elaman

GERMAN SECURITY SOLUTIONS

Network Forensic

GOVERNMENTAL SECURITY SOLUTIONS

DATA SHEET

*e*Trust™ Network Forensics r8

*e*Trust™ Network Forensics helps your organization secure its network and ensure availability by capturing real-time network data to identify how your business assets are affected by network exploits, internal data theft, and security or HR policy violations. As part of Computer Associates International, Inc.'s (CA) Enterprise Infrastructure Management strategy, *e*Trust Network Forensics can help your organization mitigate risk, comply with regulations, and reduce analysis and investigation cost by allowing your IT and security staff to visualize network activity, uncover anomalous traffic and investigate security breaches.

IT Security Forensics and Investigation Challenges

The success of organizations today relies significantly on the security and availability of their networks. However, networks are complex and their topographies are always changing, forcing your IT and security staff to react constantly. Security breaches are increasing, with more than 70% being perpetrated by authorized employees. Furthermore, businesses are under pressure to comply with regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) and Sarbanes–Oxley (SOX), as well as internal security and human resource policies to ensure the integrity and availability of their systems.

Organizations require a network security investigation and forensics solution that can help them build intelligence about their network usage, identify suspicious patterns and expose weaknesses and anomalies.

Visualize, Uncover, Investigate

*e*Trust Network Forensics effectively answers the difficult question of "What happened?" in the aftermath of a security incident by tackling the complicated task of capturing, analyzing and visualizing network data. *e*Trust Network Forensics provides a passive network monitoring solution that visualizes network activity by creating a dynamic picture of communication flows to swiftly uncover break-in attempts, weaknesses, abnormal usage, policy violations and misuse, and anomalies before, during and after an incident.

Operating like a surveillance camera, *e*Trust Network Forensics can play back events from thousands of communications to validate system threats and investigate security breaches. It identifies the offender and helps you mitigate the recurrence of the same security incident. *e*Trust Network Forensics enables your organization to reduce investigation costs, while improving efficiencies in security planning, deployment and recovery. In addition, *e*Trust Network Forensics helps monitor infractions to regulatory controls and policy violations by providing supporting reports for auditing requirements and contributes demonstrable compliance to internal controls policies and government regulations.

Distinctive Features and Functions

Network Traffic Recording and Visualization. *e*Trust Network Forensics promiscuously monitors and records network traffic in all seven layers of the Open Systems Interconnection (OSI) stack in real time and uses advanced visualization tools to create a picture of communication flows to swiftly expose anomalies, illegal connections and security and network problems.

- **Real-Time Network Data Capture.** *e*Trust Network Forensics promiscuously monitors more than 1,500 protocols and services out of the box and records network activity in real time into a central database that can be queried, providing a complete view of how network communications are impacting security and availability.

Key Features at a Glance

- Real-Time Network Data Capture
- Advanced Visualization
- Pattern Analysis
- Content Analysis
- Forensics Knowledge Base
- On-Demand Incident Playback
- Security Investigation and Reporting
- Communication Sequencing
- Architecture Flexibility

What's New

- Embedded Ingres® r3 Database
- Enhanced, Flexible Architecture
- System Availability
- Database Management
- Wireless Ethernet LAN Monitoring
- Appliance Option
- Performance
- Stability
- Turn Key System Components

