



Counterpane™
Internet Security

Log Management for Improved Compliance and Risk Mitigation

Demand for data privacy and protection audits is skyrocketing, fueled by government and industry mandates that range from Sarbanes-Oxley, California SB1386, and the PCI Standard for merchants and banks, to NERC CIP for utilities. Organizations, large and small, face the unprecedented burden of storing all IT system logs: real-time and historical evidence of access; activity and configuration changes for applications, servers and network devices. In order to meet compliance guidelines, they must also grapple with the fragmented and time-consuming process of mapping network activity to audit reporting. Smart organizations turn to Counterpane.

Key Benefits

As part of Counterpane's Managed Security services, the Log Management services benefits customers in five key ways:

Preserve 100% of logs in unaltered form, normalize security incidents and trends within Counterpane's Socrates correlation environment, and deliver immediate response.

Satisfy explicit data retention requirements in many high-profile government and industry regulations.

Enable alerting on huge volumes of raw log content without transmitting sensitive information outside the customer premises.

A cost-effective solution to store and process terabytes of logs without investing in a costly SAN infrastructure.

Provide a variety of pre-defined report templates, enabling our customers immediate utility without a time-consuming development cycle.

Core Services

Counterpane brings you security experts who capture, classify, analyze, and respond to a complete feed of security-specific intelligence from your networks.

COUNTERPANE'S CORE COMPETENCIES

- Most flexible correlation of security events and alerts of any MSSP
- Real-time inspection
- Human analysis
- Guided remediation
- Other proprietary feeds

ENHANCED CAPABILITY

- Most advanced log collection and query engine
- Raw log archiving
- Deep queries and reports
- Comprehensive tools
- Syslog, files, & LEA & SNMP alerts

Effective Protection. Intelligent Detection. Instant Response.

"Security and compliance requires specialized expertise, and it makes more sense to outsource that so my staff can stay focused on the core business objectives... Counterpane can survey all the potential threats worldwide. They can provide a much wider, more current view of the threats. That's something we can't do as efficiently, given our current staff levels."

—John Lambeth, CISSP, CISA
VP Information Technology
Blackboard, Inc.

"Because Counterpane gives us only the information we need when we need it, we can concentrate on the attacks that matter. The value of that kind of service is enormous."

—David MacLeod, Ph.D., CISSP
CISO
The Regence Group

"By outsourcing monitoring and management of established security systems to managed security service providers, most enterprises can increase security while reducing operational costs, and free up internal security resources to deal with changing business needs and new threats."

—John Pescatore
VP Distinguished Analyst
Gartner, Inc.

Contact Us

sales@counterpane.com

US: 888-710-8175

EMEA: +31 70 5170 419

Japan: +81 80 5421 8311

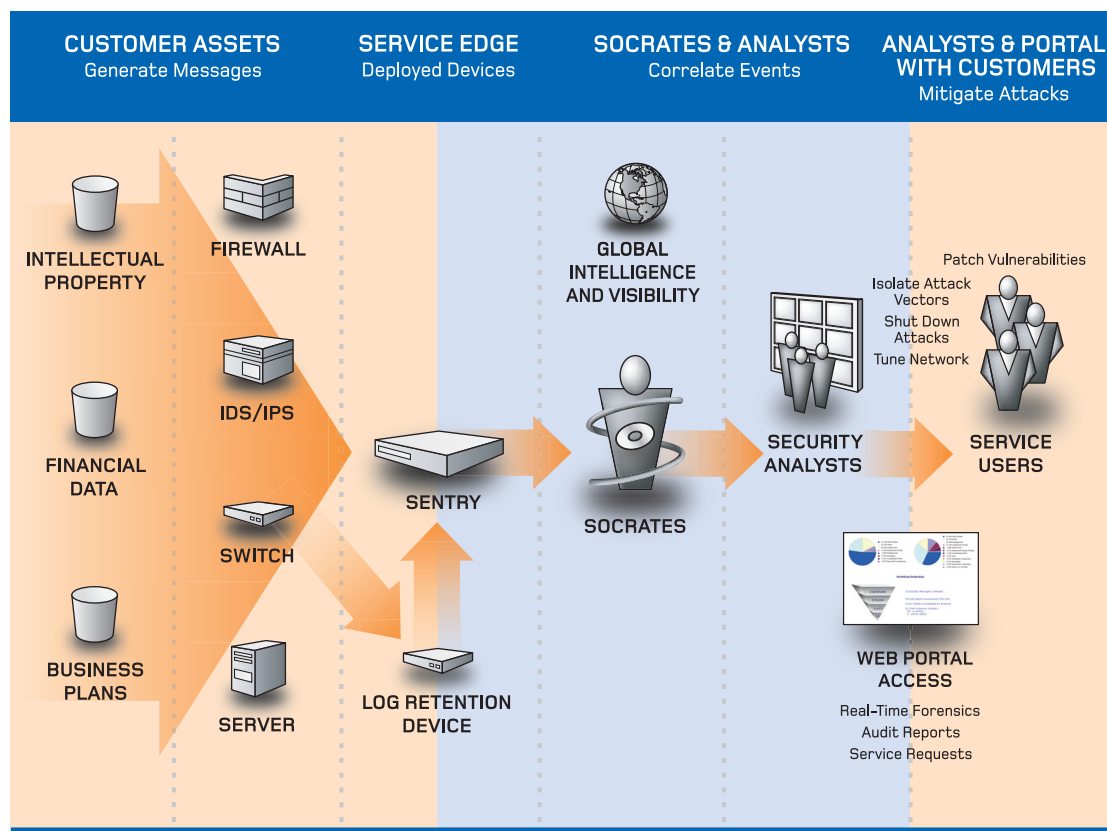
1090A La Avenida
Mountain View, CA 94043

www.counterpane.com



Counterpane™
Internet Security

© 2006 Counterpane Internet Security, Inc. All rights reserved.



The Counterpane Advantages

IMPROVING COMPLIANCE

- 24x7 Monitoring
- 24x7 Incident response
- Unaltered log retention
- Chain of custody to demonstrate evidence of data integrity
- Demonstrable evidence of reviewing user access to programs and data
- Brand name recognition of Counterpane makes auditors comfortable, pass audits easier

IDENTIFYING PROBLEMS EARLY

- Failed logins
- Exiting programs too often
- Traffic volume exceeded by a specified threshold
- Machine learning & statistical anomaly detection alerts for adaptive baseline, message volume, network policy and more

ECONOMIES OF SCALE

- ALL logs collected centrally
- Subset of critical devices monitored 24x7
- Alerts customer on non-monitored devices
- Customer gets alerts across entire environment without high costs