Q1Labs®
Total Security Intelligence

QRadar Log Manager

Real-Time Log Management for Defending the Network and Meeting Compliance Mandates

Providing comprehensive, high performance and future-proof log management for organizations looking to collect, archive, secure and analyze large volumes of network and security event logs for security, auditing and reporting requirements

Easily Meet Compliance Mandates

With over 2000 out of the box rules and reports, organizations can confidently meet auditing and reporting requirements for compliance mandates such as PCI, Sarbanes-Oxley, HIPAA, NERC CIP, and GLBA. Automated alerts to security response teams enable real-time policy enforcement.

Visibility into Log Data for Actionable IT Operations and Security Forensics

Most organizations generate huge volumes of logs and manually analyzing them can pose many challenges. With QRadar® Log Manager's flexible query engine, diverse log data is aggregated and correlated into actionable IT forensics for identifying patterns of attack, anomalies, access and usage of confidential data and insider threats. With out of the box correlation rules and pre-defined security, policy and compliance-driven searches, an organization can easily analyze all logs, generate comprehensive reports and reduce risk by investigating and resolving security threats faster.

Improve Efficiency Collecting and Archiving Logs

QRadar Log Manager easily collects and stores massive amounts of data by scaling to support hundreds of thousands of events per second. And with high compression, significant reduction is realized for efficient log storage which can eliminate the need for external storage.

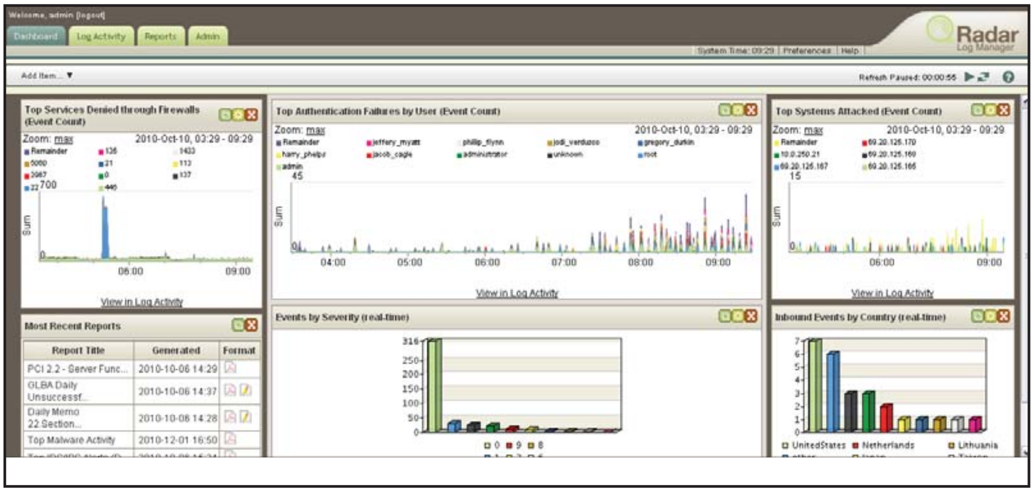
Turnkey Solution Allows for Immediate Results

The QRadar Log Manager appliance architecture provides a streamlined and easy to deploy solution for secure and efficient log management. QRadar Log Manager reduces complexity and is easy to manage with an embedded log repository and integrated log collection from a wide variety of network and security devices.

QRadar® Log Manager

QRadar® Log Manager helps security teams, IT operations, auditing and lines of business:

