Sandstorm *Secures Enterprise Networks Using Embedded MySQL*

Sandstorm Enterprises develops software to prevent, detect and fix network malfunctions and network security vulnerabilities. Their customers include the Boston Children's Hospital and the Medford, Massachusetts Police Department, Wisconsin Public Service and segments of the Aerospace Industry.

As network performance issues and security threats become more severe and harder to counter, enterprises need advanced tools to help detect network inefficiencies and uncover security breaches. Existing network monitoring and Intrusion Detection Systems (IDS) cannot provide all the information that network managers need to pinpoint network problems and investigate security breaches. Instead, users are forced to manually inspect network traffic and data, which is extremely time consuming and makes getting an in-depth view of what has crossed a network nearly impossible.

To solve this problem, Sandstorm Enterprises developed NetIntercept, a network monitoring and auditing device that is delivered as a complete solution with software pre-installed. NetIntercept relies on MySQL to store and structure the searchable data to identify network and network security issues in the most demanding customer environments.

Sandstorm Enterprises®

"MySQL enabled us to deliver an award-winning, cost-effective network analysis solution that works out of the box. Also, only MySQL provides the performance to meet the high volume requirements of our enterprise customers."

James Van Bokkelen
President
Sandstorm Enterprises, Inc.

MySQL®

Protecting Enterprise Assets

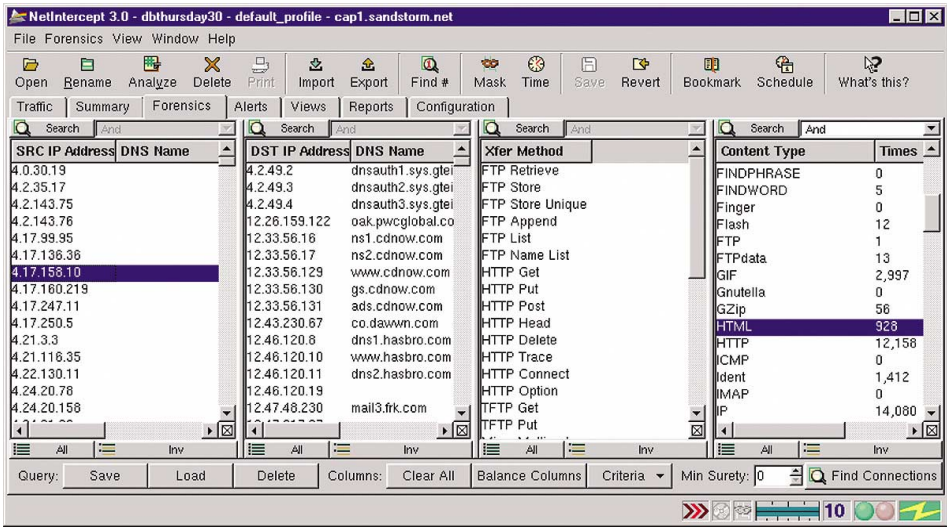
Requirements

Organizations face a number of network concerns on a daily basis including:

- Network performance issues
- Confidential information being emailed to individuals outside of the organization
- Internal files being sneaked out of the organization via FTP
- System exploitation by hackers

These are growing concerns that CIOs must manage using existing IT resources. Therefore, organizations need the right tools that help them locate 'needles' of information in the 'haystack' of raw data. These tools must be:

- Easy to use to readily detect and resolve network issues
- High-performance and scalable to process terabytes of historical data
- Cost-effective so they do not drain an organizations financial resources
- Low Maintenance so they don't require specialized skills to set-up and maintain



NetIntercept gives users the most in-depth view of their network traffic infromation.

Organizations have numerous tools to monitor networks and stop security breaches, including log files from servers, firewall records, Intrusion Detection Systems, and Network Monitoring Solutions.

However, these existing tools have their shortcomings. For example, Network Monitoring Solutions do an excellent job of helping organizations optimize network performance by measuring how much data is sent, when and by whom, but they can't analyze or identify the data in the packets.

In order to address violations of the network and network misuse, IT managers need to also understand the data being sent over their corporate networks. To do this, IT managers have to go through the painstaking task of sifting through raw network packets and piecing together packet streams. With the sheer volume of network traffic, this effort would take days or weeks to complete: not a scalable or viable solution.

A Complete Network Monitoring and Auditing Device

NetIntercept addresses these challenges by delivering an innovative solution that relies on MySQL to:

- Store data mined from network traffic to greatly simplify locating connections of interest
- Quickly analyze network traffic and easily report on data as part of a routine monitoring and security strategy
- Discover data and network abuse such as security and usage violations using a graphical interface to browse the dashboard

NetIntercept gives users the most in-depth view of any Network Forensics tools.

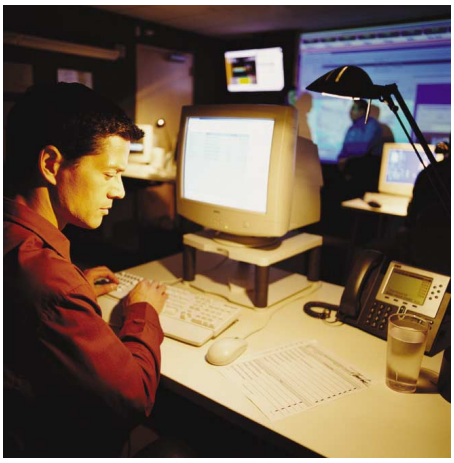
Using NetIntercept, IT Managers can:

- Interactively view network traffic categorized by many attributes such as time of day, user name, and content type
- Search traffic by hundreds of criteria such as user names, key words, phrases, and IP addresses
- Generate many different types of traffic reports that can be scheduled and run automatically to identify trouble spots
- Scan for illicit file types, file names, or content within files such as Microsoft Office documents, TAR and .ZIP files that are being sent across the network through the storage of meta data information in MySQL

Sandstorm chose MySQL because it provides:

- **High-performance** to load up to 1 million network TCP connections, enough to handle the demands of the world's largest networks with multi-terabyte disk arrays.
- **Easy to use, zero administration** database that allows customers to use NetIntercept out of the box and be immediately productive.
- **Cost-effective** database that resulted in NetIntercept earning the Best Value Award from Computerworld's Security Pipeline.
- **High reliability** database allowing Sandstorm customers to continuously benefit from uninterrupted service.

Sandstorm also relies on the robustness of MySQL in their other Information Security offerings.



PhoneSweep, the world's most popular commercial telephone scanner (war dialer) relies on MySQL and enables organizations to find unauthorized and vulnerable modems.

NetIntercept, as well as Sandstorm's other products quickly become indispensable tools for IT managers who need to investigate network issues and violations such as performance problems, identifying confidential data being sent out of the organization and studying external break in attempts. With NetIntercept, users are exponentially more productive in fine-tuning and securing their corporate networks.

MySQL®

Technical Specifications

Hardware:	Dell
OS:	Free BSD
CPU:	Dual Intel Xeon 2.4 GHz
RAM:	2 GB
Hard Drive:	1 TB
Database:	MySQL Server
Database Size:	1 GB

About MySQL

For over ten years, MySQL has been an attractive choice among leading technology companies worldwide, due to its award-winning speed, scalability and reliability. Our reputation has been built on understanding the needs of OEM customers and delivering the low-cost software, support and services to make them successful. More than 100 companies have embedded or bundled MySQL with their market-leading products, including Adobe, Cisco, Motorola, NEC, Nortel, NetIQ, SAP, SAS, Siemens, Sony, and Symantec.

For more information about MySQL, please go to **www.mysql.com/oem**

The World's Most Popular Open Source Database