

# Security Management Under Control Computer Associates

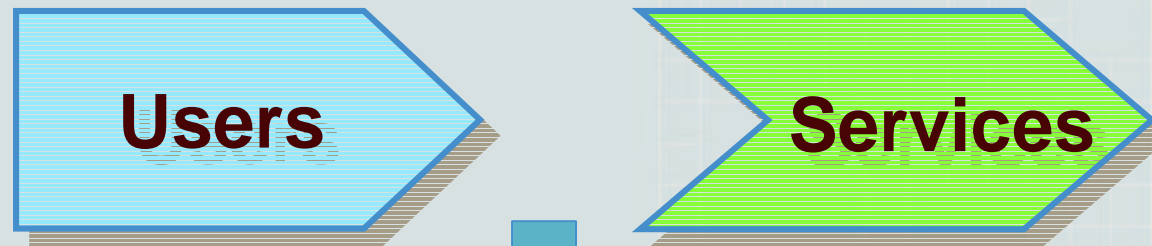
The eTrust logo is displayed in a white rectangular box. The word "eTrust" is written in a bold, dark red, sans-serif font. A small "TM" trademark symbol is positioned to the upper right of the word. The background of the box is white with a faint, light-colored grid pattern.

**eTrust™**

# Introducing The eTrust Solution



# The Business Goal



**Transactions**

# Security : The New Realities

- In order to connect users to services
  - Security must shift to enablement
  - A cultural shift - Security is everyone's business
  - Complexity of tools poses new management challenges
  - Legal and industrial regulations
    - Romania - Romanian Government NO. 611/2000; In accordance with law no. 233/2001
    - EU – privacy and spam directive
    - Industrial - Basel II Accord

# The User Challenge

- Who are the right users?
- How do you identify them?
- How do you manage outside users?
- How do you grant them appropriate access?
- How do you achieve this at business speed, and at lowest cost?

