Enterprise Security:
La gestione delle informazioni

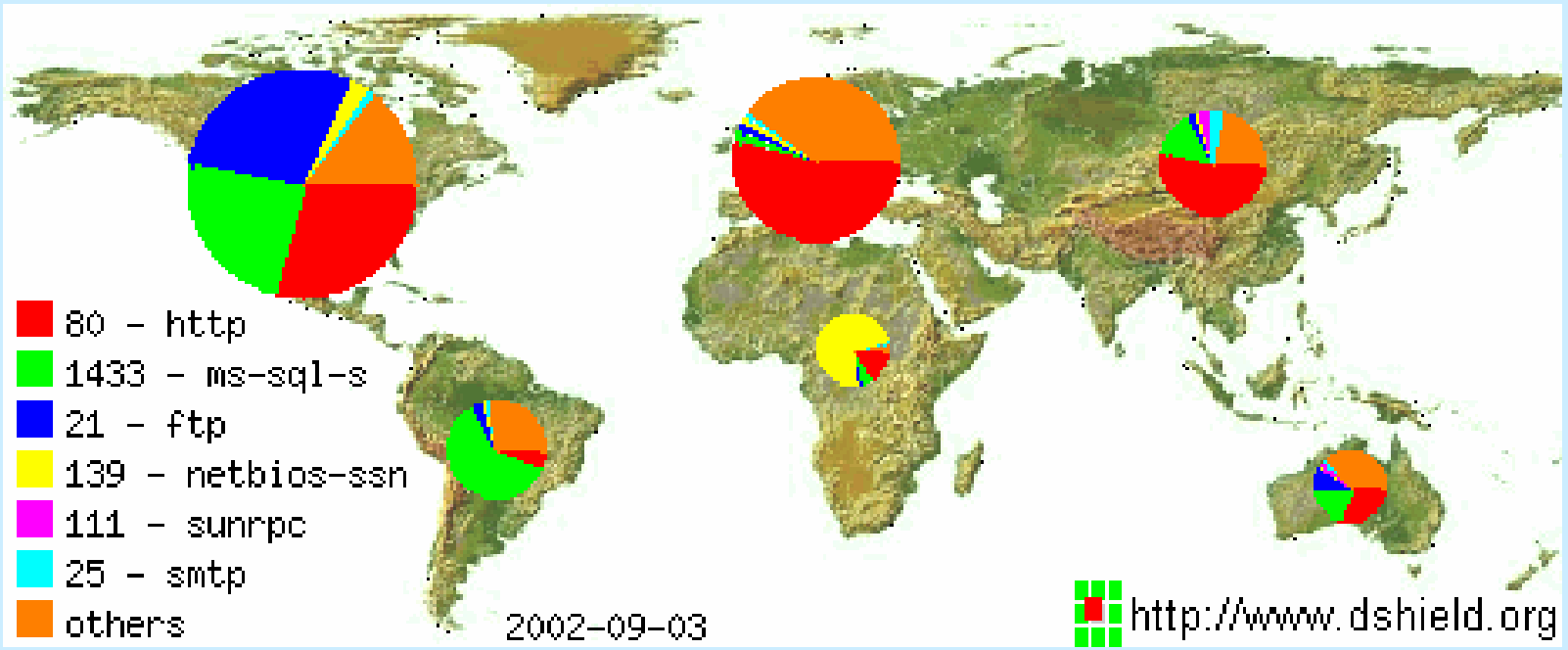
Massimo Cipriani
Consulting Manager – Technology Services
Computer Associates Italia S.p.a.
massimo.cipriani@ca.com

Internet Growth Trends

- 1977: 111 hosts on Internet
- 1981: 213 hosts
- 1983: 562 hosts
- 1984: 1,000 hosts
- 1986: 5,000 hosts
- 1987: 10,000 hosts
- 1989: 100,000 hosts
- 1992: 1,000,000 hosts
- 2001: 150 – 175 million hosts
- 2002: over 200 million hosts
- By 2010, about 80% of the planet will be on the Internet

Internet Society

Evoluzione dello scenario



"The Morris Worm" *(November 1988)*

...security works in an era of (computer) worms that can sprea
across the Internet in 10 minutes"

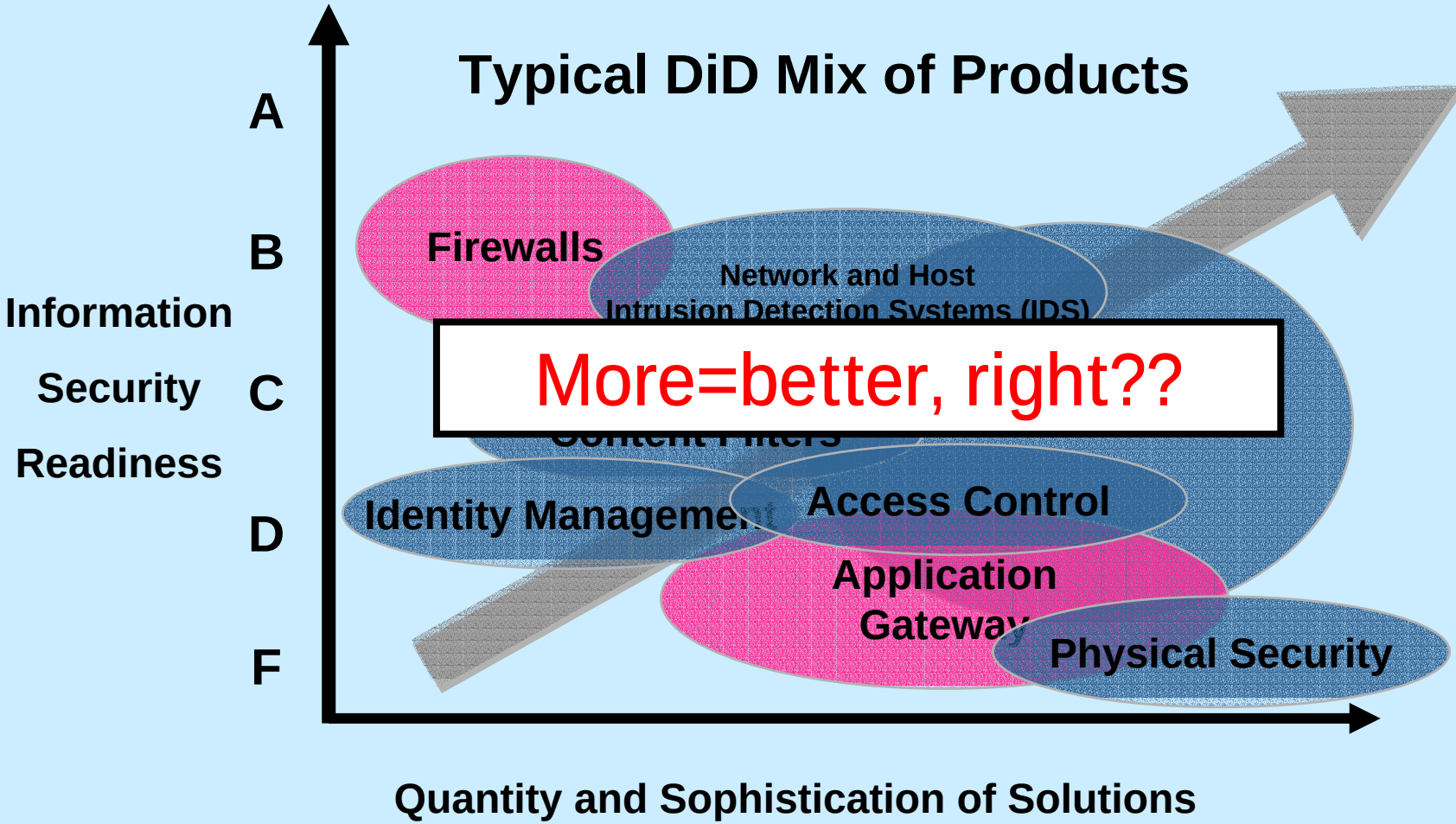
(Bruce Schneier - IEEE S&P, July/August 2003)

Le contromisure

- Router: filtraggio pacchetti (IP Spoofing)
- Firewall (Stateful Packet Inspection)
- Antivirus
- IDS (HIDS, NIDS, KIDS)
- Crittografia
- VPN
- ...

Ognuna di queste soluzioni ha il suo sistema di event e alert management, oltre a differenti sistemi di reporting.

The Theory of “Defense in Depth” (DiD)



Current State Of Information Security: Information Overload


Security information overload


Complex services and new technologies

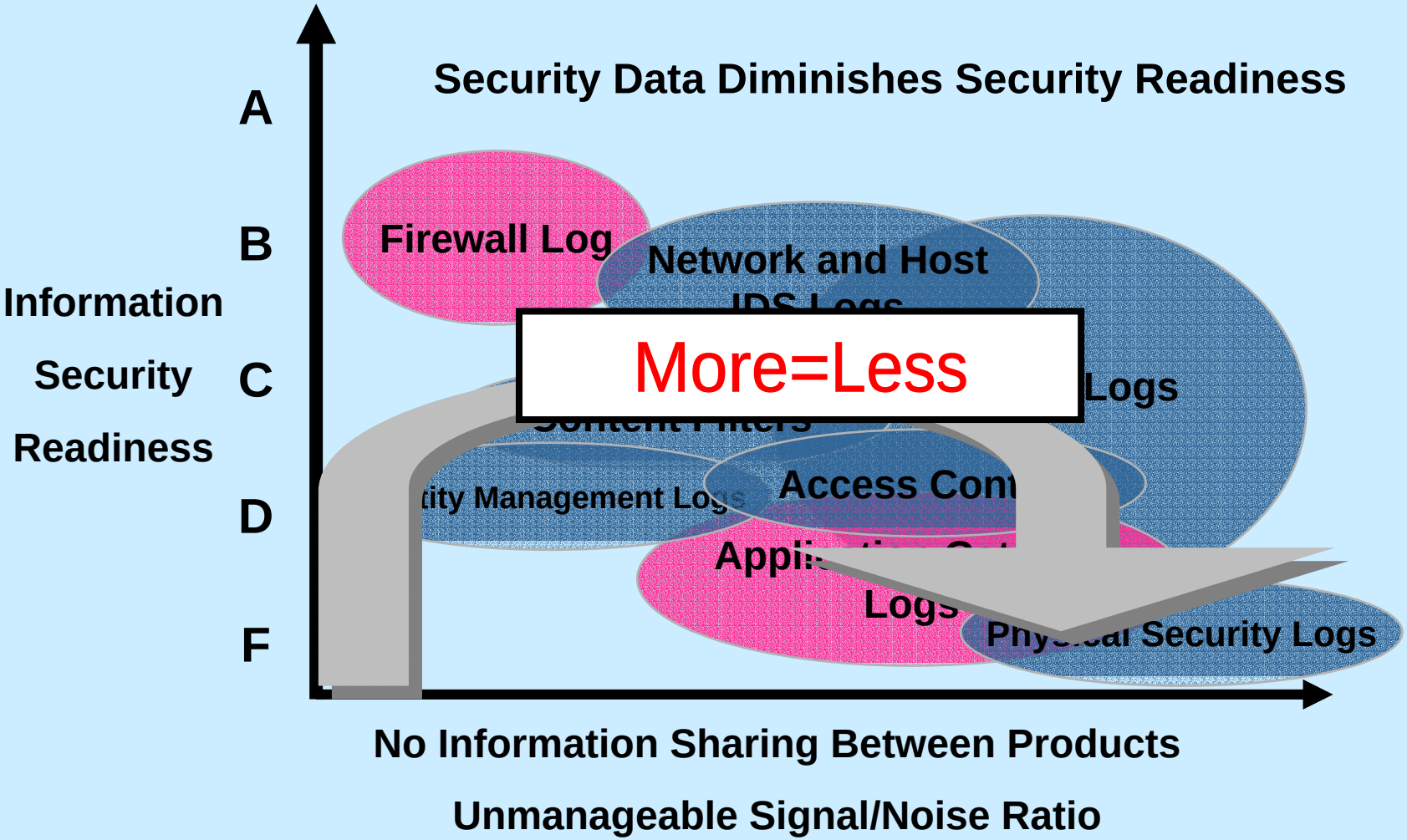
"I have 1.3 million events a day – I need more than a GUI that will display these. I need to see only what's important without saturating my network."

