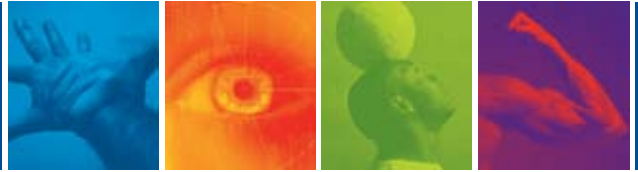


ConSentry® InSight Command Center



The command center for LAN visibility and control

ConSentry Networks enables enterprises to secure their LANs. The LANShield™ Controller and LANShield Switch use deep packet inspection to admit users onto the LAN, provide visibility into LAN activities, control access based on identity, and contain malware and other attacks. ConSentry InSight provides IT with the means for capturing and viewing all the data as well as for setting policies.

InSight aggregates all traffic capture data and presents IT with actionable information, showing key security incidents in at-a-glance summaries and drill-down, detailed views. InSight also enables rapid forensic troubleshooting, auditing, and reporting. InSight's GUI-based tools simplify policy creation and distribution. InSight includes templates that make it easy for IT to create policies and deploy them on LANShield devices. The LANShield platforms automatically derive users' roles, and InSight uses that role information as the basis for security policies. InSight also supports filters that let IT treat policies as building blocks and layer on multiple levels of control more easily. The flexible exception rules, combined with the policy filters, let IT create unique controls by role without creating a separate policy for each variation.

InSight is available as an appliance or in a software-only version.

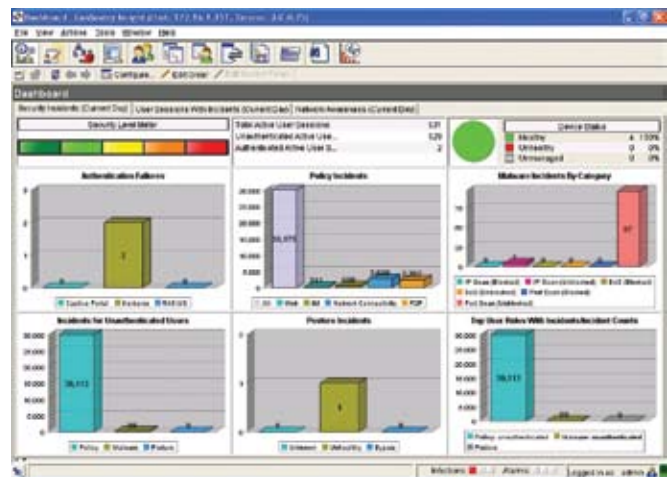
Visibility Features

InSight provides IT with a view of the overall health of the LAN and all security incidents. The LANShield products bind users to their addresses and applications, so InSight is able to display all LAN status information, incidents, and policy violations by username.

InSight retains statistics about all flows, including both real-time and historical data. This information includes such details as the packets and bytes in and out by application and protocol, the individual file name involved in a Windows file sharing (CIFS) or FTP operation, the usernames of users who accessed particular files, and the duration of all sessions.

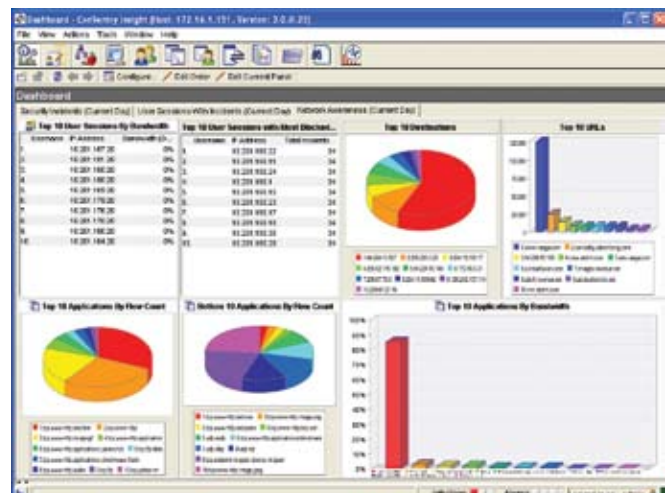
InSight also provides an aggregated view of the LAN security health – the InSight dashboard displays:

- the overall network threat level
- user counts by authenticated, unauthenticated, and guests
- authentication failures
- incidents for unauthenticated users
- policy, malware, and posture incidents
- the top user or device roles responsible for incidents



The Security Incidents dashboard enables quick response to policy, malware and posture violations

Other dashboard views such as Network Awareness show network resource usage, with data including top network users, top applications by bandwidth and instance, top destinations, and top URLs being accessed during the course of the day.



The Network Awareness dashboard provides a quick snapshot of network usage by user and application

InSight provides a range of other statistics that can be selected to create custom dashboard views. IT can select from data such as

top policy violators, top FTP file transfers, top IM files, top policy incidents, and malware incidents by type.

Detailed forensic drilldown is available from the dashboard views that provide information on user activity, applications and hosts used, and policies enforced. IT can also use InSight to track individual application flows for a user. IT can select which traffic InSight should make visible. For example, an IT administrator may choose not to see details on traffic related to a management VLAN. IT can also set filters for InSight's visibility by application and role.

