



Computer Associates®

eTrust™ Network Forensics

Filling Gaps in Your Toolkit

Donald French CISSP, ITIL
Senior Consultant
eTrust™ Forensic Practice

eTrust™ Security Management Solutions

- Security management
 - Who has access to what?
 - What is happening in your environment?
 - How can you address it?
- Enabled by a world-class research team
- Integration with network and systems management tools
- On-demand security management



Forensics Business Drivers

- Risk mitigation
 - Protection of sensitive data
 - Need to ensure confidentiality of the data flowing through the network
 - Finding unauthorized (rogue) systems
- Operational efficiencies
 - Streamlining investigations
 - Correlate network data with security events
- Regulatory compliance
 - Demonstrate organizational compliance
 - Track flow of proprietary data
 - Audit network traffic

eTrust Network Forensics Benefits

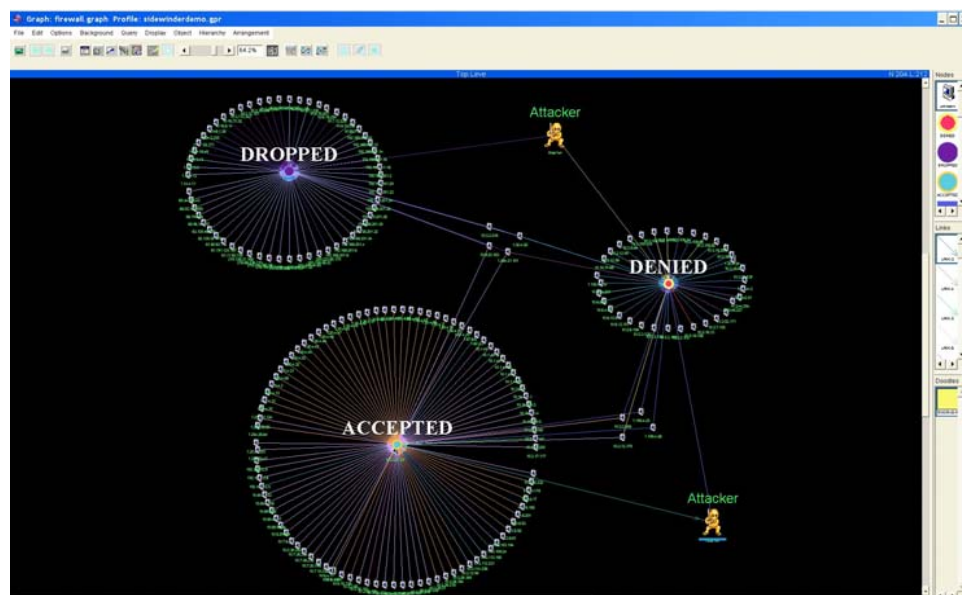
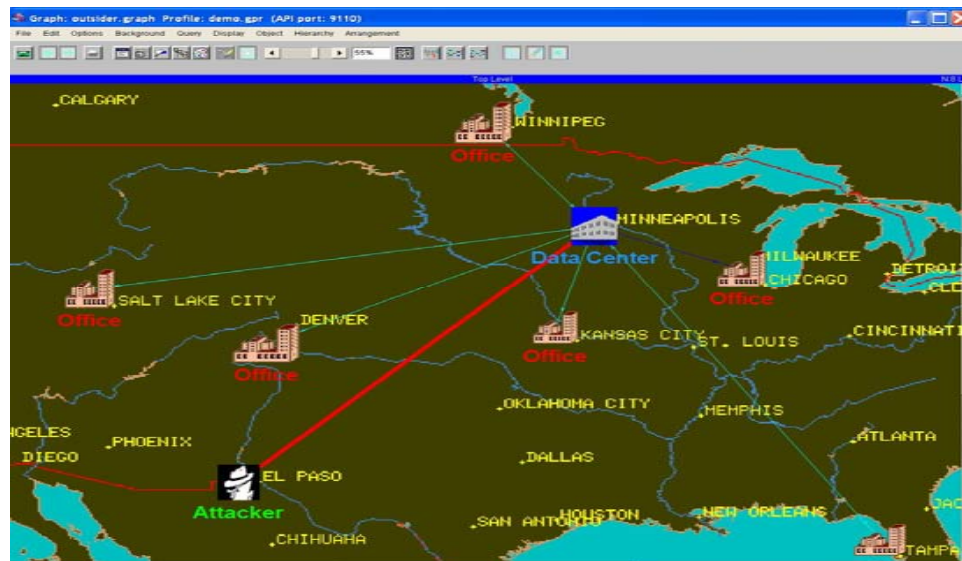
- **Business continuity**
 - Correlate security events with network activity
 - Monitor network security
- **Risk mitigation**
 - Identify the perpetrator and expose the incident
 - Mitigate recurring exploits
- **Cost and operational efficiencies**
 - Reduce investigation time
 - Provide faster data capture, analysis and visualization
- **Regulatory Compliance**
 - Provide supporting reports for auditing requirements and regulatory compliance

