

Secure Computing® is a global leader in Enterprise Security solutions. Our award-winning portfolio of solutions help our customers create trusted environments inside and outside their organizations.

### Secure Firewall Reporter turns audit and log data “noise” into actionable information:

#### For Everyone:

- Enjoy a personalized reporting experience – see the data you want to see, how and when you want to see it

#### For Management

- Quickly see the overall security posture of the organization
- Proves the value of your Secure Computing investment

#### For Security Administrators:

- Receive security alerts on real hacker and malware security threats, triggered automatically
- Forensic quality data shows attack type, source, destination, port, protocol, severity, rule, etc., in real time
- Understand protocol usage by device, user, and department
- Analyze security issues and trends over time

#### For Auditors:

- Give quick evidence of regulatory compliance for Sarbanes-Oxley (SOX), PCI, HIPAA, GLBA, and FISMA

Web vers. May08

© 2008 Secure Computing Corporation. All rights reserved. SRPort-PO-May08v1: Secure Computing, IronMail, MobilePass, SafeWord, SecureOS, SecureSupport, Sidewinder, SmartFilter, SnapGear, Strikeback, Type Enforcement, and Webwasher are trademarks of Secure Computing Corporation, registered in the U.S. Patent and Trademark Office and in other countries. SecureWire, SmartReporter, and TrustedSource are trademarks of Secure Computing Corporation.

## Security Event Analysis and Reporting

*An award winning enterprise security event management (SEM) reporting solution to combat hacker/threat behavior and give quick evidence of regulatory compliance.*

### The Challenge

IT security administrators face a true challenge in getting actionable information from the vast audit and log data associated with the many layers of security systems now required to keep enterprise assets safe. Hacker and malware threats are increasing exponentially and becoming more and more complicated to manage, and with regulatory compliance obligations growing, there’s too much data noise to combat and not enough useful information to act on.

### The Solution

Secure Firewall Reporter software delivers central monitoring, correlated alerting, and reporting of Secure Firewall (*Sidewinder*) and Secure SnapGear audit streams to identify real security threats from meaningless noise. It gives immediate action points to keep the enterprise safer. The graphically rich tool strengthens your overall security posture, gives quick evidence of regulatory compliance, and proves the effectiveness and value of your Secure Computing® investment to management.

### A Central, One-Stop Solution

Secure Firewall Reporter provides a central aggregation point for data from one to many thousands of Secure Computing Network Gateway Security appliances globally, making it scalable to the largest enterprises. You receive a complete picture of the enterprise with no wasted man hours in manual log analysis from separate devices.

### Actionable Information in Real Time

Collecting, monitoring, correlating, and threat alerting happen in real time for decisive, intelligent action. Actionable information is prioritized by business impact so you can minimize response time and take corrective action before sensitive information is accessed or a threat has spread across the network.

### IT Security Investment Value Becomes Visible and Tangible

Using security products from Secure Computing, you have much less unwanted and infected traffic entering your network, especially when using Secure Computing TrustedSource™ reputation-based global intelligence, which drops well over 70% of unwanted spam instantly at the outside edge. This incredibly positive security impact is made visible and tangible with Secure Firewall Reporter’s TrustedSource Global Reputation Report.



*Figure 1: Secure Firewall Reporter’s vast capabilities identify and report real security threats automatically, and take the pain out of regulatory compliance with full template reports.*

# The Personalized Dashboard Experience – Monitoring, Alerting, and Event Management

## Real-Time Dashboard Monitoring

Get a quick and easy-to-understand bird's eye view of the environment with the graphical Dashboard.

- The customizable Dashboard shows six security measures at a glance. Choose the security measures that are useful to you on your portal.

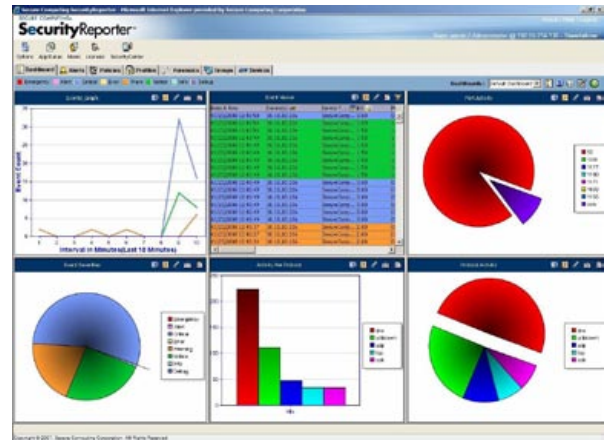


Figure 2: The Dashboard – A real-time, personalized snapshot of security measures you choose, for the information you want, how, and when you want it.

## Alerting and Event Management

Create and define any number of alerts to trigger automated response strategies. Identify real threats from data noise, reduce false positives, and get visibility to blended attacks.

- Event Manager prioritizes events based on business impact for decisive, strategic action before an incident occurs.

## Advanced Alerting Provides Personalization as Well

<b>Event Classification</b>	Classify events based on each policy and apply which queries will be affected by the classification.
<b>Threat Level Classification</b>	Change the event severity of the threat level based on policies.
<b>More Alerting Choices</b>	Users can set alert correlation interval, severity of alerts, precedence, and can negate per alert rule. Includes pattern analysis based on filter expressions.

