

Full Data Mining & Forensics Capabilities

The Web Log Problem

Over 80 % of the traffic leaving an enterprise is HTTP and HTTPS traffic. This traffic generates a massive amount of logs: the web traffic of a typical Fortune 500 company generates 30-100 Gigabytes of web logs everyday. Worse, there are no easy tools that provide either consolidated reporting or specific data mining. Companies with multiple Internet gateways generate multiple, disjointed web logs, which do not provide a consolidated view of overall corporate Internet activity.

Current Solutions

Most companies need to store web logs for at least a year. Current web log solutions use relational databases, which do not scale to handle such large amounts of data storage. They are too slow to access and analyze information. In addition, companies spend a great deal of money on storage media to save logs that cannot be effectively retrieved and used.

NanoLog Technology

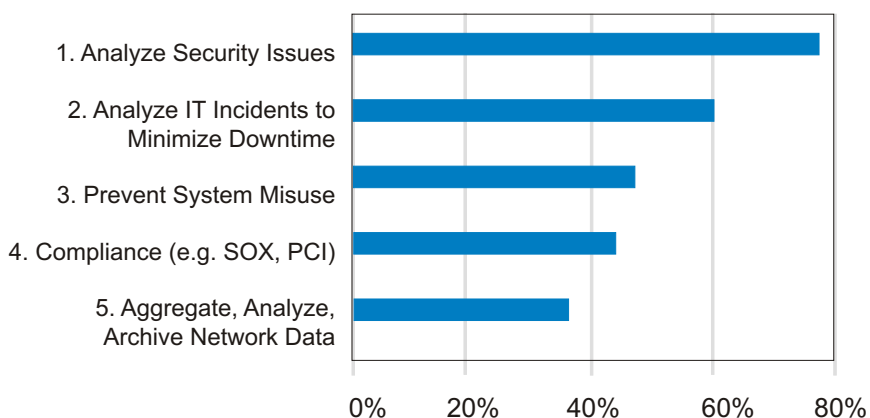
Efficient Storage of All Internet Activity

Zscaler's web log technology, NanoLog, can handle enormous amounts of data for storage and analysis. It allows organizations to analyze information about Internet use, such as employee activity, web mails and attachments sent, information published on social networking sites, or instant messaging transcripts with partners or competitors.

Granular Data Mining Capabilities

Zscaler allows companies to mine web logs for investigations, either for regulatory reasons or internal inquiries. Companies can see a drill-down of activities of specific periods of time, employees, departments, locations, and more. For example, which employees at the Atlanta office sent an IM message with an attachment, including confidential information, to a competitor? In addition to analyzing specific behavior, Zscaler gives organizations a better understanding of broad traffic trends, which provides insight into anomalous behavior and planning for bandwidth and network requirements.

Figure 1:
The top five reasons companies keep web logs, according to a 2008 SANS report. Event detection for security is the number one reason.



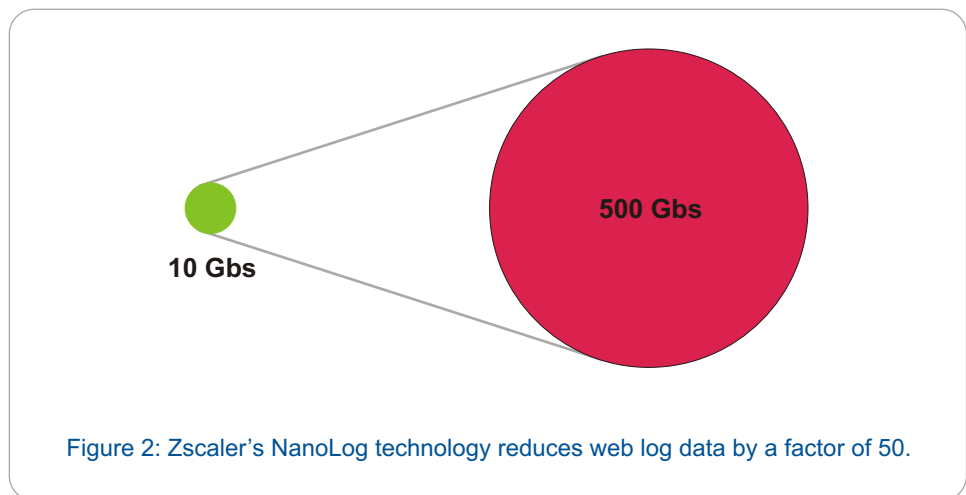
Full Data Mining & Forensics Capabilities

Our Technology

Patent-Pending Technologies for Efficient Storage & Query

NanoLog uses three key technologies: differential data technology, indexing, and compression. Together, these technologies reduce web log data by a factor of 50. A typical web log for each transaction is 500 bytes; without discarding any information, NanoLog reduces it to 10-12 bytes. For a company typically requiring 500 Gigabytes of storage per month, NanoLog requires 10 Gigabytes.

Zscaler also consolidates web logs from multiple Internet gateways into one central location in real-time and provides rapid response time for creating queries and analyzing data. Efficient storage allows organizations to keep web logs for a longer time, which may be required by law.



Solution Benefits

Flexible & Powerful Reporting and Analysis

Zscaler provides organizations a flexible & powerful system to view the broad trends and traffic patterns of Internet activity, as well as drill down to specific events. Our technology reduces the cost for web log retention and offers high-speed web log retrieval. In addition to helping organizations meet their regulatory obligations, Zscaler provides organizations with a complete picture of their Internet activity that can be used for managing new policies and forecasting Internet bandwidth requirements.

Contact Us

Zscaler, Inc.

Visit: www.zscaler.com Email: info@zscaler.com