Increa

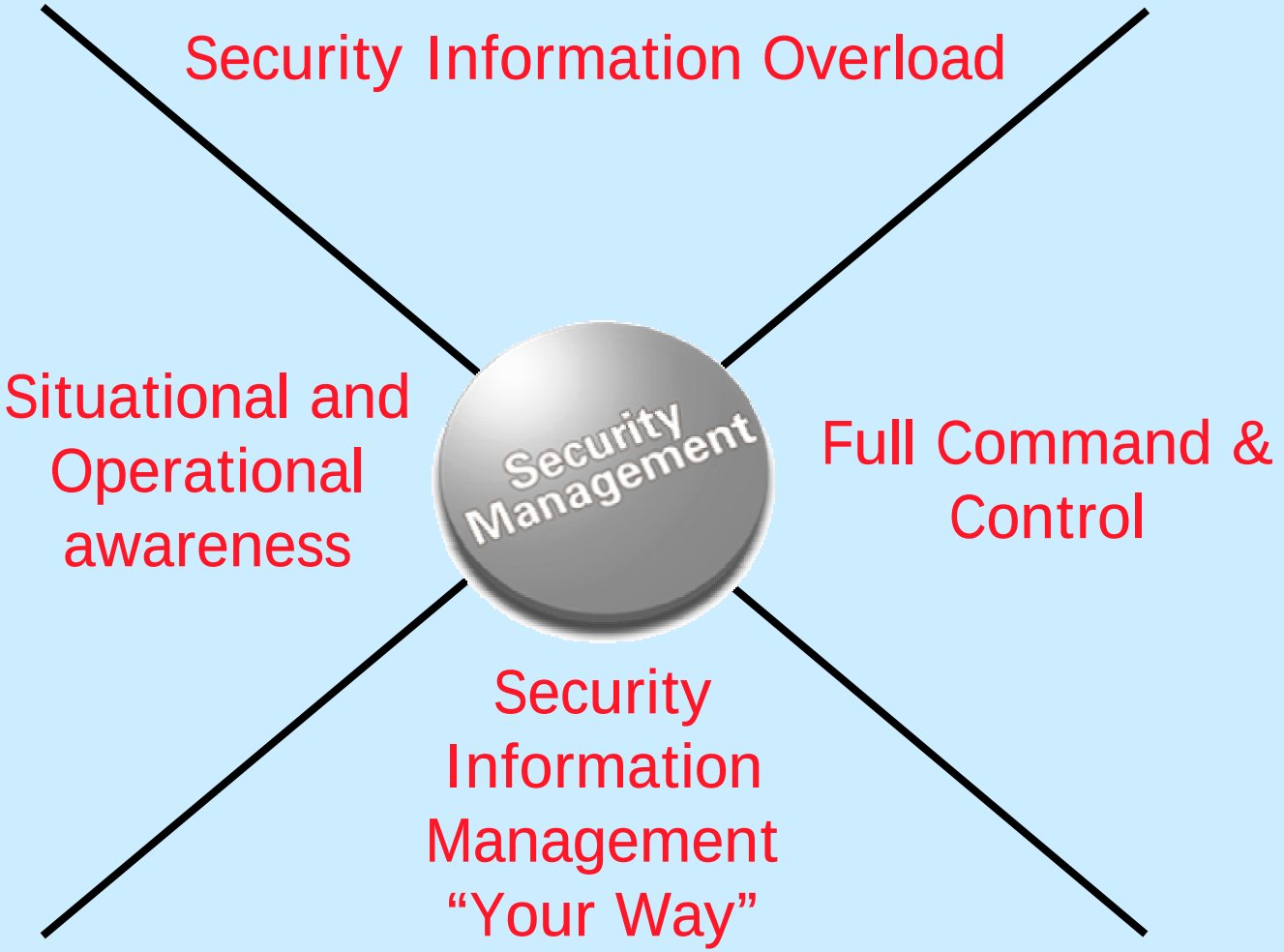
ystems


Integrating a variety of platforms and vendors


The Reality of “Defense in Depth”



I problemi dell'Enterprise Security Information Management



Le conseguenze

Per i Security Administrator:

- Necessità di analizzare moli di dati eterogenei provenienti da una molteplicità di fonti diverse, basati su protocolli differenti (Syslog, OPSEC, SNMP, Event Log, ecc.) ;
- Difficoltà di discriminare i “Falsi Positivi” dei FW e degli IDS;
- Difficoltà di riconoscimento dello stesso evento rilevato da dispositivi differenti;
- Difficoltà di mettere in relazione i dati ed estrarre informazioni rilevanti, ai fini del riconoscimento di un attacco.

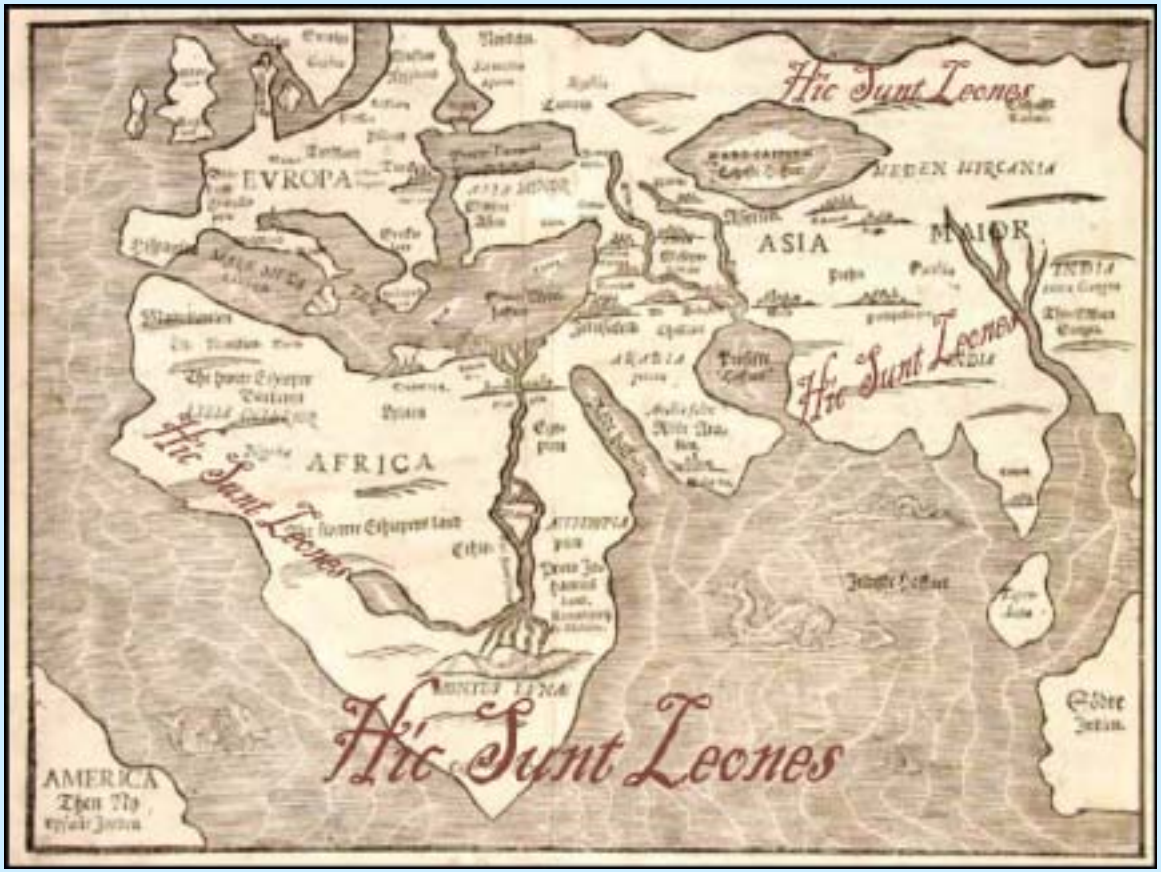
Cosa accade dei dati nativi di auditing ?

TURNED ON	TURNED OFF
So much data is created that important events can't be found. **Auditors use different tools for each environment.**	**No data.** 
Organizations don't know what's happening on their systems.	

“Prevention is ideal but detection is a must”

(SANS Institute)

Da chi bisogna difendersi?