To protect privacy, InSight supports a four-eye mode that requires two IT staff be involved when accessing information such as user-names and IP addresses.

Custom queries allow IT to view specific data when troubleshooting network performance or security issues. Among the possible queries are:

- New applications (by bandwidth) seen over a period of time specified by IT
- New network users seen over a period of time specified by IT
- Network users seen over a specific time period but not currently visible

Reporting Features

InSight provides comprehensive reporting on the visualized data. Built-in reports include the Daily File Access Report and the Enterprise Security Report, which includes user and incident information.

IT can also generate custom reports to meet their individual needs. For example, an administrator could build a report that showed all users that have incidents associated with a given policy during a specified time period or all users that accessed a particular application during a specified time period. An IT administrator can also add graphical charts from the InSight dashboard to report templates to enhance their visual presentation.

Central Configuration and Management

InSight provides centralized management and configuration of all LANShield devices deployed in a network. Capabilities include:

- **Central policy management:** InSight enables IT to configure policies just once and then push them out to all applicable LANShield devices.

InSight Command Center Appliance Specifications

- Dual 2.8 GHz processor
- 2 GB, 333 SDRAM Reg DDR1 x4
- SCSI 146G/10K disk drive
- Two 1 Gbps Ethernet connections
- Four USB 2.0 ports
- 1U chassis

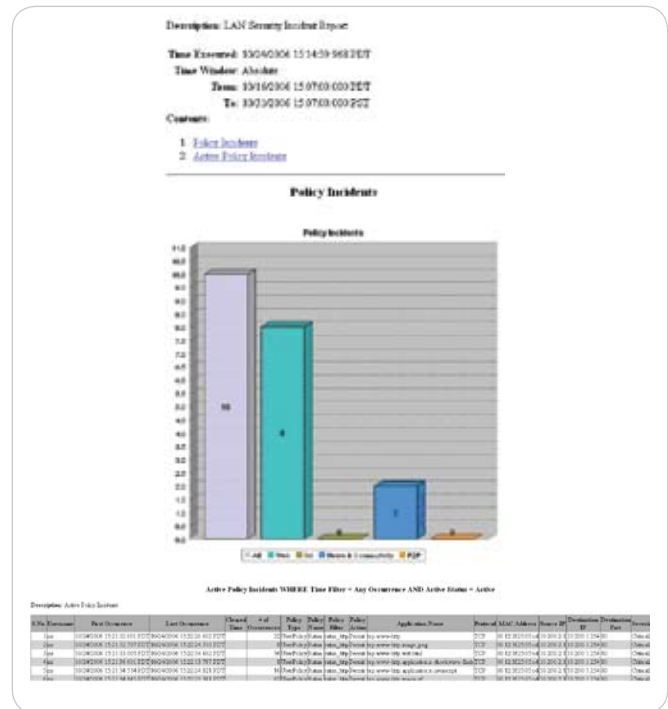
Minimum System Requirements for InSight Software Installation

- Dual 2.8 GHz processor
- 2 GB RAM
- 60 GB hard disk space
- Microsoft Windows 2003 Server with SP1 Operating System (Web or Standard Edition, 32 bit)

Client Requirements for InSight

The InSight client can be run on most Windows systems. Minimum requirements are:

- Windows 2000 Server, Windows 2003 Server, or Windows XP Professional
- 2.8 GHz single CPU
- 512 MB RAM
- 20 GB hard disk
- Internet Explorer 6.0 or higher
- Screen resolution of 1024 x 768 pixels
- Internet connectivity



The LAN Security Incident Report includes a bar chart showing policy incidents by application type and a tabular listing of all policy incidents. IT can define the time duration covered by the report.

- **Software updates of multiple LANShield devices:** IT can use InSight to distribute updated LANShield OS releases to all deployed devices.
- **LANShield device health:** This configuration view provides status on a LANShield device's CPU usage, memory usage, fan speeds, current temperature, and power supply status.
- **Custom captive portal:** Using InSight, IT can distribute a customized captive portal page to multiple LANShield devices.
- **Distribute posture check configuration file:** IT can use InSight to send these endpoint files to multiple LANShield devices.
- **Audit logging:** IT can track all actions done via InSight, with the associated users, time, and status of each activity.



Corporate Headquarters
 ConSentry Networks
 1690 McCandless Drive
 Milpitas CA 95035
Phone 408.956.2100 **Fax** 408.956.2199
Toll-Free 866.841.9100
Email info@consentry.com
 www.consentry.com

Germany
 ConSentry Networks
 Lyoner Strasse 6 D-605 8
 Frankfurt Germany
Phone +49 69 677 33 4
Fax +49 69 677 33 00

United Kingdom
 ConSentry Networks
 Lakeside House 1, Furzground Way
 Stockley Park, Heathrow, UB11 1BD
Phone +44 (0) 2086 22 3020
Fax +44 (0) 2086 22 3200

Japan
 ConSentry Networks
 Hibiya Central Bldg. 14F
 1-2-9, Nishi Shinbashi, Minato-ku
 Tokyo 105-0003 Japan
Phone +813-5532-7630
Fax +813-5532-7373