What is network security analysis

- *WHO* did it?
 - Determine collusion, or if a node was used as a proxy
- *WHAT* “happened”?
 - Find dependencies between a suspicious/malicious event and other traffic, which may appear normal
 - Expose diversionary tactics
 - Expose vulnerabilities which use normal communication methods (e.g.. unauthorized proxy servers)
- *WHEN* did it occur?
 - Playback incident propagation to determine precedent
- *WHERE* did it occur?
 - Identify exposed assets
- *HOW* did it happen?
 - Track network activity down to the millisecond!

eTrust Network Forensics Features

- Network Traffic Recording and Visualization
- Pattern and Content Analysis
- Investigation and Reporting
- Forensics Knowledge Base
- Flexible architecture

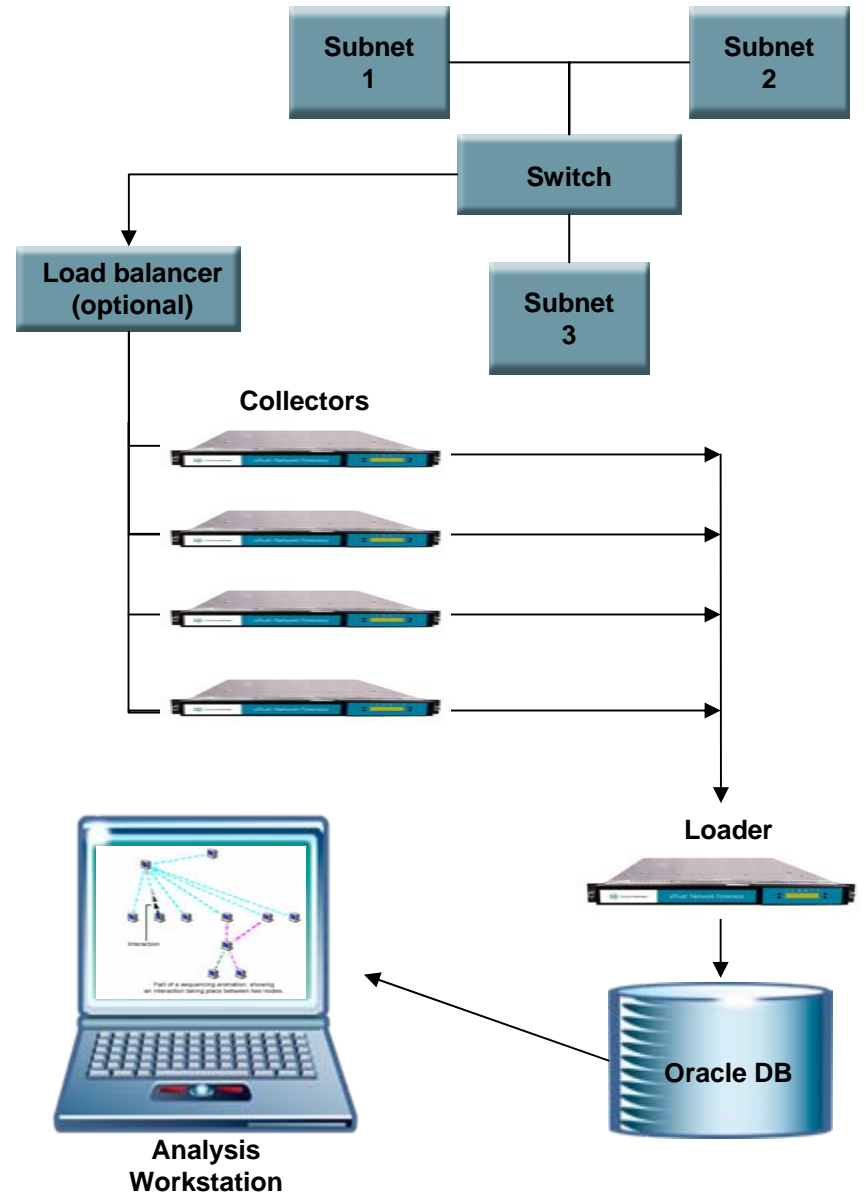


Solution Deployments

- **Single Platform (portable)** - All product components are installed on the same hardware
 - Audit Teams
 - Incident Response Teams
 - System Integrators
 - Risk Assessment Teams
 - Consultants
- **Enterprise** – Product components are installed on separate hardware
 - Permanent monitoring/forensics security solution
 - Deploy multiple Collectors at key areas of enterprise network

Flexible Architecture

- Simplifies management and controls costs by leveraging existing investments
- Integrates with eTrust and third-party network content and security products, such as Cisco syslogs, Check Point firewall logs and so on
- Supports mobile deployments for local policy audits and investigations



Complimentary Technologies

- eTrust Security Command Center/Audit
- Firewalls
- IDS/IPS Devices
- EnCase®/System-level forensics tools

Summary

- Protect shareholder value by monitoring and analyzing usage of business assets
- Support Identification of unknown security exposures and policy compliance issues
- Complement existing security and network management systems
- Turn data into knowledge through powerful visualizations and forensics analysis



Computer Associates®

Questions

Donald French CISSP, ITIL
Senior Consultant
eTrust™ Forensic Practice