

eTrust™ Intrusion Detection

Managing eBusiness Security

eTrust™ Intrusion Detection is a complete session security solution that incorporates three key capabilities in one product—network protection, network session monitoring and Internet content blocking. It defends against network attacks and helps enforce corporate security policies. eTrust Intrusion Detection is a scalable, high-performance solution that meets the needs of all organizations, including those with large, high-traffic enterprise networks.

Today's Need: Ironclad Network Security

Networks stand at the center of today's organizations, transmitting vital, often highly sensitive information while connecting users to essential resources. As networks grow in size and complexity, protecting them from threats such as low-level protocol attacks, and server and desktop intrusion becomes increasingly difficult. Other potential threats include viruses and malicious applets that traverse internal networks. It is necessary to detect and block inappropriate network access to internal services and desktops, as well as outside URLs.

Comprehensive Network Protection

eTrust Intrusion Detection from Computer Associates International, Inc. (CA) delivers state-of-the-art network protection by automatically detecting network traffic patterns that indicate potential intrusions, attacks and abuses. eTrust Intrusion Detection provides leading-edge, enterprise-ready network protection technology with unprecedented levels of flexibility, adaptability and ease-of-use. Its effective, centralized session monitoring capability allows network administrators to monitor and control one or more stations—locally or remotely—running eTrust Intrusion Detection. Strategically placed and centrally controlled, eTrust Intrusion Detection sensors can be placed on different network segments, allowing administrators to view alerts and generate reports based on the consolidated information collected. Additionally, eTrust Intrusion Detection offers an easily deployable network protection solution that can be implemented without introducing any points of failure.

ask about our certification program



eTrust Intrusion Detection offers superior benefits to help your organization:

- **Provide more comprehensive security** with a combined solution that includes three key capabilities—network Intrusion Detection System (IDS), session monitoring and Internet content control.
- **Conserve network bandwidth resources** by allowing you to see how much of your network capacity is being used by non-business activity on HTTP, SMTP, Telnet and FTP.
- **Boost employee productivity** through use of the advanced management facilities, which streamline administration and save time.

Distinctive Functionalities

For Enterprise-Ready Management:

- **High Performance.** eTrust Intrusion Detection supports high-throughput network environments and integration with ca smart™ certified, third-party load balancing solutions to accommodate extremely high network traffic.
- **Automatic Signature Updates.** eTrust Intrusion Detection automatically obtains updated signatures, even through proxy connections. A streamlined administration process helps ensure the use of the most current software updates for maximum protection.
- **Centralized Console Management.** Administrators can monitor and control an entire network from a single console, allowing them to set rules and policies, and monitor network usage and intrusion attempts. Critical alerts can be issued so administrators can respond quickly to intrusions.
- **Remote Management.** Remote users can access a station running eTrust Intrusion Detection using TCP/IP or a modem connection. Once connected, users can view and monitor eTrust Intrusion Detection data, change rules and create reports—depending on the permissions defined by the eTrust Intrusion Detection administrator.

For Network Protection:

- **Complete Network Protection.** eTrust Intrusion Detection provides network-wide, reliable, distributed, real-time network protection. By deploying eTrust Intrusion Detection to multiple locations within the enterprise, its powerful capabilities protect the entire network. This includes monitoring and responding to



Computer Associates®

enterprise-wide events from a remote or centrally located consolidation console. eTrust Intrusion Detection also includes a central event database repository, additional reports and a distributable "see-it-all" content viewer.

- **Integrated Virus Scanning.** eTrust Intrusion Detection scans network traffic for malicious code and alerts the network administrator if a virus is found. This raises the level of awareness of a potential virus outbreak within the enterprise.
- **Swift Attack Containment.** eTrust Intrusion Detection offers automated rule updates for various integrated network devices, including firewalls and routers.

For Session Monitoring:

- **Load Measuring.** A new utility called NetLoad lets customers monitor and log both total and service-/protocol-specific traffic rates. By knowing network utilization rates up front, users can more accurately implement an IDS.
- **Network Usage Logging and Reporting.** eTrust Intrusion Detection provides network administrators with greater visibility of what is happening in their environments. They can track network usage by end users, applications, protocols, server sources and more, and create reports so management can quickly identify issues and trends. This helps improve network policy planning and enables protection against sources of abuse.
- **Content Monitoring.** eTrust Intrusion Detection provides out-of-the-box content monitoring of HTTP, SMTP, Telnet and FTP traffic, allowing administrators to view how email and Web services are being used for more complete views of their networks.
- **Intrusion Logging and Analysis.** eTrust Intrusion Detection provides a comprehensive system that captures information and makes it available for analysis. After installing the software and designating an archive location, users define a rule that logs the session data into an archive. They can then use the browser to

filter, sort and view the archived information, and create detailed reports. eTrust Intrusion Detection uses industry-standard, ODBC-compliant databases, such as Microsoft SQL and Oracle.

For Internet Content Blocking:

- **Provides URL Blocking and Access Control.** Administrators can designate URLs that users are not allowed to visit, maximizing network resources by reducing unproductive web surfing. To simplify administration, administrators can also select and block entire categories of websites.
- **Watch and Patrol.** Administrators can detect traffic that violates policy and automatically terminate the session. This allows organizations to unobtrusively enforce policy with zero impact on performance.

eTrust™: Managing eBusiness Security

eTrust solutions proactively secure an organization's cross-platform, heterogeneous IT infrastructure. Powerful, comprehensive solutions address every security issue and offer complete security infrastructure management from the IT industry's leading security vendor.

CA Services™ — Enterprise Solutions for Business

CA Services defines solution leadership through customer partnerships that leverage a combination of industry-proven methods, education and global experience. The disciplined and systematic approach of CA Services provides consistent methodologies and processes that help ensure quality results and optimal success. Visit ca.com/services or ca.com/education to learn more.

Supported Environments

- Windows 98, Windows Me, Windows 2000 (original or SP2), Windows NT 4.0 (equipped with SP5 or SP6)
- TCP/IP networks

For more information, call 1-800-875-9659
or visit ca.com



Quality
Endorsed
Company
ISO 9002
Lic. 2443



Computer Associates®