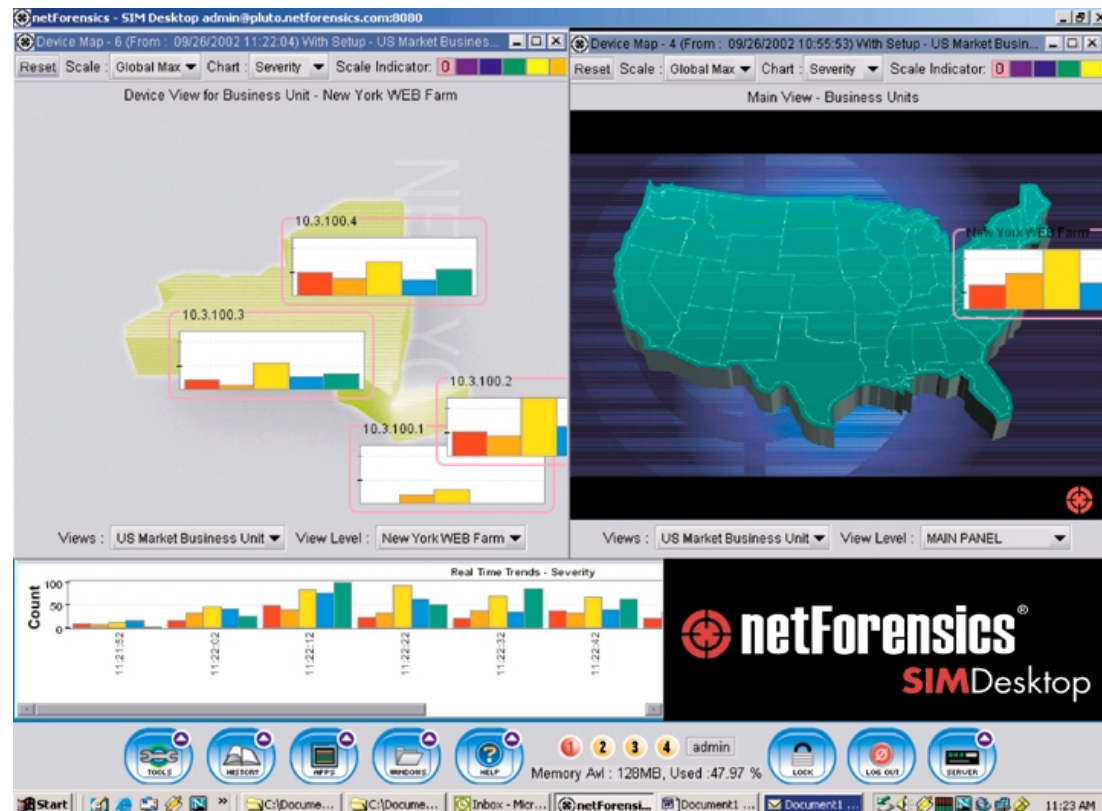
**Correlation** measures the relationship of two or more security events to determine Incident potential. netForensics Engines Statistically Correlate normalized and aggregated security data in real-time





## *netForensics 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 Risk Assessment Report

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

netForensics - SIM Desktop woliphant@nfdemo30.netforensics.com:80

Risk Assessment

File Severity Option Chart Defaults

Report Options Inputs Report Chart Chart Data

**Risk Assessment Report**

Generated On: Fri, Sep 27, 2002 From: 09/26/2002 15:47:04 To: 09/27/2002 15:47:04 Page: 1

Generated For (Business Units): test3, test2, test1, newIDS, IDS, Perimeter Defence, netforensics1, Unconfirmed Business Unit

Asset Name	5	4	3	2	1	Threat Score	Popularity	System Value	Exposure	Risk Score
CorporateMailServer	16	43	1750	23567	35500	240041	25	5	7	14402460
IIS-WEB1	0	23	345	342	1270	1054	2	2	8	63240
IIS-WEB2	0	1	423	1500	2237	2318	5	4	3	139080
IIS-WEB3	3	14	232	3559	9981	12567	10	2	9	754020
IIS-WEB4	1	2	122	2123	2380	7542	8	1	8	452520
BEA APPSERV 2	0	0	416	270	714	245	6	10	34	14700