# eTrust Identity and Access Management



**eTrust Admin**

**eTrust Access Control**

**eTrust Single Sign-on**

**eTrust Web Access Control**

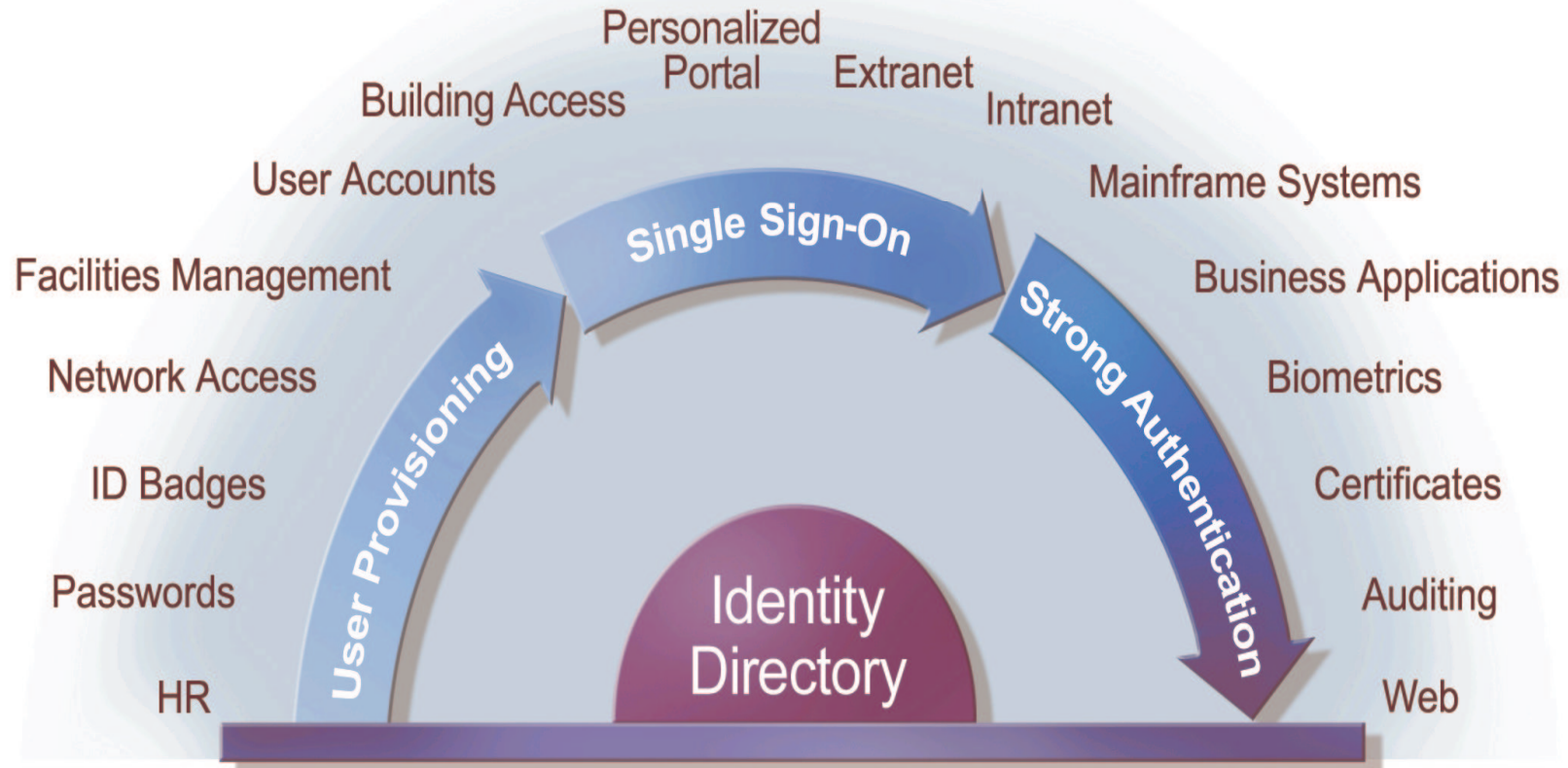
***Identity Infrastructure***

**eTrust Directory**

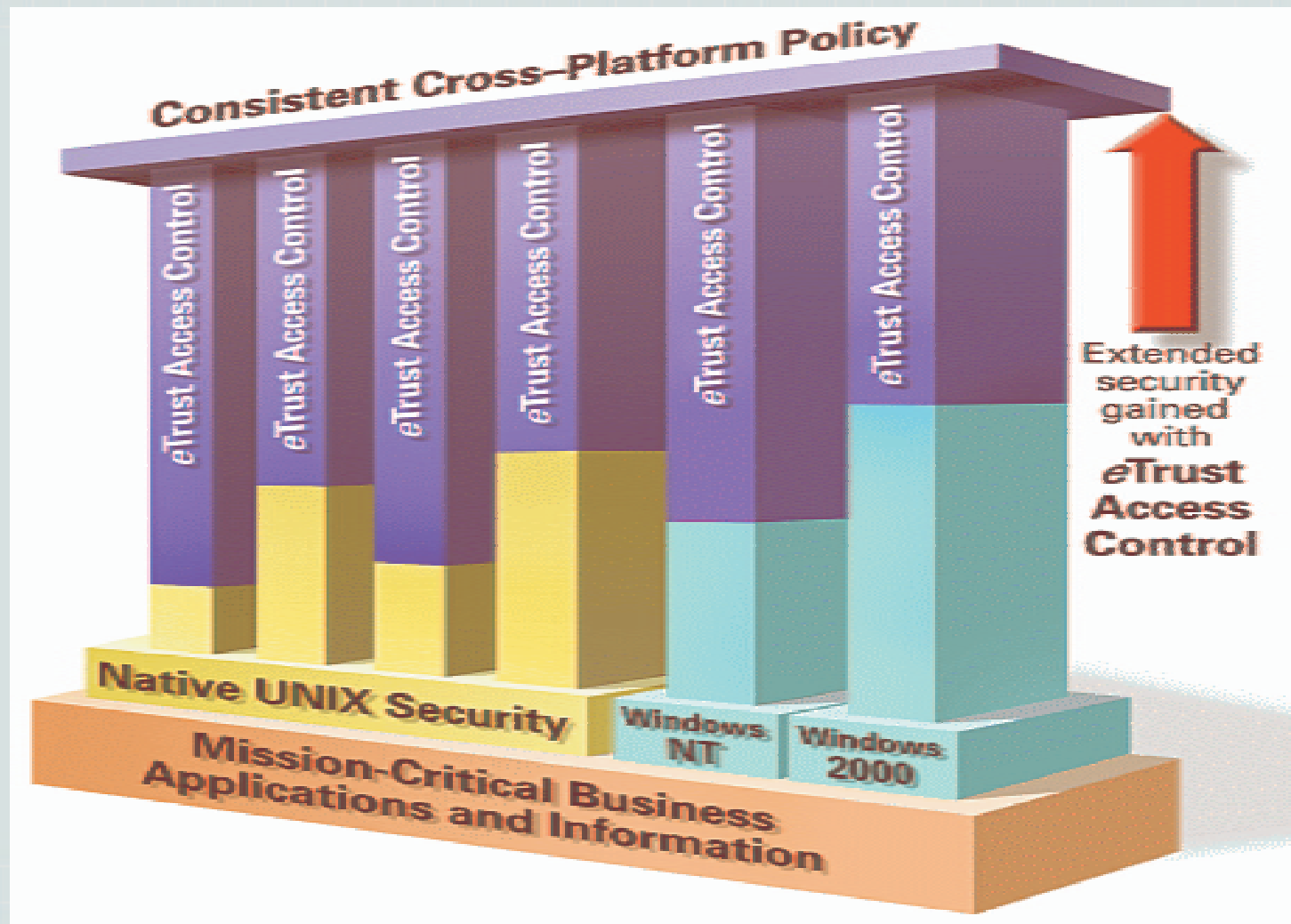
**eTrust PKI**

**eTrust OCSPPro**

# eTrust Identity Management



# eTrust Access Management



