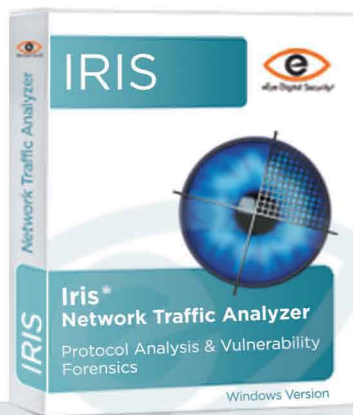




# IRIS Network Traffic Analyzer<sup>®</sup>

## Visual Data Monitoring & Reassembly.



Iris Network Traffic Analyzer empowers your security and operations teams by providing granular data monitoring and precise packet and session reconstruction capabilities. The solution is designed to combine process and technology into a single effective system for network forensics, and monitoring.

Today's organizations rely on the continuity and security of underlying IT systems at all times. This requirement is further amplified when you take into account the fact that most security or performance issues, whether due to malicious acts, user non-compliance or simple bandwidth misallocation, generally reside above your network in the applications being serviced by your infrastructure.

eEye Digital Security's solution to the problem is the Iris Network Traffic Analyzer. Iris allows professional teams to quickly and easily examine the inner workings of a network. This highly sophisticated system supports the investigation into security and performance issues, decreasing the amount of detective work while enhancing the overall productivity of your security and performance monitoring systems.

## Fast Facts

- o Available as software or bundled with the Retina 651 Security Management Appliance<sup>®</sup>
- o Provides instant network data capture and the ability to decode traffic in real time
- o Records and replays traffic for a complete audit trail of suspicious network activity
- o Helps identify performance problems before they result in network downtime
- o Advanced searching and filtering for quick identification of desired datum
- o Compatible with network adapters up to gigabit speeds

## Session Reconstruction

Most packet capture solutions and network sniffers only display raw packets and leave it to the user to decode and determine the potential problems they represent. Iris collects network traffic and reassembles it as its native session based format, enabling users to quickly and easily make business decisions based on the service it was providing. Iris users can reconstruct the actual text of an email, as well as any attachments, exactly as it was sent. It provides reconstruction of full HTML pages that an end users visited and reassemble cookies for entry into password-protected websites. Iris will even display bi-directional instant messaging communications allowing full session reconstruction as the end user sees it.

## Data Capture

The Iris<sup>®</sup> Traffic Capture Engine<sup>™</sup> is designed as a service oriented architecture, permitting security professionals to gather forensic information while performing other tasks in parallel. Iris is designed to capture specific data via filters based on a myriad of traffic metrics. This approach ensures that all targeted traffic is captured, regardless of whether the solution is run interactive or as a service. For capacity and service level agreement planning, Iris allows users to leverage traffic captured in one area of a network for use elsewhere, as well as for the monitoring of applications in development. Additionally, Iris allows for advanced functions such as keyword searching and protocol distribution.

## Statistical Analysis

Iris provides a large variety of statistical measurements, supplying information on protocol distribution, top hosts, packet-size distribution and bandwidth usage. By regularly analyzing how systems and applications are being used, administrators can proactively identify and eliminate issues before they can result in downtime. Iris can also provide the proof required to drive the creation and enforcement of policies related to appropriate system and application usage.

**Secure  
Your Business.**  
[www.eEye.com](http://www.eEye.com)  
866-282-8276

**Professional Grade Security Solutions<sup>™</sup>**

### Statistics and Reports

Iris provides DNS names and comprehensive statistical measurements for granular monitoring of session traffic. The metrics can be viewed in an assortment of graphical formats (e.g. pie charts, bar graphs, etc.) and include:

- **Protocol Distribution Stats:** Reports network usage based on MAC, IP and IPX layer protocols.
- **Top Host Statistics:** Provides an analysis of the IP Layer traffic statistics collected for each host in real time and is ordered by the most “talkative” hosts.
- **Size Distribution Statistics:** Displays the number of packets with sizes in six different ranges.
- **Bandwidth Usage:** Charts the number of packets per second and bytes per second flowing across the network in real time.
- **Traffic Reports:** Complete traffic data that can be viewed in a browser, saved, printed, or copied into another program.

### Data Reconstruction

Iris takes raw data in packets and turns it into complete HTTP, SMTP and POP3 sessions in their original format. The following are some of the protocols Iris reconstructs:

- **Outgoing and incoming email messages:** The text of the message is readable as well as the subject and recipient. Iris will launch an email client to open the message, as well as any attachments, exactly as they were sent.
- **Web browsing sessions:** Reconstruction of HTML pages in their original format.
- **Instant messenger exchanges:** Iris will reconstruct all IM communications from both sides of the conversation.
- **Non-encrypted web-based email**

## About eEye Digital Security

eEye® Digital Security is pioneering a new class of security products: integrated threat management. This next-generation of security detects vulnerabilities and threats, prevents intrusions, protects all of an enterprise's key computing resources, from endpoints to network assets to web sites and web applications, all while providing a centralized point of security management and network visibility. eEye's research team is consistently the first to identify new threats in the wild, and our products leverage that research to deliver on the goal of making network security as easy to use and reliable as networking itself. Founded in 1998 and headquartered in Orange County, California, eEye Digital Security protects more than 9,000 corporate and government organizations worldwide, including half of the Fortune 100. **For more information, please visit [www.eEye.com](http://www.eEye.com).**

U.S. Tel: 1.866.282.8276

N. America: 1.949.333.1900

Germany: +49 (0) 8031 2227 432

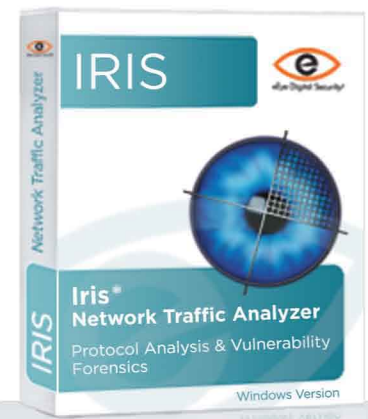
U.K.: +44 (0) 20 8144 1102

Asia Pacific: +603 79581575

N. America Sales: [sales@eEye.com](mailto:sales@eEye.com)

International Sales: [sales.eu@eEye.com](mailto:sales.eu@eEye.com)

Asia Pacific Sales: [apacsales@eEye.com](mailto:apacsales@eEye.com)



## System Requirements

- Microsoft Windows 2000, XP, or 2003 (latest service packs recommended, 32 bit only)
- Internet Explorer 5.x, 6.x, or 7.x (or higher)
- Pentium 4 2GHz, 512MB RAM, 20GB HDD for capture storage (or higher)