Computer Associates®

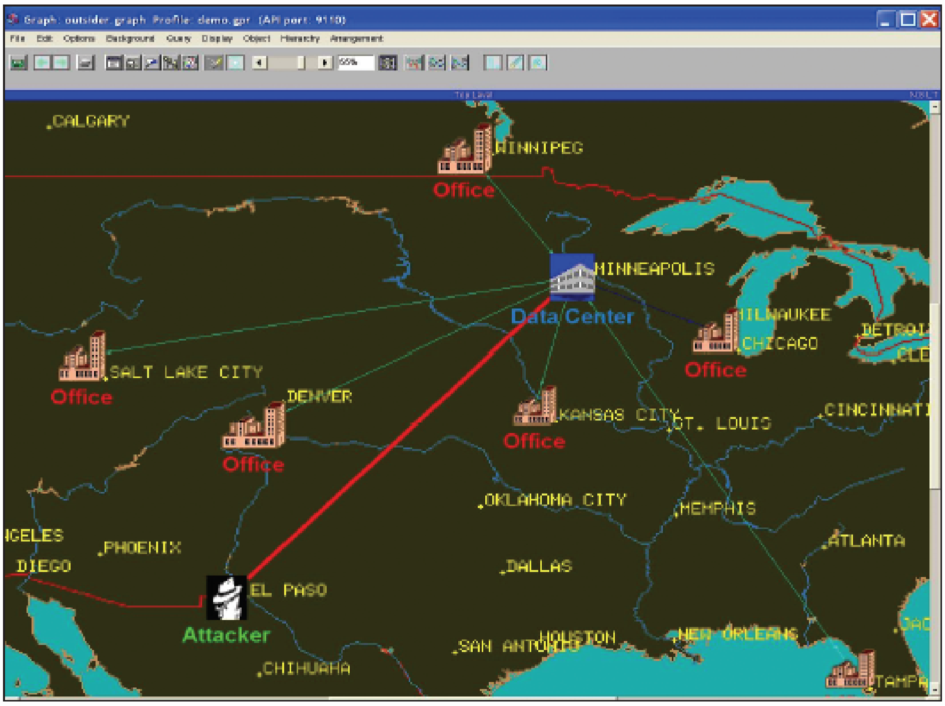


Figure 1. Critical Path: Visualize nodal communications and expose patterns or hidden data relationships with geospatial accuracy to reflect physical asset locations.

- **Advanced Visualization.** *e*Trust Network Forensics helps you detect anomalies or trouble spots by transforming raw network data into actionable knowledge. It generates interactive graphical representations of the series of events representing the propagation of an attack or other suspicious activity. Through visual representations, you can efficiently analyze users, hosts, domains, applications, protocols and addresses — detecting changes or abnormalities from established network baselines (see Figure 1).

Pattern and Content Analysis. Visualize and depict abnormal usage, and analyze emails, keywords, images or other references to reveal improper data exchange or leakage.

- **Pattern Analysis.** *e*Trust Network Forensics allows you to identify network usage patterns and build "integrated maps" of certain assets or users — such as after-hours usage spikes, and mapping of viruses and worms proliferation — and then examine the forensics evidence to determine the root cause of a security breach. By correlating network activity with security events, it can quickly distinguish between diversionary and truly malicious incidents.
- **Content Analysis.** *e*Trust Network Forensics utilizes a statistical process called *n*-gram analysis to evaluate similarities within emails, documents, spreadsheets and so on. Independent of keyword or linguistic matching, you can determine how proprietary or inappropriate information proliferated from code servers, HR or financial databases, R&D labs and others.

Forensics Knowledge Base. *e*Trust Network Forensics stores and catalogues network data into a central repository allowing you to play back the exact sequence of events aiding to ensure effective and accurate investigations.

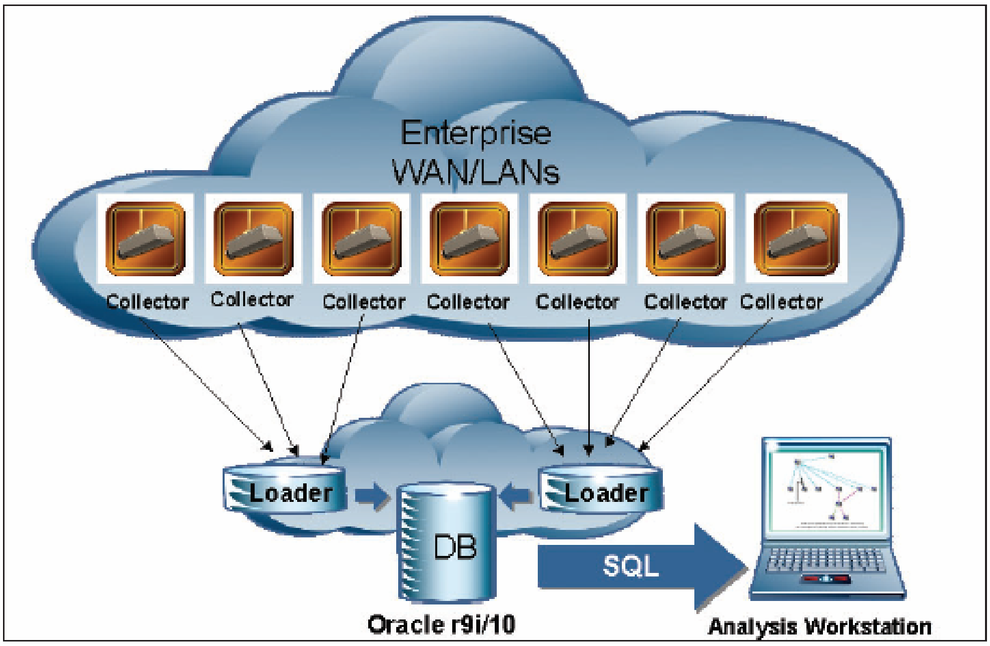
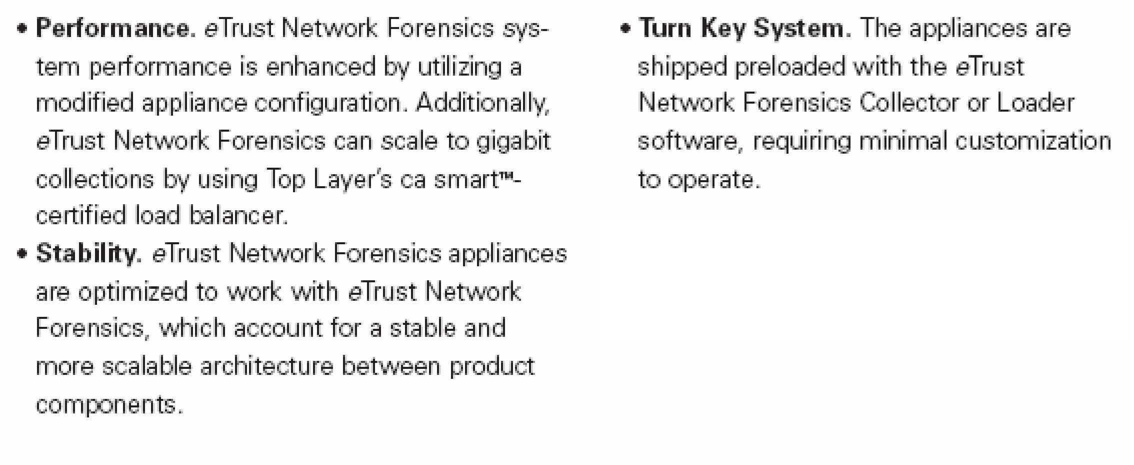