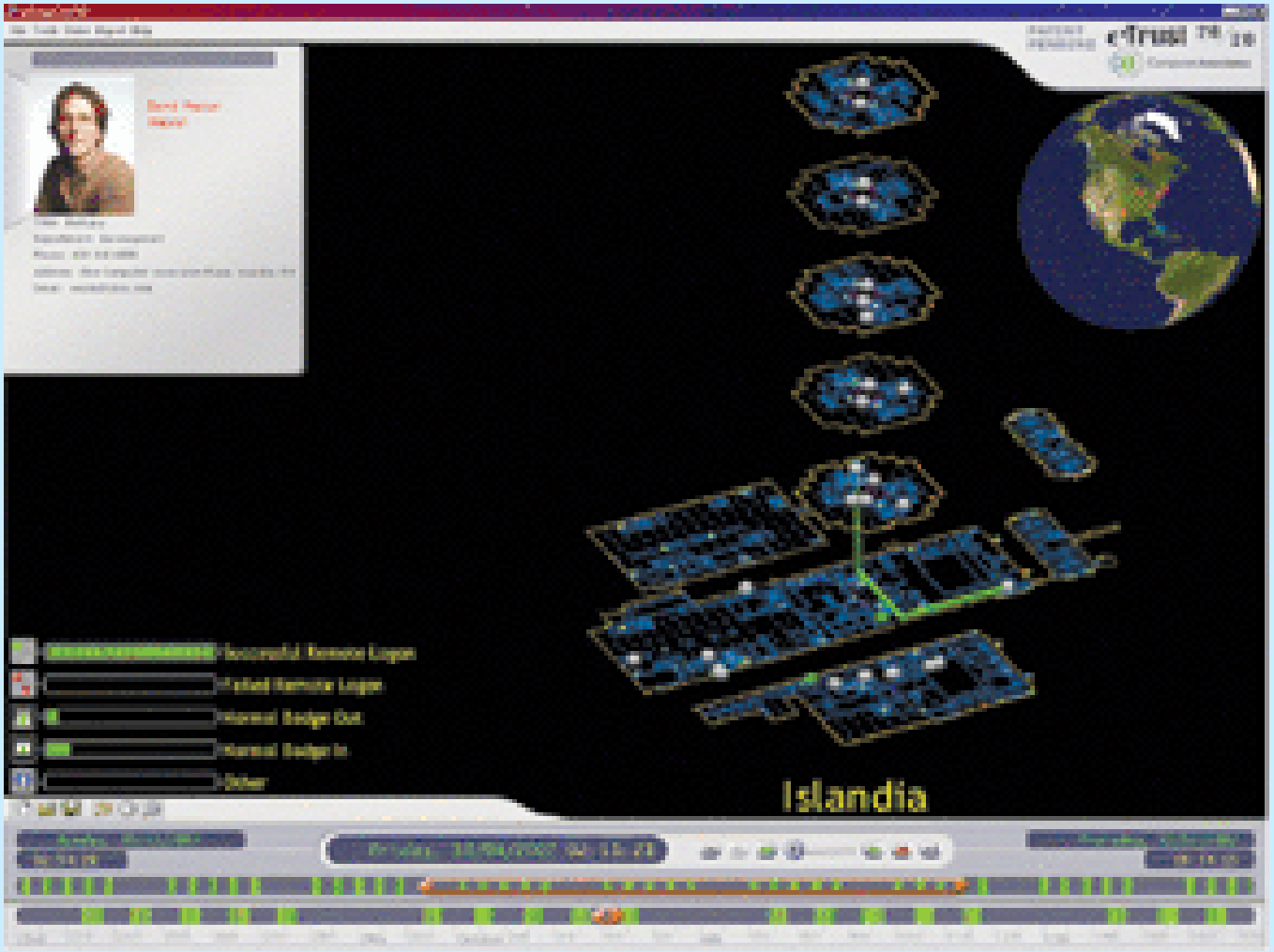
Le questioni aperte

- Probabili fonti di Attacchi – Utenti interni “scontenti”?
- Perdite Finanziarie - Utilizzo improprio (abuso) degli accessi alla Rete ?
- Incidenti per accessi interni non autorizzati?
- Conformità alle normative?
- Capacità di riconoscimento di un attacco?

I numeri

- 90% - Probabili fonti di Attacchi – Utenti interni “scontenti”
- 70% - Perdite Finanziarie - Utilizzo improprio (abuso) degli accessi alla Rete
- 55% - Incidenti per accessi interni non autorizzati
- 48% - Mancanza di conformità alle normative
- 33% - Incapacità di riconoscimento di un attacco

Convergenza tra Sicurezza Fisica e Logica



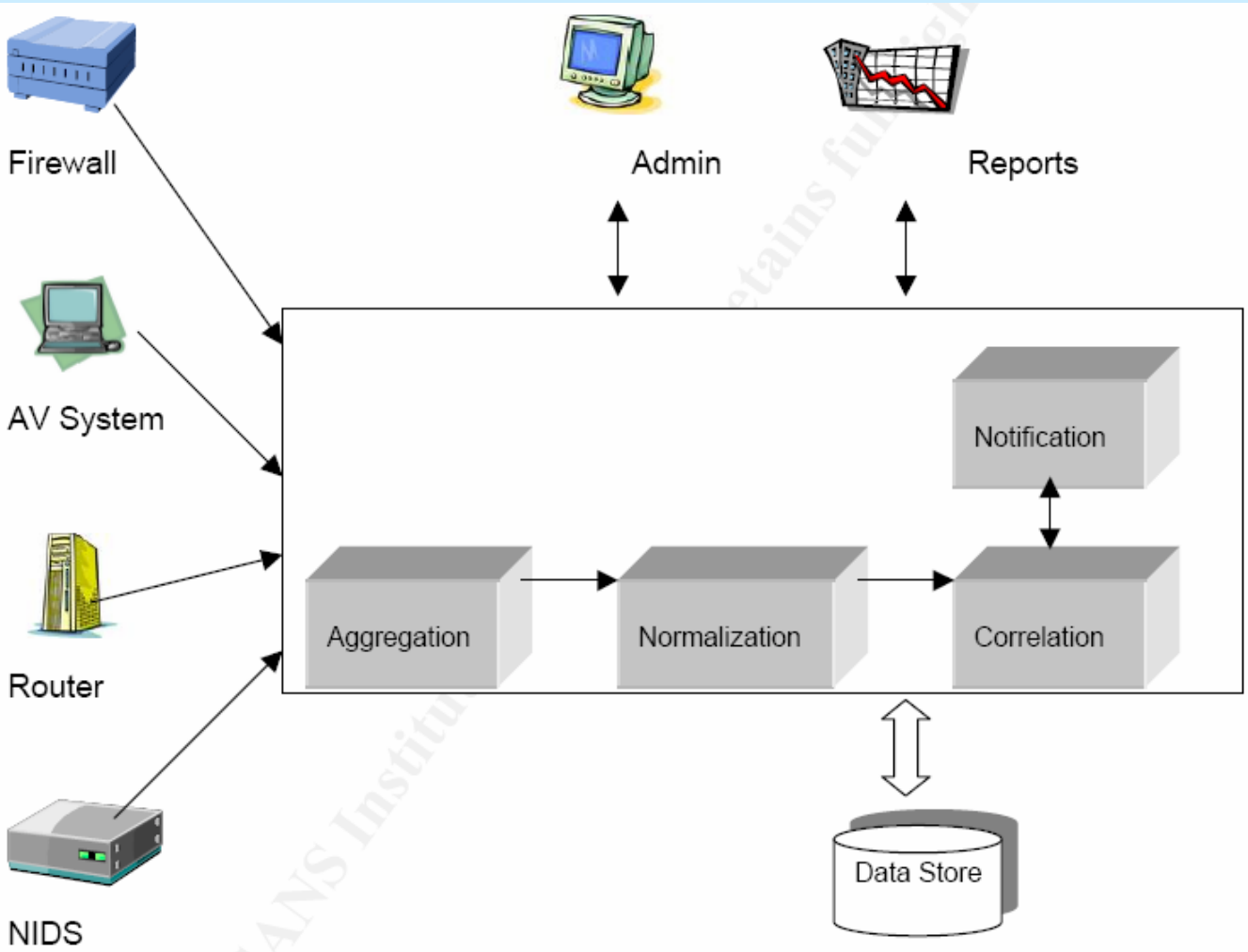


Figure 1: Enterprise Security Information Management (ESIM) Architecture

Fonte:SANS Institute 2003

Sistema di Enterprise Security Information Management

Componenti architetturali

- Agenti
- Motore di analisi
- Data Store
- Management Console
- Report

Sistema di Enterprise Security Information Management

Agenti

Raccolgono informazioni sulle attività in rete o sui sistemi.

Possono interfacciare i Log file o ricevere gli eventi direttamente dai dispositivi.

Ruotano gli eventi al server centrale di Management.

Sistema di Enterprise Security Information Management

Motore di analisi

E’ il componente critico e centrale del sistema che realizza le funzioni di:

- Aggregazione
- Normalizzazione
- Correlazione
- Notifica

Sistema di Enterprise Security Information Management

Data Store

Rappresenta il Repository centrale delle informazioni.

Consente analisi Real-time e produzione di report

Sistema di Enterprise Security Information Management

Management Console

- Permette la definizione delle policy.
- Consente la vista centralizzata dell'intero sistema.
- Rappresenta il punto di raccolta degli allarmi.
- Permette l'aggiornamento automatico dei pattern/signature.

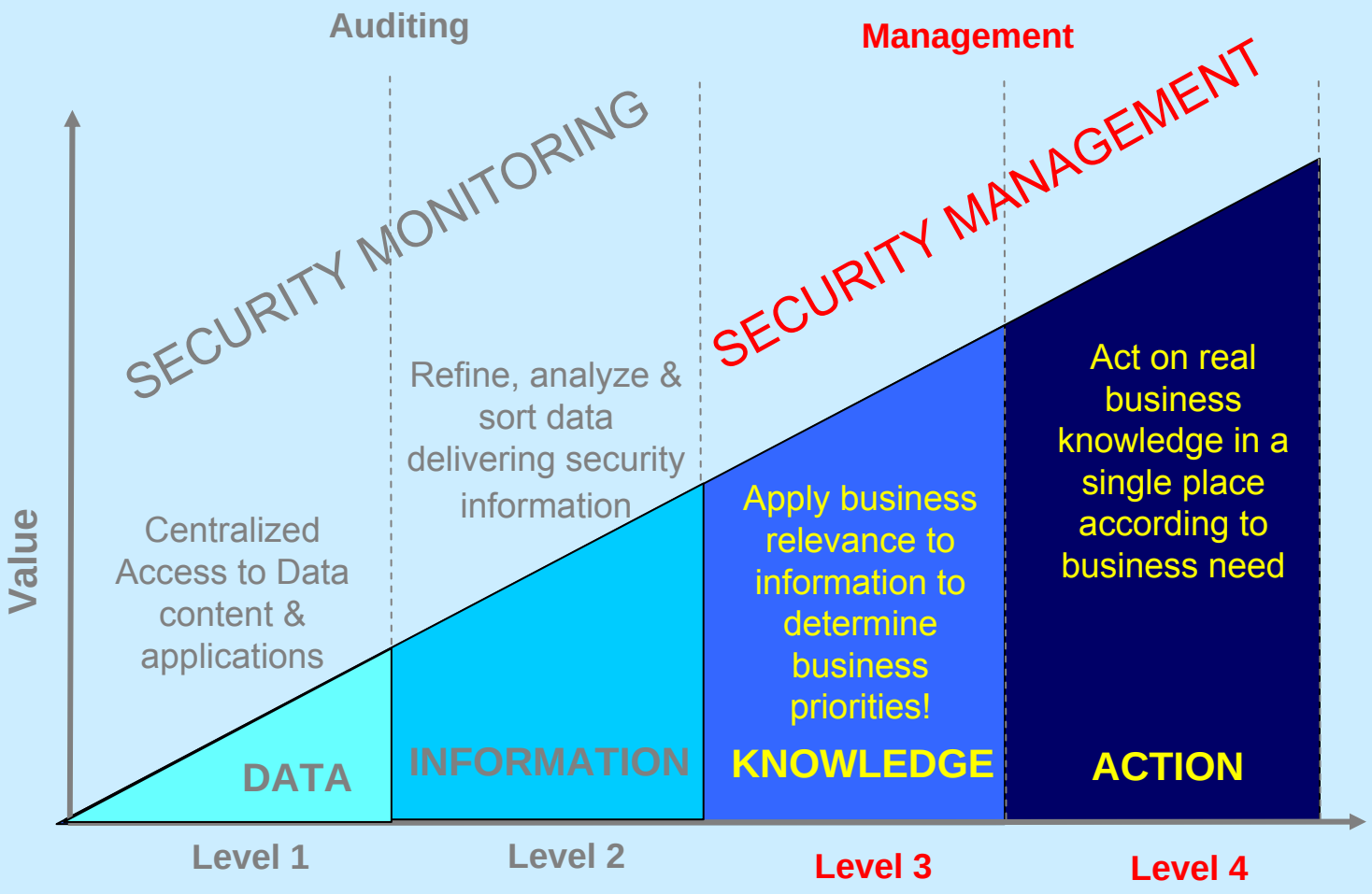
Sistema di Enterprise Security Information Management