# eTrust Threat Management

**eTrust Antivirus**

**eTrust Secure Content  
Management**

**eTrust Intrusion  
Detection**

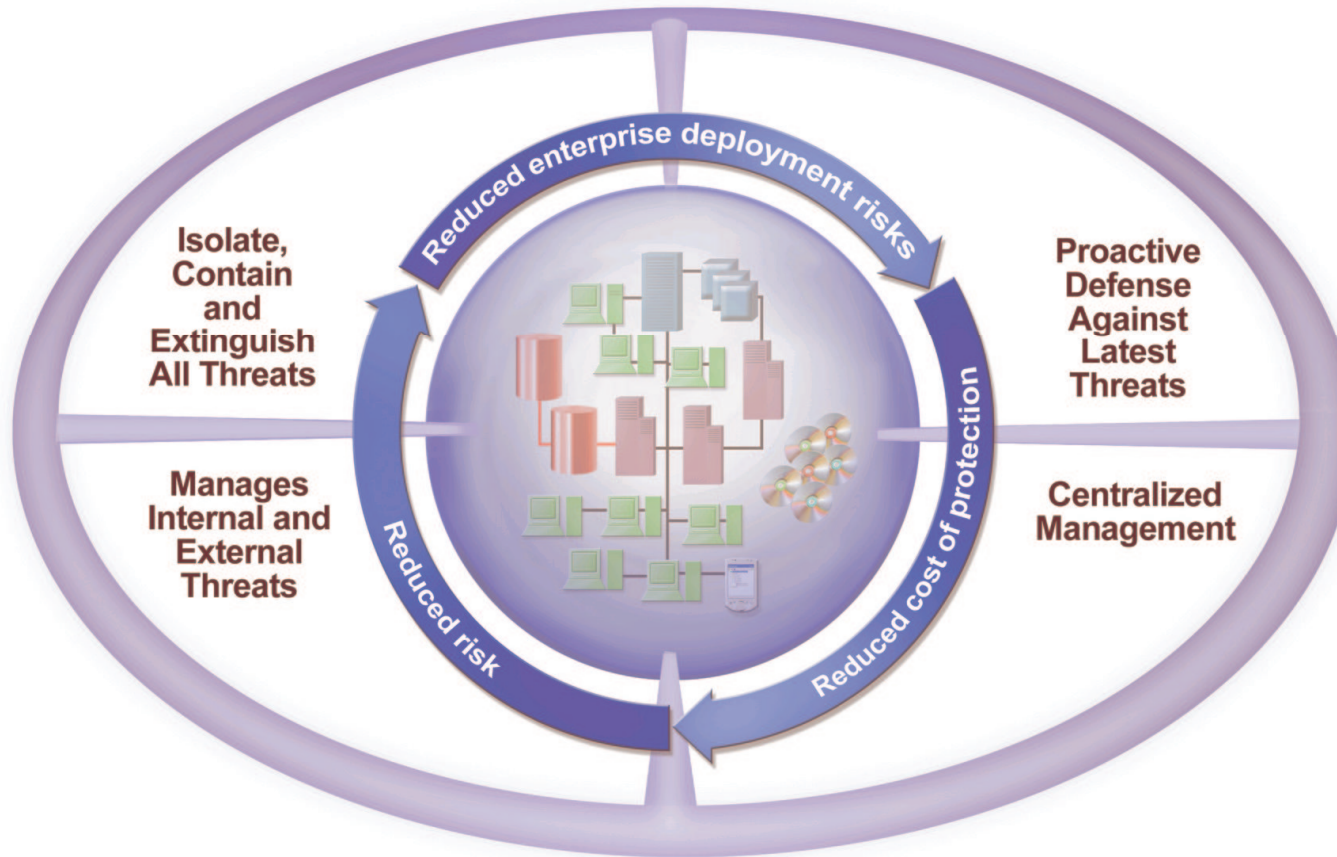
**eTrust Policy Compliance**

**eTrust Vulnerability  
Manager**



# eTrust Threat Management

## eTrust™ Threat Management



**The Power of Complete Protection**

# Security Management Under Control



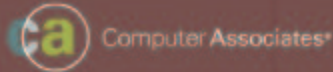
**eTrust Audit**

**eTrust 20/20**

**eTrust Security  
Command Center**



# eTrust Security Command Center



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



systems



Integrating a variety of platforms and vendors



# eTrust Audit

- The industry leading log consolidation solution
- Clients include Discount Bank, P&G, CSC/Nortel

