



Securing Your Data is Our Business



PacketSure™ Data Loss Prevention 8.5 Product Overview

The Leaky Network Challenge

Your network is leaking secrets, and you don't even know it. Users are emailing unencrypted credit card numbers over the public Internet, sending Social Security numbers, using Internet file transfers to share protected medical records and more.

Leaks cost millions in fines under regulations including Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), Sarbanes-Oxley (SOX), the Children's Internet Protection Act (CIPA), and state privacy rules. The laws require companies to inform customers about data leaks. When word gets out, companies suffer lost reputation and business.

The Solution – Palisade's PacketSure™

PacketSure™ 8.5 guards your enterprise network, monitoring the perimeter for data leaks and providing Data Loss Prevention (DLP). It's available as an appliance, for enterprises requiring an on-premises solution, or as a service from Palisade's Managed Service Provider (MSP) partners.

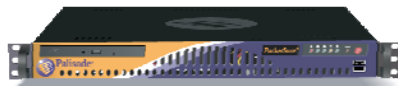
PacketSure™ analyzes the content of files and data being transferred on your network in real time. It identifies private data and blocks the data, quarantines it for later inspection, or sends it to a third-party encryption engine. PacketSure™ also identifies private data residing on local or remote file systems. PacketSure™ can block specific network protocols. It is the only solution that secures both private content and the protocols running on your network.

Protect private data in:

- ▶ **Data at Rest:** PacketSure's Endpoint protection discovers private information residing on your network servers and workstations. It scans local and remote file systems to identify confidential data. It also blocks a user from copying files to external devices.
- ▶ **Data in Motion:** PacketSure monitors outgoing communications and identifies private content. The solution blocks outgoing email, Web, and instant messaging communications that contain private content. It can quarantine email messages for further review when those messages contain sensitive data.

Identify private data in:

- ▶ **Structured data:** PacketSure monitors and identifies data with recognizable patterns such as credit card or Social Security numbers. PacketSure also matches data elements from a database, such as account or claim numbers.
- ▶ **Unstructured data:** PacketSure monitors the network for unique, proprietary information by generating fingerprints of files to match data. Create custom lexicons and regular expressions to capture data that is specific to a company or industry.



Prevent Data Loss

Stop private information from leaving your network. Comply with government regulations such as HIPAA and state privacy rules. Ensure protection of personal health and financial information, credit card numbers, and private client information.



Network Policy Enforcement

Control user access to unauthorized applications such as instant messaging, Web mail such as Gmail or Hotmail, file sharing, video, telnet, and more. You can set limits on user access, or block those applications entirely.



Maximum Protection

Maximum Performance

Palisade

Securing Your Data is Our Business



Achieve Regulatory Compliance

U.S. and state governments are tightening the net of regulations requiring enterprises to protect the privacy of personal information. PacketSure helps you achieve compliance with laws and regulations including HIPAA, GLBA, SOX, and CIPA. PacketSure also helps companies comply with the Payment Card Industry Data Security Standard (PCI DSS).

“We selected PacketSure over other competitors’ products as it offered a cost-effective and comprehensive solution for our data security and compliance needs.”

Dan Carlson, Director of IT Security
Meredith Corporation



Manage Internet Access

Use PacketSure’s Web filtering to control user access to sensitive sites organized in 40 categories, including pornography, online shopping, crime, chat rooms, and more. You can either log user access to sites, or block access entirely.

Web, Email, and IM Proxies

PacketSure stops users from sending confidential information over the Internet using email, instant messaging, or the Web. PacketSure blocks violations in real time, and lets both the sender and administrator know about it.

Cisco IronPort® S-Series Web Security Appliance™

PacketSure™ DLP also works with the IronPort® S-Series Web Security appliance™ (WSA) to control confidential data.

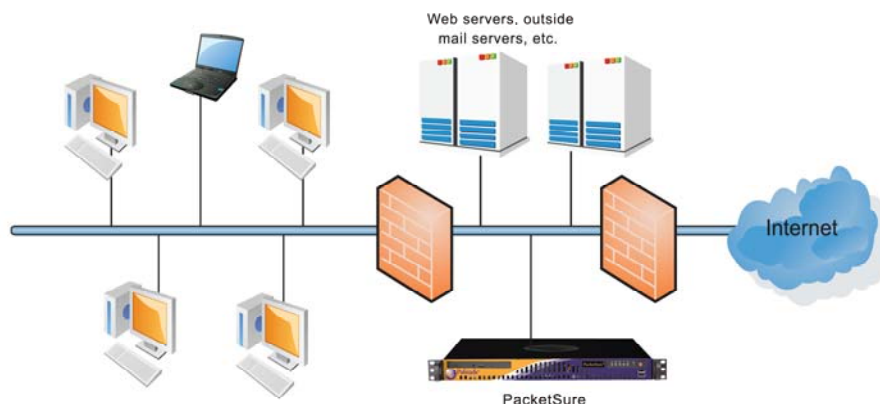
Reporting Options

- ▶ More than 75 standard reports.
- ▶ Customize reports to meet your needs.
- ▶ Save report queries for favorite reports.
- ▶ Automatically generate and email reports.

Content Analysis File Types

PacketSure performs content analysis on nearly 500 file types:

- ▶ Word processing files such as Microsoft Word, Adobe FrameMaker, and text files.
- ▶ Spreadsheets such as Microsoft Excel and Lotus 1-2-3.
- ▶ Presentation files such as Microsoft PowerPoint and Adobe PDF.
- ▶ Container formats such as ZIP and Microsoft Outlook Personal Store (PST) files.



Visit <http://www.palisadesystems.com/protocols.pdf> for a complete list of protocols PacketSure manages and file types that are analyzed for content violations.