Report

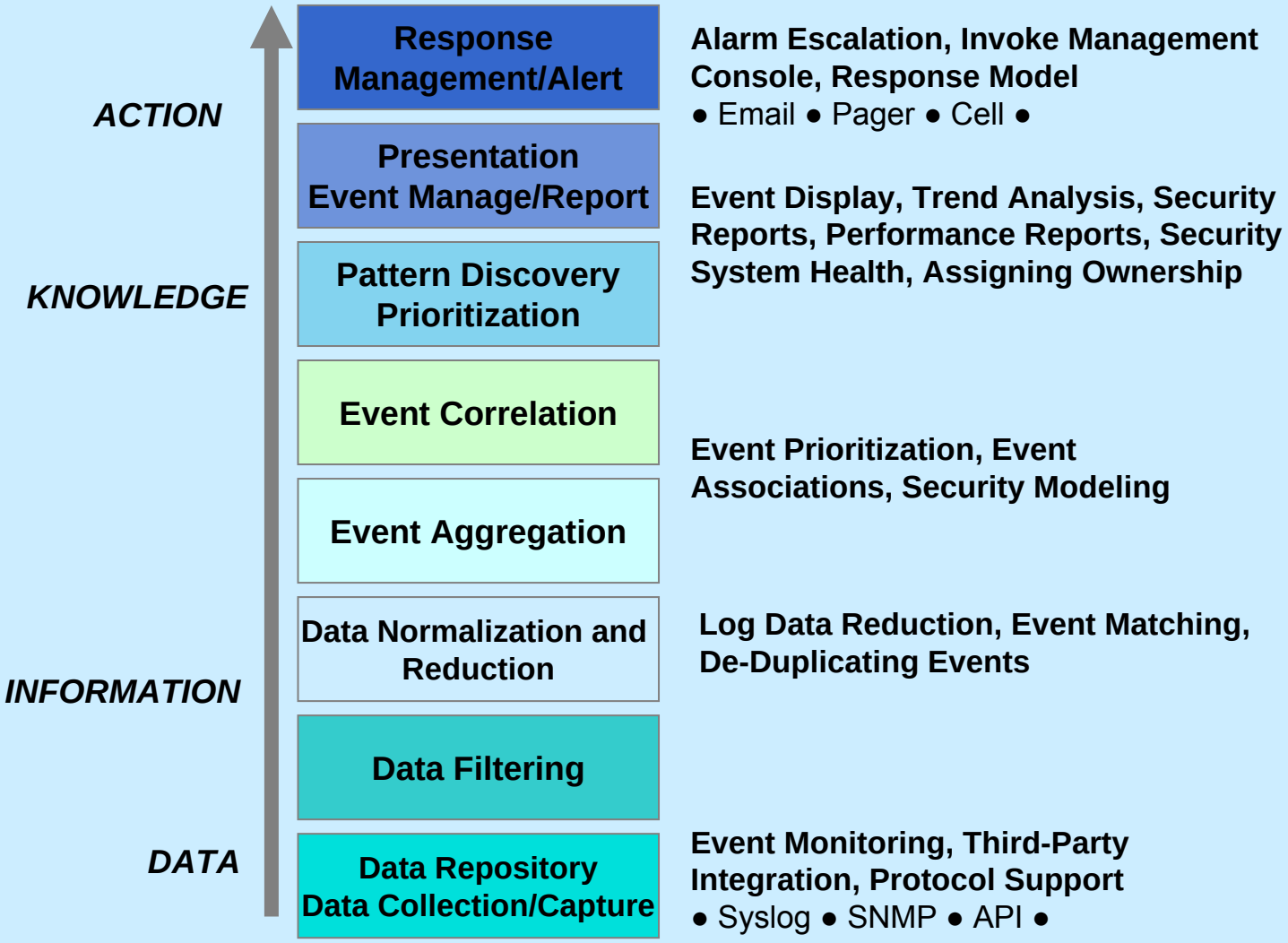
La sicurezza è un processo continuo non una soluzione definitiva.

I Report vengono generati per comprendere i trend degli eventi e per rappresentare il livello di Security al management dell'organizzazione

Information Delivery Maturity Level



Enterprise Security Information Management: Data Hierarchy

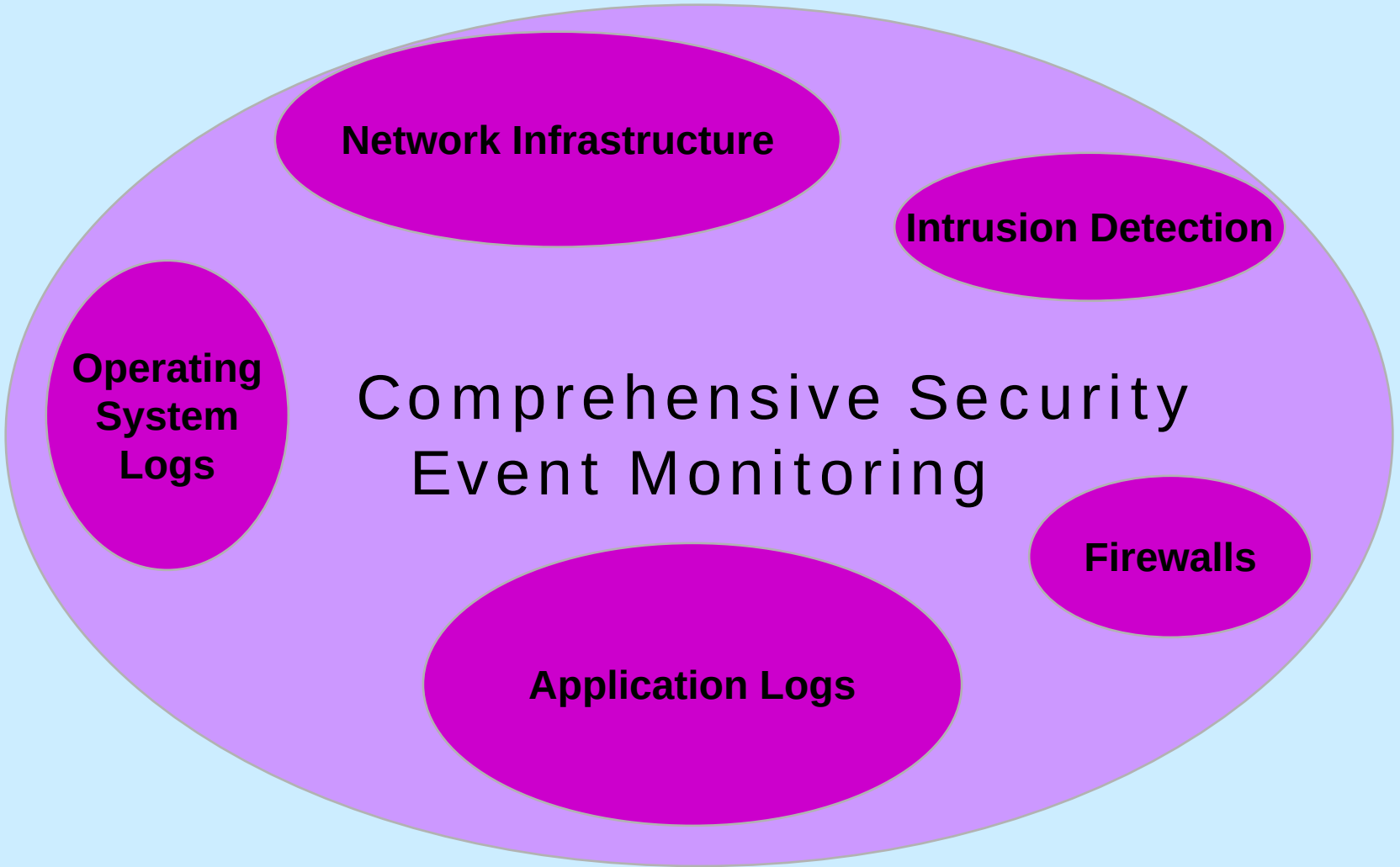


Sicurezza tra processo e tecnologie

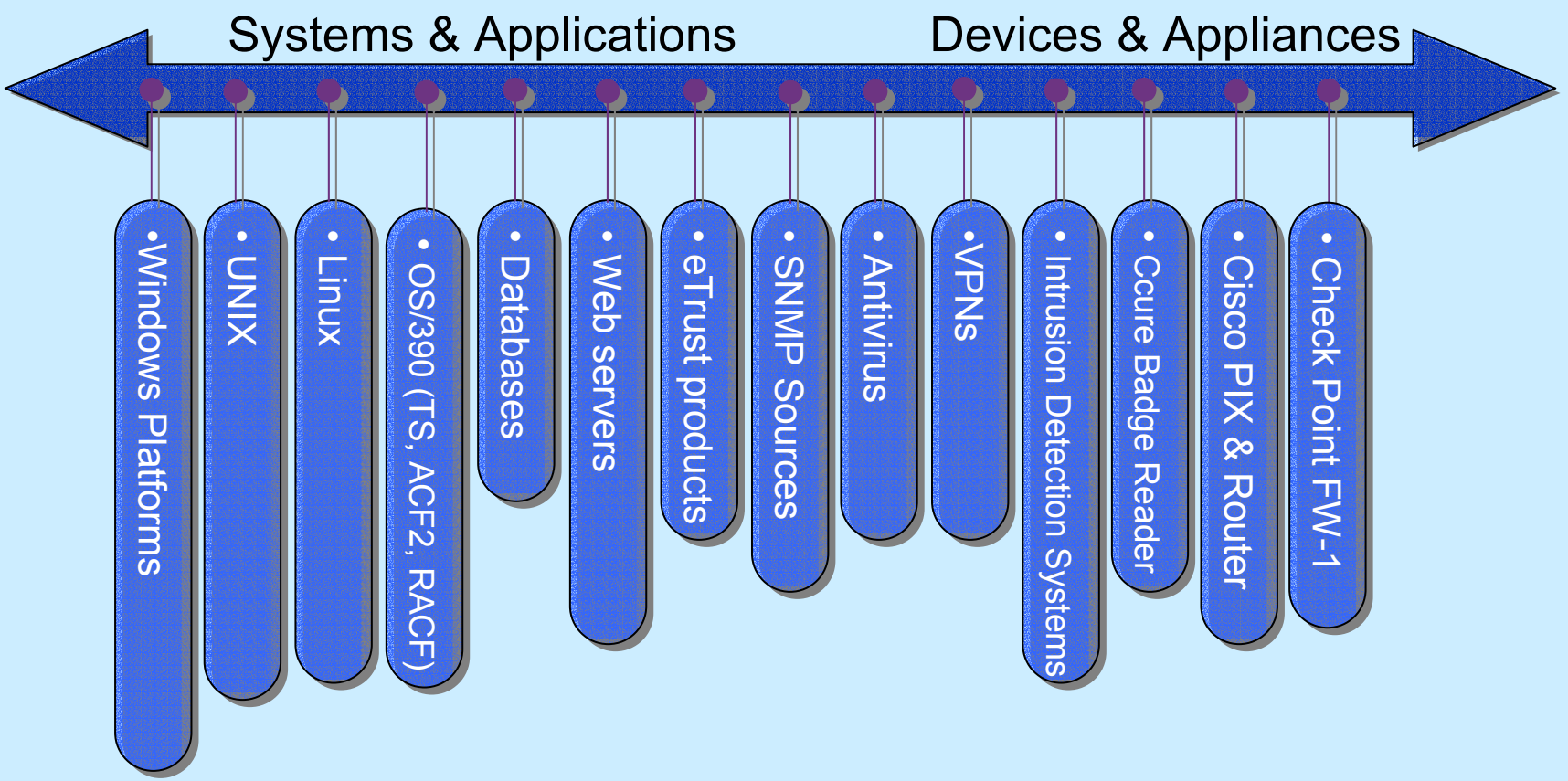
- “La sicurezza è un processo, non un prodotto”
  Bruce Schneier