*Figure 3. Flexible Architecture: e*Trust Network Forensics *components can be implemented on a single laptop or on either software-based distributed enterprise deployment.*

architectures to provide quick and efficient data analysis. Real-time network data is collected from either single or multiple collection points within the network. *e*Trust Network Forensics then enables you to analyze and investigate a targeted traffic, allowing you to filter the data that should be sent to the centralized data store. With this flexibility, you can reduce the size of your datastore and increase your efficiency as only relevant data about your networks and their structure are examined from one central repository. For data storage, you can use CA's Ingres r3 DBMS, which is embedded and distributed with eTrust Network Forensics or Oracle 9.x and 10x, which are also supported.

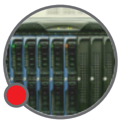
- **Distributed Monitoring.** Gain visibility into multiple networks at once and correlate network data across the enterprise. *e*Trust Network Forensics utilizes a flexible and secure way to transfer data from multiple *e*Trust Network Forensics Collectors to a centralized data store. Data transmission between system components is compressed and encrypted using SSL with certificates.
- **Mobile Solution.** Mobility is key when investigating an incident. *e*Trust Network Forensics supports mobile deployments for local policy audits and investigations.

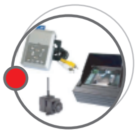
- **Forensic Analysis on Correlated Events.** *e*Trust Network Forensics visualizes audit logs and alerts, and correlates actual network traffic to provide a complete picture of activity around the time a suspicious event occurred (see Figure 4).
  - **Firewall, IDS, Syslog.** *e*Trust Network Forensics can extract and visualize events or alerts from IDS, Firewall, Syslog or other reporting system directly. *e*Trust Network Forensics supports the following third-party products: Radius, AventTail VPN, NetScreen VPN Syslog, Cisco PIX and IDS, ISS RealSecure, Check Point FireWall and more.
  - ***e*Trust™ Audit.** *e*Trust Network Forensics visualizes security events that have already been aggregated, normalized and reduced by *e*Trust Audit.



- **Performance.** *e*Trust Network Forensics system performance is enhanced by utilizing a modified appliance configuration. Additionally, *e*Trust Network Forensics can scale to gigabit collections by using Top Layer's ca smart™-certified load balancer.
- **Stability.** *e*Trust Network Forensics appliances are optimized to work with *e*Trust Network Forensics, which account for a stable and more scalable architecture between product components.
- **Turn Key System.** The appliances are shipped preloaded with the *e*Trust Network Forensics Collector or Loader software, requiring minimal customization to operate.

GOVERNMENTAL SECURITY SOLUTIONS





If you would like further Information about ELAMAN,
or would like to discuss a specific requirement or project, please contact us at:

Elaman GmbH
German Security Solutions
Seitzstr. 23
80538 Munich
Germany

Tel: +49-89-24 20 91 80
Fax: +49-89-24 20 91 81
info@elaman.de
www.elaman.de