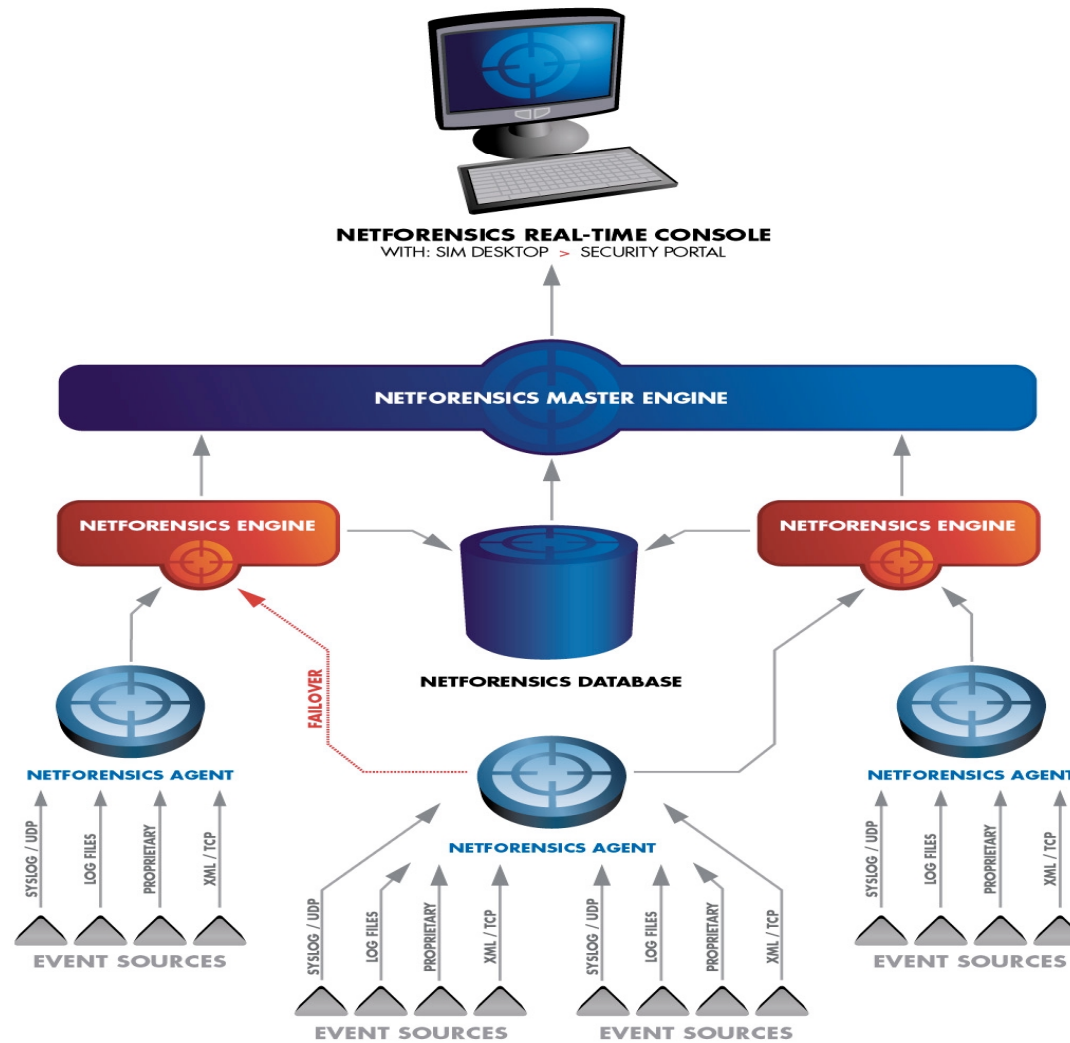
Total Rows: 1

Set Data Select All Clear

TOOLS HISTORY APPS WINDOWS HELP Memory Avl : 128MB, Used :6.342 % LOCK LOG OUT SERVER

***netForensics Provides Quantitative Risk Assessment***

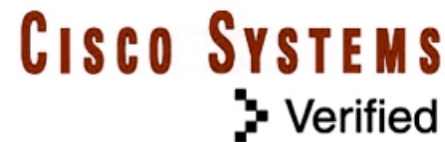
# netForensics Architecture



# Agent Supported Products



- Cisco Secure PIX
- Cisco Secure IDS
- Cisco Secure ACS
- Cisco IOS Firewall / IDS / ACL
- Cisco VPN Concentrators
- Cisco-OKENA – Host based IDS
- Enterscept – 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





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

**S  
O  
F  
T  
W  
A  
R  
E**

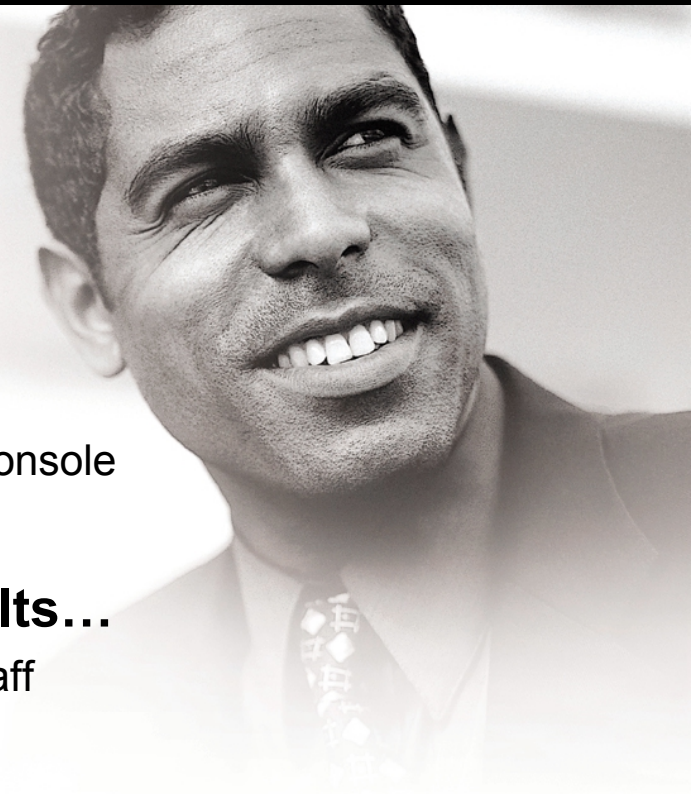
CWSIM-3.1-SS-K9	<b>Starter Kit - Solaris</b>
CWSIM-3.1-SL-K9	<b>Starter Kit - Linux</b>
CWSIM-3.1-EN-K9	<b>Additional Distributed Engine</b>
CWSIM-3.1-DS-K9	<b>Additional Database Solaris</b>
CWSIM-3.1-DL-K9	<b>Additional Database Linux</b>
CWSIM-3.1-ADD20-K9	<b>Additional 20 Devices</b>
CWSIME-1160-K9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



## 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](mailto:rafael@netforensics.com)  
1 508 904 5923

David Avezov  
Engineer

[Davezov@netforensics.com](mailto:Davezov@netforensics.com)  
1 732 393 6027

Amy McCoy  
Inside Support

[amccoy@netforensics.com](mailto:amccoy@netforensics.com)  
1 732 393 6040

Fiaz Khan  
Sales

[fkhan@netforensics.com](mailto:fkhan@netforensics.com)  
44 7764 163 310

John Stiley  
Engineer

[Johns@netforensics.com](mailto:Johns@netforensics.com)  
44 7764 163 310