- La sicurezza è un processo che coinvolge le tecnologie, le persone, le organizzazioni, ma non c’è sicurezza senza tecnologie

I requisiti di un sistema di gestione delle informazioni di Enterprise Security



End-to-end Security Monitoring



Broad Coverage of Security Technologies

Il numero di eventi è dato da:

SOLUZIONI SICUREZZA

- Multiple AV Vendors
- Firewall
- VPN
- Access Control
- Web Access Control
- Intrusion Detection
- User Administration
- PKI
- Vulnerability Tools
- Alarms / Alerts

×

PIATTAFORME

- MS Windows 98
- MS Windows 2000
- MS Windows XP
- Linux
- Unix
- ZOS
- Embedded Systems

×

NUMERO DI

- Servers
- Gateway
- DesktopS
- PDAs
- Phones
- Mobile Handhelds

×

APP

- SAP
- Oracle
- Peoplesoft
- External
- Internal
- Shared

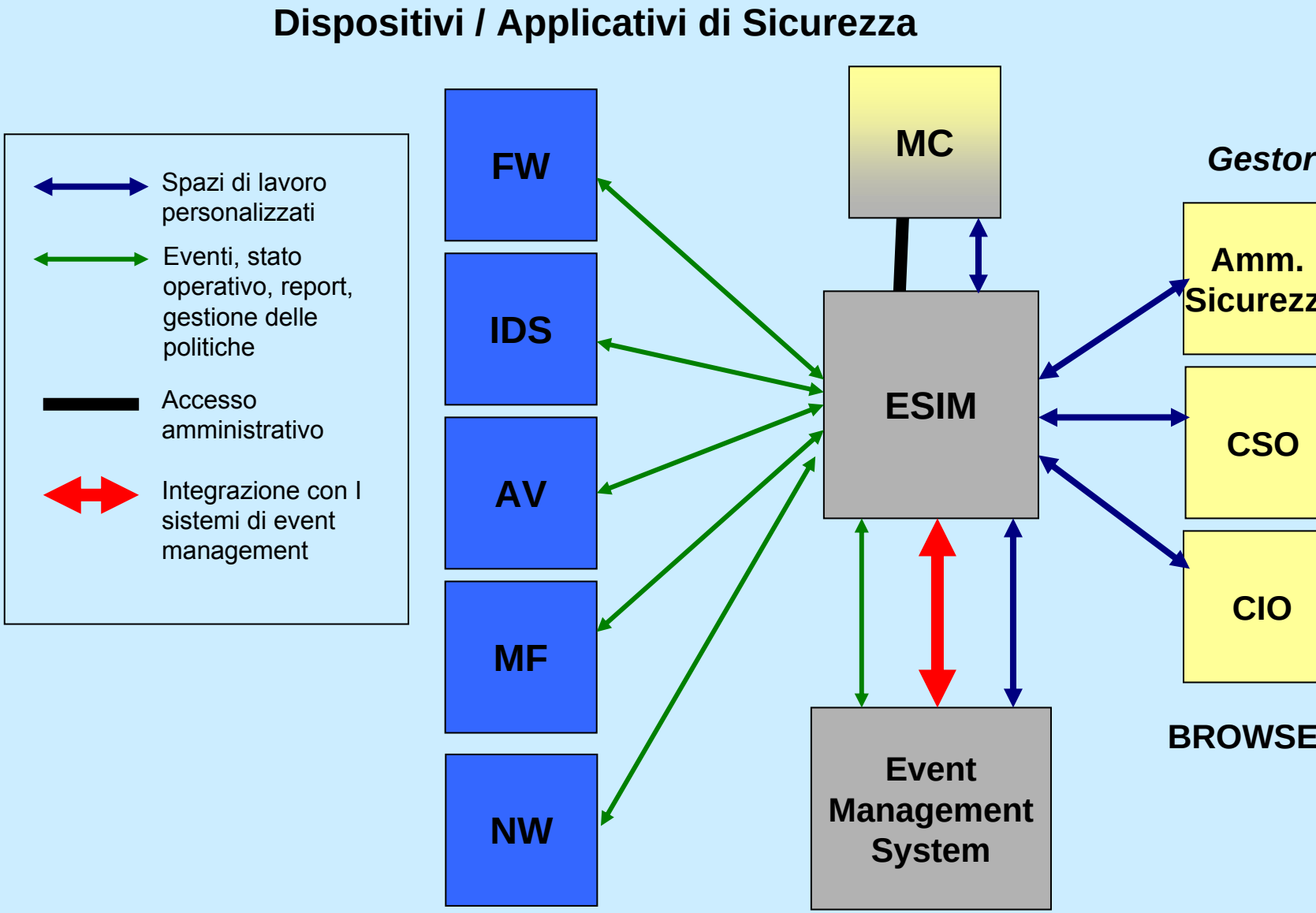
×

Numero Utenti

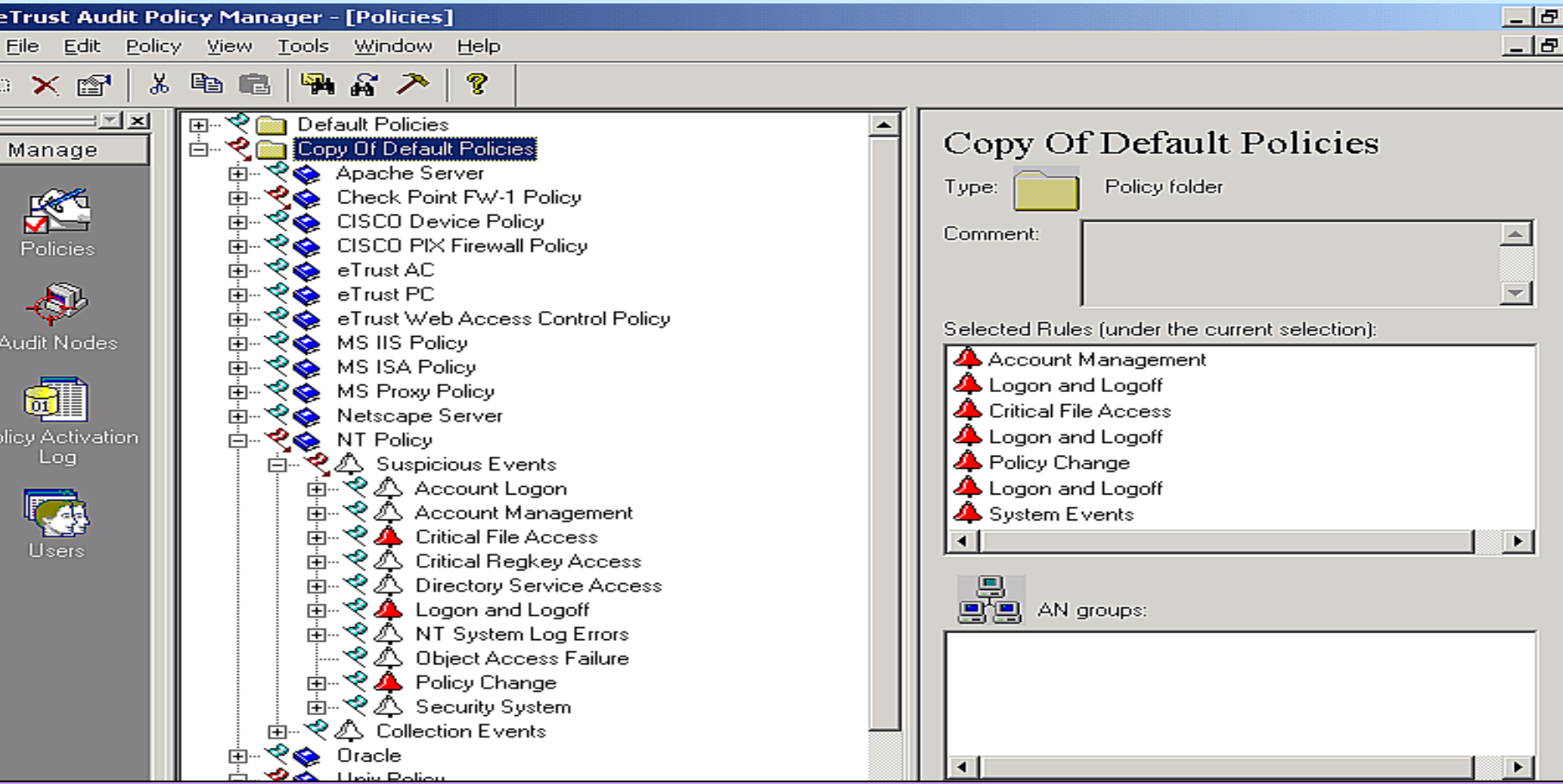
Enterprise Security Information Management : Caratteristiche Funzionali

- ❑ controllo centralizzato dei dati di auditing
- ❑ gestione centralizzata delle policy di auditing
- ❑ gestione degli eventi di sicurezza granulare, selettiva e su log separato
- ❑ sistema di sort, filtering e analisi sui dati di auditing
- ❑ sistema di correlazione degli eventi
- ❑ monitor centralizzato dello stato operativo dei sistemi di sicurezza
- ❑ profilazione degli utenti di amministrazione
- ❑ sistema di reporting centralizzato
- ❑ supporto nativo cross-platform, cross-protocol
- ❑ monitor degli incidenti integrabile con un sistema di gestione (help desk, system/network management)