### Secure Firewall (Sidewinder)

#### Device Compatibility:

- Secure Firewall (Sidewinder) 7.0 or higher and Secure Firewall 6.1.1 or higher

### Secure SnapGear

#### Device Compatibility:

- Secure SnapGear firmware version 3.1.5u3 or higher

#### Minimum System Requirements:

- Processor – Pentium 4 – 2.8 GHz
- Disk space – 10 GB
- RAM – 1 GB
- Operating System – Windows® NT/2000/XP/2003
- Java 2 Runtime Environment JRE v1.5 u6 and above
- Internet Explorer 6.0 or any DOM-compatible Web browser with Shockwave Flash plug-in

#### Recommended System Requirements:

- Processor – Pentium 4 – 2.8 GHz or higher
- Disk space – 20 GB or higher
- RAM – 2 GB or higher
- Operating System – Windows server 2000 or 2003
- Java 2 Runtime Environment JRE v1.5 u6 and above
- Internet Explorer 6.0 with Shockwave Flash plug-in

## Reporting Benefits: Advanced Security Intelligence

**Broad, Exhaustive Reporting** – 300 reports allow you to proactively secure the network, manage bandwidth requirements and ensure appropriate usage. Historical attack reports can be generated for events categorized by hour, day, week, month, quarter, and current comparison by each device, as well as across all devices.

<b>Spam, Spyware, and Anti-Virus</b>	Over 100 reports identify Spam, spyware and viruses across enterprise networks, and provide information on virus type, source, destination, frequency, file name, extension, and protocol.
<b>TrustedSource Global Reputation Report</b>	Graphically see the Spam that has been dropped at the network edge using the industry-first, reputation-based filtering of TrustedSource. Quickly shows the large value of your Secure Computing investment.
<b>Protocol and Web Usage</b>	Provides a firm handle on protocol and Web usage by user, department and/or device. Identifies inappropriate usage including user activity associated with the URL filtering enabled on security appliances.
<b>Bandwidth Usage</b>	See bandwidth utilization by department, client, and protocol.
<b>Regulatory Compliance</b>	Report templates take the pain out of regulatory compliance for Sarbanes-Oxley (SOX), PCI, HIPAA, GLBA, and FISMA.
<b>Configuration Management</b>	Show configuration change detail to prove that corporate networks are configured to government requirements.

### Easy, Automated Report Generation and Distribution

- Email reports automatically to multiple recipients on a scheduled basis and ad-hoc.
- Formats include: HTML, MHTML, PDF, Word, Excel, and Text

## Forensics Analysis Benefits – Regulatory Compliance

Secure Firewall Reporter's monitoring, alerting, and reporting tools also take the pain out of regulatory compliance, and can identify anomalies and employee corporate policy violations.

### Expansive Tools for Forensics Include:

**Ready-Made Compliance Reports** – Complete report templates streamline annual efforts associated with Sarbanes-Oxley (SOX), PCI, HIPAA, GLBA, and FISMA. Compliance audits can be efficient with quick evidence and not a drain on time.

**Configuration Management Report** – Complementing the compliance reports, show configuration change detail to prove that corporate networks are configured to meet government requirements.

**Powerful Drilldown with Workbench** – The Workbench event drilldown feature quickly displays forensic quality details. See 2nd- and 3rd-level detail with a single click.

**Log Archiving for Compliance** – Automatic log storage compresses, encrypts, and archives log files for investigative analysis and regulatory compliance. Easily search hundreds of gigabytes of log data as needed.

Workbench	
Choose Action: [Drill down]	
Column Name	Value
Date & Time	04/11/2007 10:58:27
Group	Default Group
Device(s)	10.10.10.136
Device Type	SecureComputingSidewinder
BIT	2.00
Flow	0
Source IP	221.12.113.238
Destination	192.55.214.136
Protocol	udp
Event ID	UDP netprobe
Event Category	Kernel
Event Class	Unknown
Dest. Port	1027
Event Description	Policy Violation:Network packet probe
Attack ID	UDP netprobe
Virus	Unknown
Virus ID	Unknown
Interface	em0
URL	Unknown
Native Log	Apr 11 10:56:41 auditd: date="Apr 11
Priority	Warning (4)

Figure 3: Workbench drilldown

## System Conveniences

### Anytime, Anywhere Access, and Management

Browser-based access allows report generation from any computer on the local network or remotely.

### Installation Is Straight Forward and Simple

Easy-to-use and requires little or no installation help. Installs on any system running Windows NT/2000/XP/2003 and is completely managed through a browser (Web-based interface).

### Embedded Database and ODBC Support

Stores syslog data using a powerful embedded database.

### International Language Support

Generates reports in English, Japanese, and Korean languages.



Figure 4: Typical Secure Firewall Reporter Setup

Note: Some reporting functions require optional Secure Firewall (Sidewinder) and Secure SnapGear "add-on modules" be purchased. Some reporting functions are dependant on which Secure Computing appliance has been deployed.



### For More Information

Contact your local reseller, or Secure Computing at:  
 1-800-379-4944 (inside U.S.)  
 1-408-979-6100 (worldwide)  
[sales@securecomputing.com](mailto:sales@securecomputing.com)  
[www.securecomputing.com](http://www.securecomputing.com)

## Secure Computing Corporation

### Corporate Headquarters

55 Almaden Blvd., 5th Floor  
 San Jose, CA 95113 USA  
 Tel: +1.800.379.4944  
 Tel: +1.408.494.2020  
 Fax: +1.408.494.6508

### European Headquarters

Berkshire, UK  
 Tel: +44.(0).1344.312.600

### Asia/Pacific Headquarters

Wan Chai, Hong Kong  
 Tel: +852.2598.9280

### Japan Headquarters

Tokyo, Japan  
 Tel: +81.3.5339.6310

For a complete listing of all our global offices, see  
[www.securecomputing.com/goto/globaloffices](http://www.securecomputing.com/goto/globaloffices)