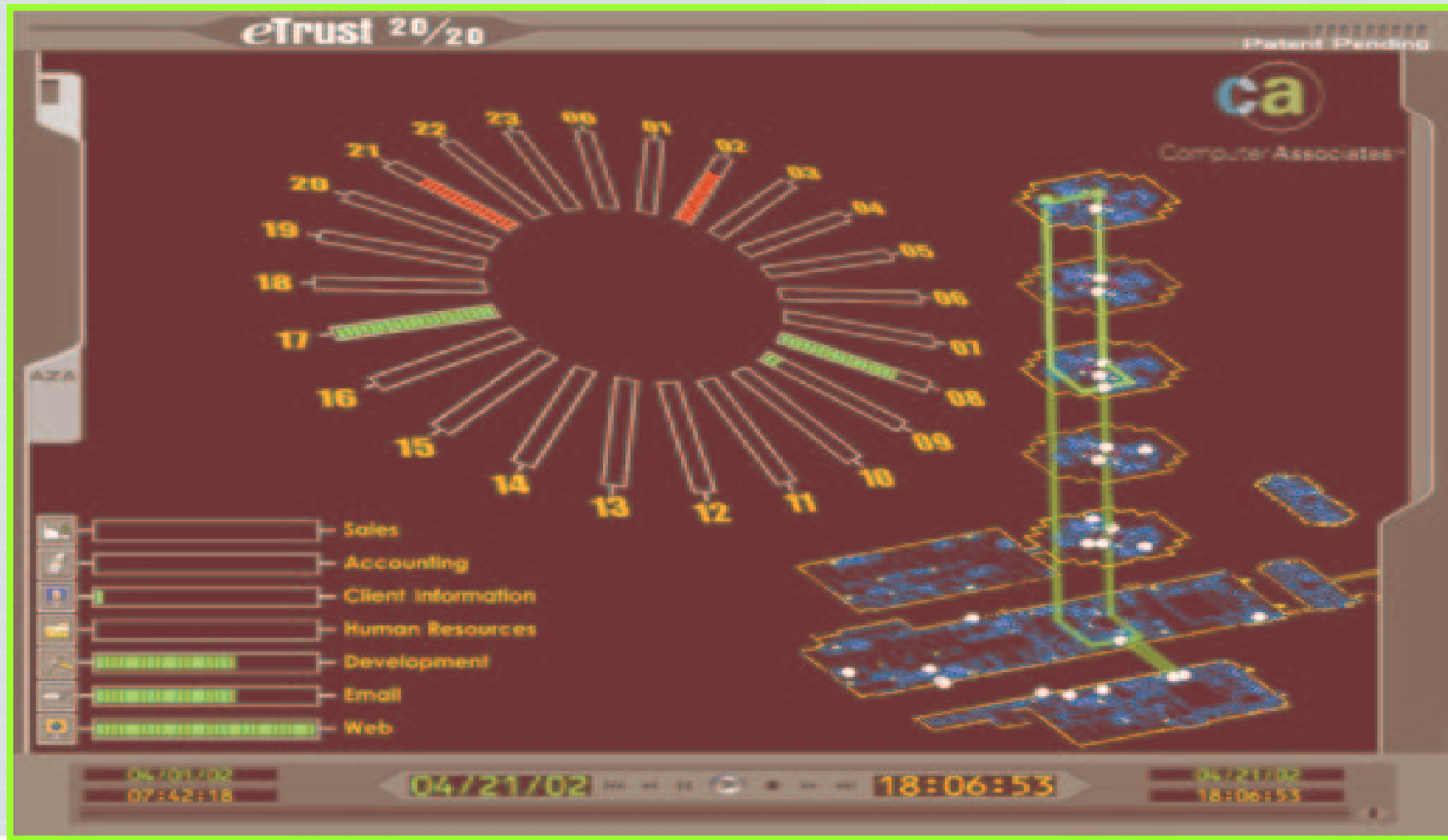
*“Before implementing the eTrust Audit software, collecting audit data had taken 16-20 hours. Now it takes about 10-15 minutes.”*

Bob Daly, VP  
ICT Group



# eTrust 20/20

- Align physical & IT security processes



## Contain Security Information Overload

- **True command and control**
  - Single, centralized console
  - Remote control capability
  - Automation
- **Improve “Operational and Situational Awareness”**
  - Role-based views
  - Shorten and improve the discovery, research and response processes
  - BUILD A SECURITY STATE MODEL!!
- **Breadth and Depth of coverage**
  - Number of 3<sup>rd</sup> party products supported

**“See it All, Manage It All”**

# Centralized Command and Control

The screenshot displays the eTrust Security Command Center interface, which includes a navigation menu with options like WORKPLACES, STATUS, EVENTS, REPORTING, POLICY MGMT, and KNOWLEDGE. The main content area is divided into several panels:

- Access Management Events:** A table showing audit log entries for Access Management.
- Access Management Status:** A panel showing the status of eTrust World, currently in a 'Ready' state.
- Alert:** A green panel indicating 'Security Condition 0: Normal Status'.
- Access Management Menu:** A panel with a world map and a pie chart, listing various services and their counts.

Message	Entry ID	Timestamp	Domain	User	Log Name	Source
The descrip...	323421	02/14/2003 0...	CALI-ETRUS...	SYSTEM	NT-Security	Security
The descrip...	32342	02/14/2003 1...	CALI-ETRUS...	eAdmin	NT-Security	Security
The descrip...	32339	02/14/2003 1...	CALI-ETRUS...	eAdmin	NT-Security	Security
The descrip...	32338	02/14/2003 1...	CALI-ETRUS...	eAdmin	NT-Security	Security
The descrip...	32337	02/14/2003 1...	CALI-ETRUS...	eAdmin	NT-Security	Security

**Access Management Menu Data:**

- 137 - netbios-ms
- 80 - http
- 1434 - ms-sql-m
- 53 - domain

# Real-time status for all security technologies

The screenshot displays the eTrust Security Command Center interface by Computer Associates. The top navigation bar includes "My Profile | Logoff" and a search box. Below the navigation bar, there are tabs for "WORKPLACES", "STATUS" (highlighted with a mouse cursor), "EVENTS", "REPORTING", "POLICY MGMT", and "KNOWLEDGE". A dropdown menu shows "Access Management" with options for "New | Manage | Configure | Reset | Help".