Architettura di un Enterprise Security Information Management

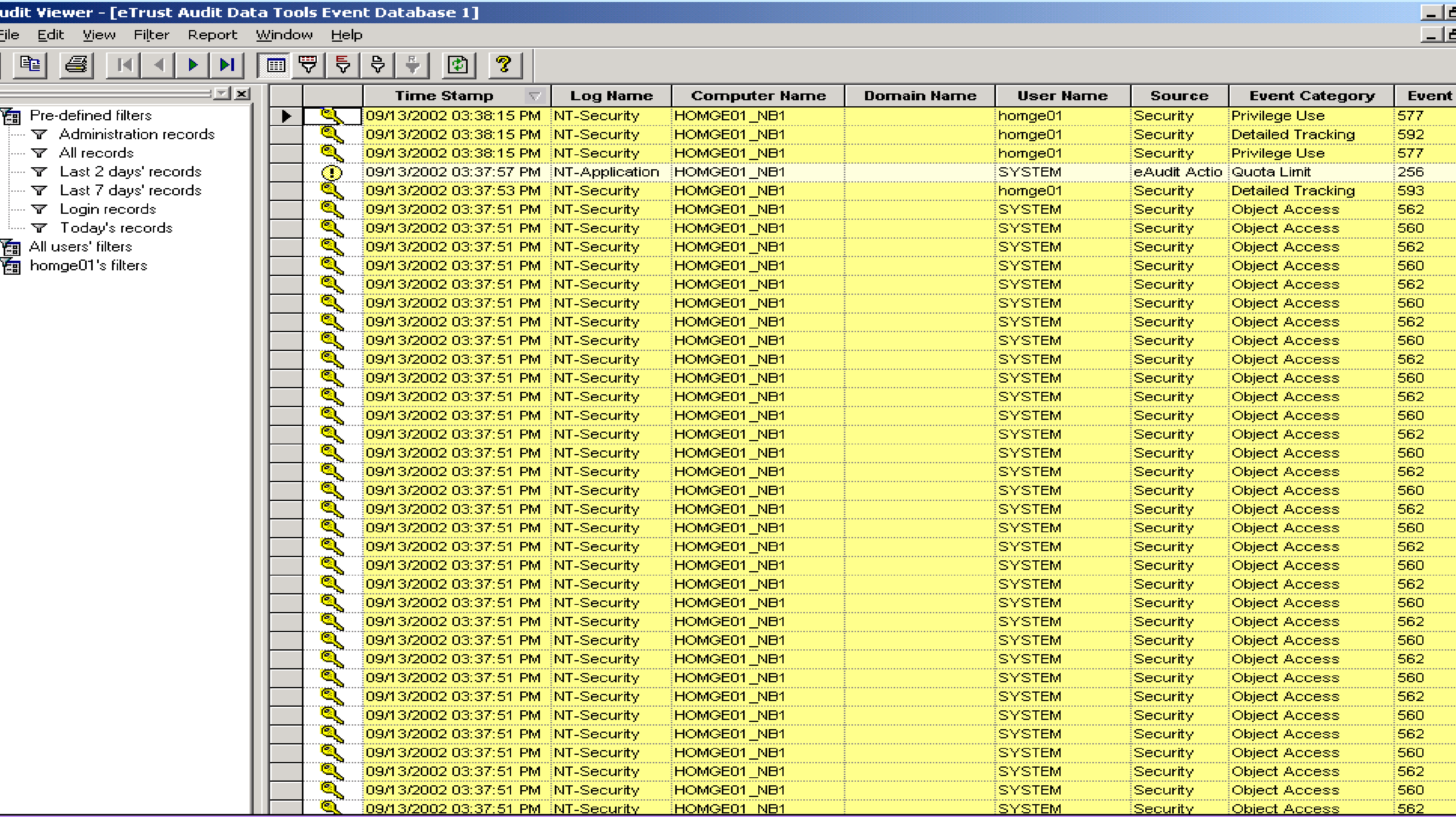


Centralized Security Event Policy Management



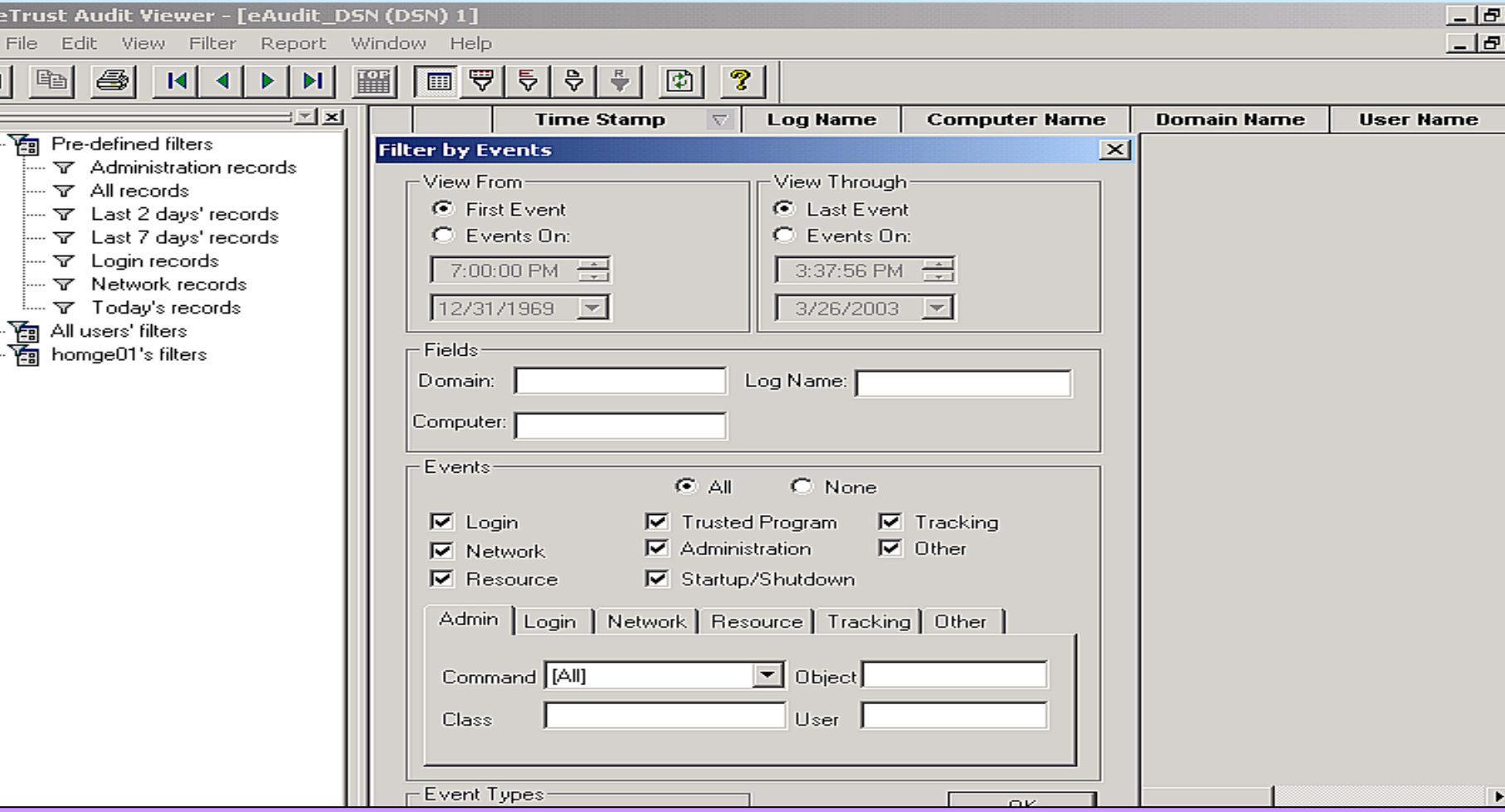
Predefined, customizable rules and policies

Audit Log Repository



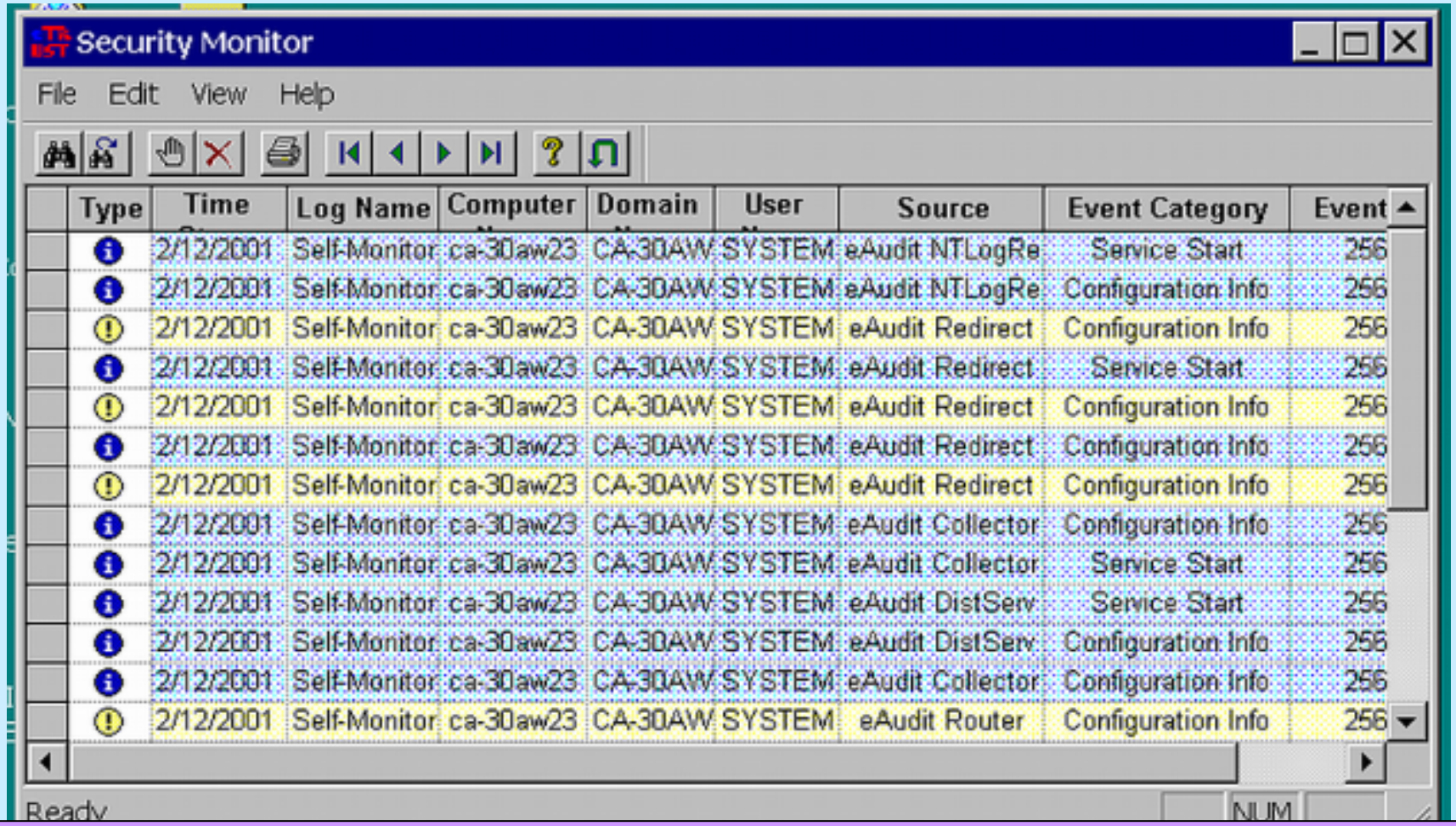
Database-driven querying

Versatile Filtering



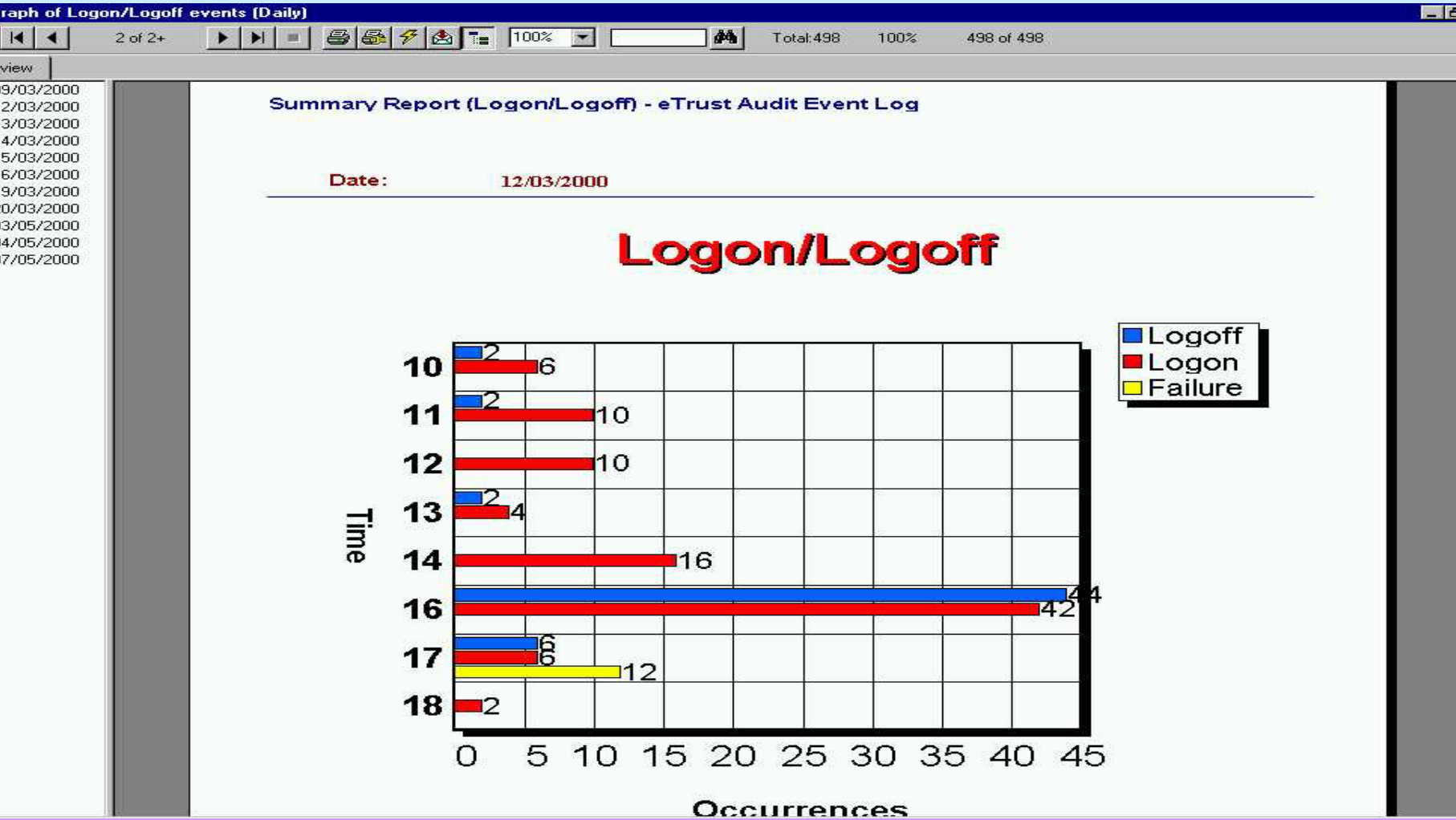
Multi-layered Filtering and data reduction of Security Events

Continuous Security Monitoring



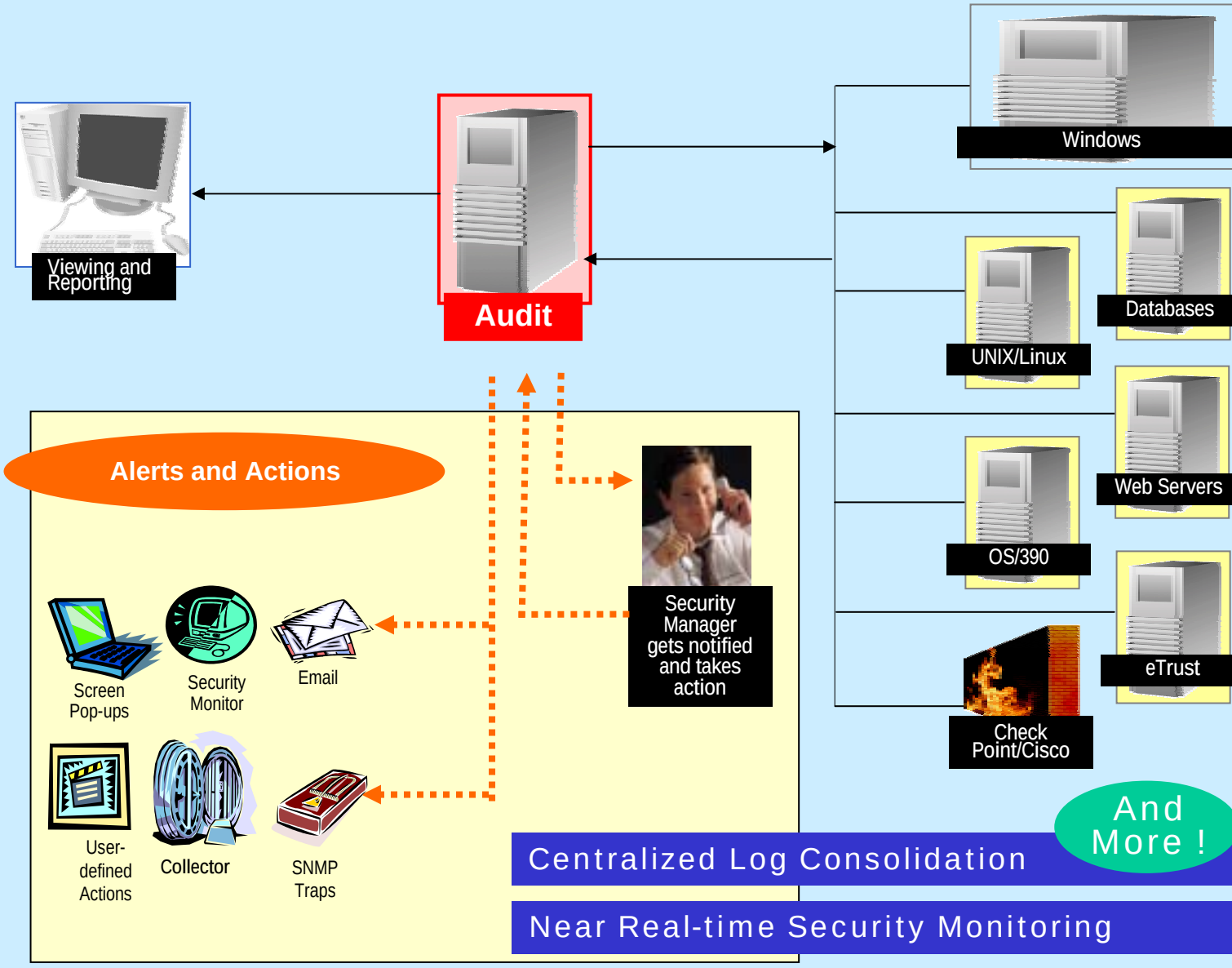
Near real-time monitoring,attack detection and alerting

Robust Reporting



Predefined, Customizable, Detailed, Graphical

Esempio di gestione degli eventi



Esempio di gestione degli eventi

Audit

Windows

Databases

UNIX/Linux

Web Servers

OS/390

eTrust

Check Point/Cisco

Alerts and Actions

Security Manager gets notified and takes action

Screen Pop-ups

Security Monitor

Email

User-defined Actions

Collector

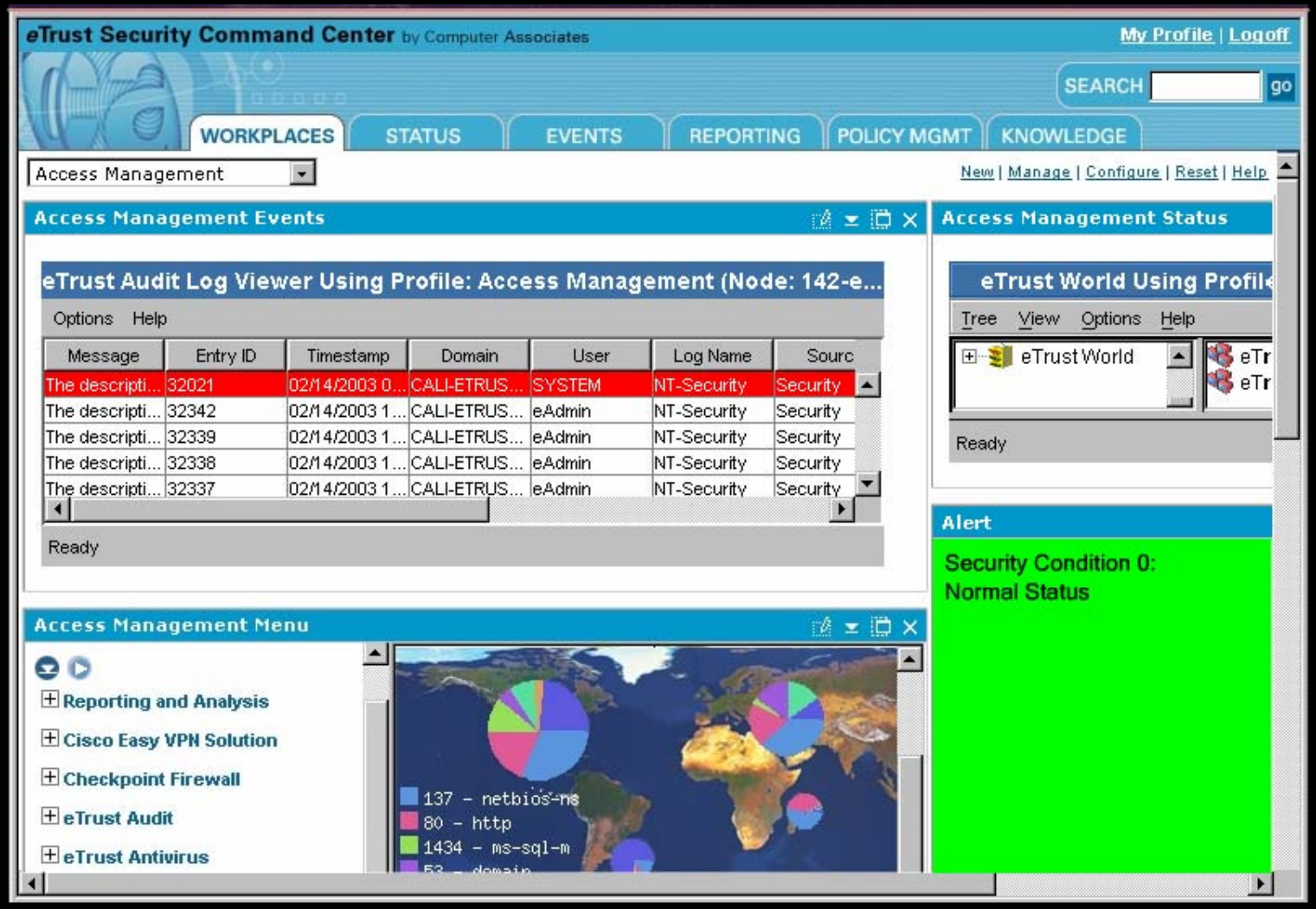
SNMP Traps

And More !