The main content area is divided into four panels, each showing the status of a different security technology:

- Check Point firewalls:** Three status indicators (orange, yellow, green) are shown, with the green indicator being the most prominent.
- Critical Intranet Systems:** Three status indicators (orange, yellow, green) are shown, with the green indicator being the most prominent.
- Cisco Router Status:** Three status indicators (orange, yellow, green) are shown, with the yellow indicator being the most prominent.
- Critical Extranet Systems:** Three status indicators (orange, yellow, green) are shown, with the green indicator being the most prominent.

Each panel includes a "Details" link below the status indicators.

# State Models: Real-time notification and alert

The screenshot displays the eTrust Security Command Center interface. At the top, there is a navigation bar with tabs for WORKPLACES, STATUS, EVENTS, REPORTING, POLICY MGMT, and KNOWLEDGE. A search bar is located on the right. Below the navigation bar, the 'Access Management' section is active, showing a table of 'Access Management Events'. The table has columns for Message, Entry ID, Timestamp, Domain, User, Log Name, and Source. The events listed are related to 'The descri...' and 'eAdmin' users. To the right, the 'Access Management Status' section shows 'eTrust World Using Profile' and 'Ready'. At the bottom right, an 'Alert' box is displayed with a red background, indicating a 'Security Condition 2: Correlation has found events consistent with an automated attack'. The 'Access Management Menu' at the bottom left lists various components like Reporting and Analysis, Cisco Easy VPN Solution, Checkpoint Firewall, eTrust Audit, and eTrust Antivirus. A world map with pie charts is also visible in the bottom right area of the menu.

**eTrust Security Command Center** by Computer Associates My Profile | Logoff

SEARCH  go

WORKPLACES STATUS EVENTS REPORTING POLICY MGMT KNOWLEDGE

Access Management New | Manage | Configure | Reset | Help

**Access Management Events**

eTrust Audit Log Viewer Using Profile: Access Management (Node: 142-e...)

Options Help

Message	Entry ID	Timestamp	Domain	User	Log Name	Source
The descri...	32341	02/14/2003 0...	CALI-ETRUS...	SYSTEM	NT-Security	Security
The descri...	32342	02/14/2003 1...	CALI-ETRUS...	eAdmin	NT-Security	Security
The descri...	32339	02/14/2003 1...	CALI-ETRUS...	eAdmin	NT-Security	Security
The descri...	32338	02/14/2003 1...	CALI-ETRUS...	eAdmin	NT-Security	Security
The descri...	32337	02/14/2003 1...	CALI-ETRUS...	eAdmin	NT-Security	Security

Ready

**Access Management Status**

eTrust World Using Profile

Tree View Options Help

eTrust World eTr eTr

Ready

**Alert**

Security Condition 2:  
Correlation has found events  
consistent with an automated  
attack

**Access Management Menu**

- Reporting and Analysis
- Cisco Easy VPN Solution
- Checkpoint Firewall
- eTrust Audit
- eTrust Antivirus

137 - netbios-ms  
80 - http  
1434 - ms-sql-m  
53 - domain

# Security Management Leadership

- **Requires** a company that understands security
- **Requires** a company that understand enterprise integration and management
- CA has been delivering security solutions since 1983
- CA has over 15,000 Unicenter customers collectively managing 16,000,000 machines

- Question: “How real is it to expect that security management of a heterogeneous environment is possible?”
- Answer: “CA has been doing it successfully for over 10 years, so I’d say its very real”

John Thompson, Symantec CEO



# Security Management Is CA's Business