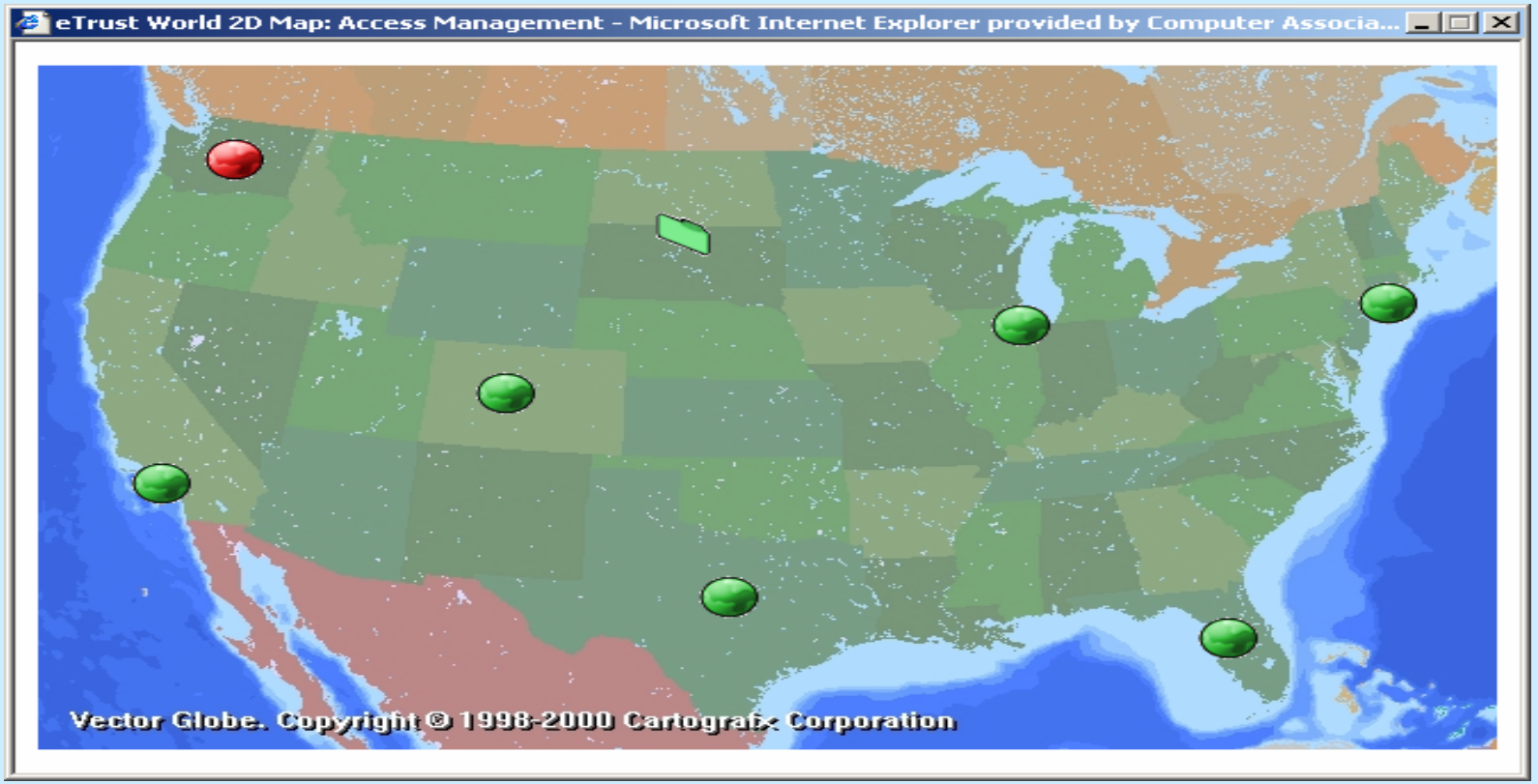
Total Security Management

Real-Time Audits and Views

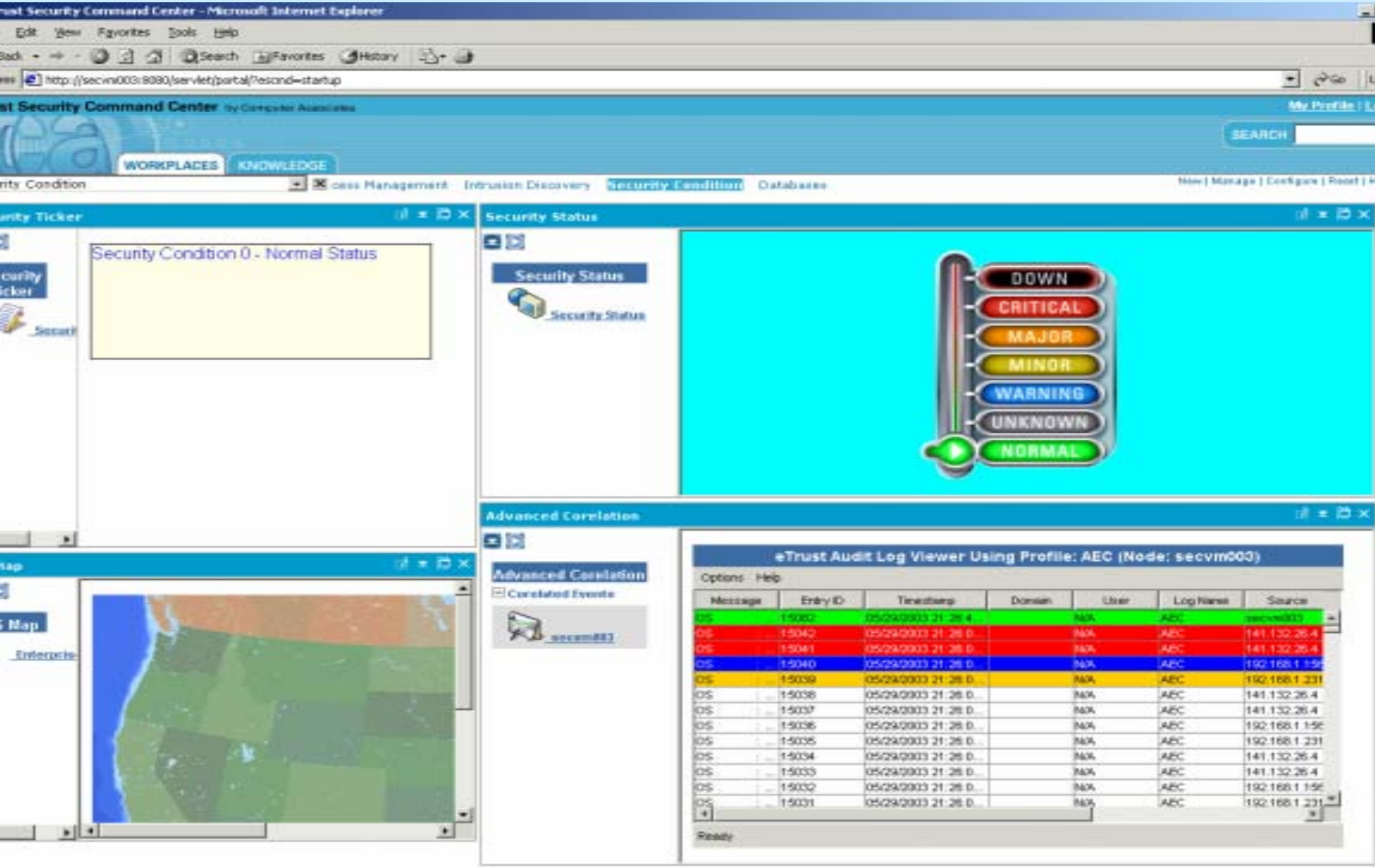
*e*Trust Security Command Center



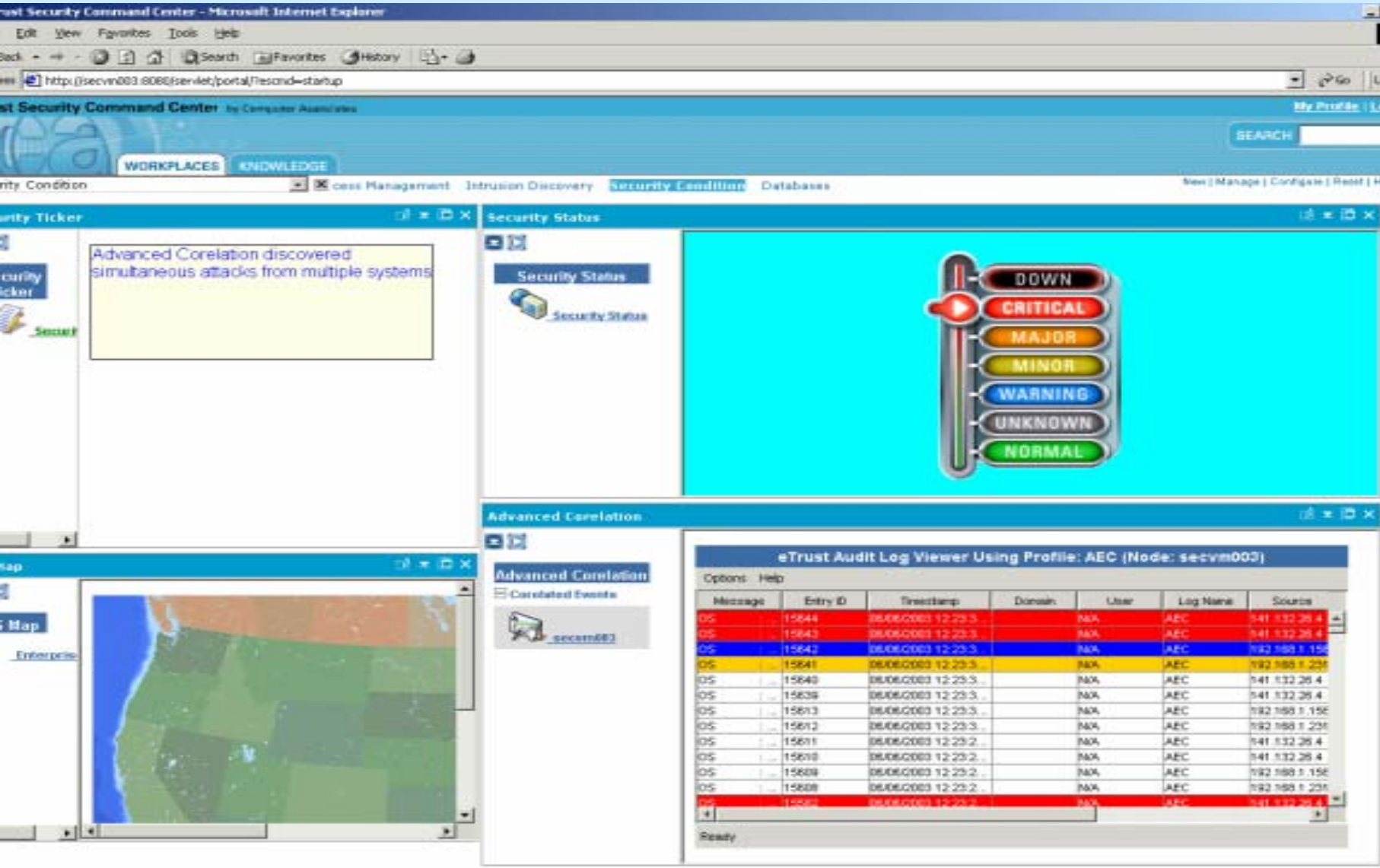
Status By Location



Security Condition- Normal



Security Condition- Critical



MORE SECURITY DOESN'T MAKE YOU MORE SECURE.

BETTER MANAGEMENT DOES.

The secret to a secure enterprise lies in not just monitoring the parts, but managing it as a whole. That's exactly what *e*Trust™ lets you do. In fact, our *e*Trust™ Security Command Center is the perfect solution to security information overload. It gives you the big picture from a single vantage point, with all your event information prioritized. So you can identify actual internal and external threats before they can wreak havoc. Anything less would be, well, alarming. For more information on security management, go to ca.com/etrust/management.

*e*Trust™ | ACCESS • THREAT • IDENTITY SECURITY MANAGEMENT SOFTWARE | Computer Associates®

Bibliografia

1. Sridhar, Juvvadi. “ Requirements For Managing Security Information Overload”. 20 June 2003.
http://www.sans.org/rr/papers/index.php?id=1147

2. Boettger, Larry. “The Morris Worm: how it Affected Computer Security and Lessons Learned by it”. 24 December 2000.
http://www.giac.org/practical/gsec/Larry_Boettger_GSEC.pdf