- EXCEED REGULATION MANDATES
- RESOLVE THREATS FASTER
- DEFEND THE NETWORK
- IMPROVE EFFICIENCY AND OPERATIONS

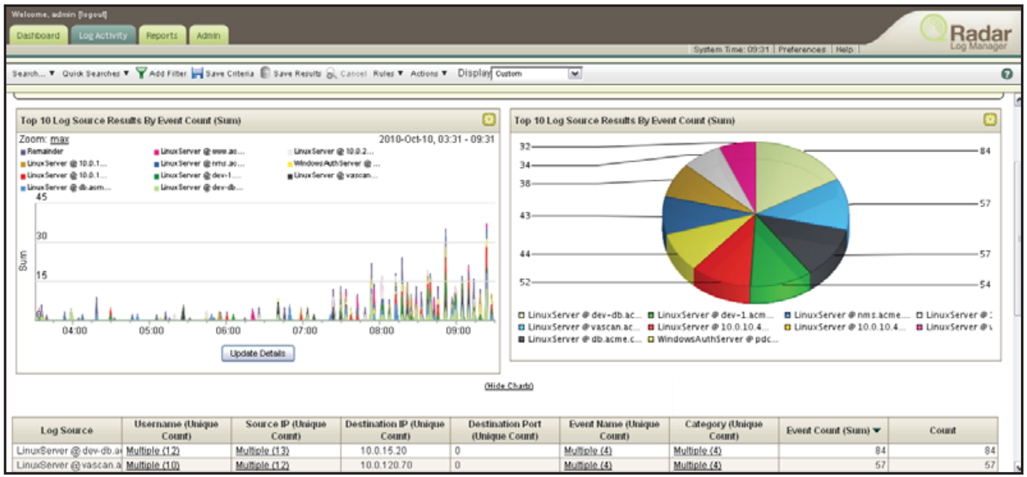


Report Title	Generated	Format
PCI 2.2 - Server Func...	2010-10-06 14:29	
GLBA Daily Unsuccessf...	2010-10-06 14:37	
Daily Memo 22 Section...	2010-10-06 14:28	
Top Malware Activity	2010-12-01 16:50	

Customizable dashboard offers role-based access by function and a global view to real-time log analysis, incident management and reporting.

Q1 Labs®
Total Security Intelligence

QRadar Log Manager



Log Source	Username (Unique Count)	Source IP (Unique Count)	Destination IP (Unique Count)	Destination Port (Unique Count)	Event Name (Unique Count)	Category (Unique Count)	Event Count (Sum) ▼	Count
LinuxServer @ dev-db.a	Multiple (12)	Multiple (13)	10.0.15.20	0	Multiple (4)	Multiple (4)	84	84
LinuxServer @ vascan.a	Multiple (10)	Multiple (12)	10.0.120.70	0	Multiple (4)	Multiple (4)	57	57

Log Activity allows for custom viewing of log sources as well as drilling down to a time series view for long-term trending of data.

Drill Down Capabilities Put You In Control

With a highly intuitive centralized user interface that offers role-based access by function and a global view to access real-time analysis and reporting, QRadar Log Manager provides a solid and straightforward foundation for an organization's security or networking team. Default dashboards are available by function and users can create and customize their own workspaces to monitor specific activities and drill down to a time series view for long-term trending of data. This makes it easier to identify anomalies or possible threats to the organization.

Reliable, Scalable and Tamper Proof Log Storage

QRadar Log Manager delivers up to 6 Terabytes of fault tolerant storage per appliance for archiving event logs and supports extensive log file integrity checks, including NIST Log Management Standard SHA-x (1-256) hashing for tamper-proof log archives. A distributed architecture allows for scalable storage up to hundreds of Terabytes. The embedded purpose built database is self-maintaining for ease of use and lower total cost of ownership.

Comprehensive Device Support

QRadar Log Manager supports log management for a wide variety of network and security devices including: Routers/Switches, Firewalls, Virtual Private Networks (VPNs), Intrusion Detection/Prevention Systems (IDS/IPS), Anti-virus Applications, Host & Servers, Database, Mail and Web Applications, Custom Devices and Proprietary Applications. QRadar Log Manager normalizes all data into a simple to understand yet flexible taxonomy which facilitates easy searching, correlation and reporting across a diverse security and network device landscape.

Future-proof Growth Path for Full Security Information and Event Management (SIEM)

QRadar Log Manager processes and normalizes every event making it easy to gain security intelligence while also providing an organization with a future proof path for transitioning to SIEM. As part of the QRadar Security Intelligence Platform, QRadar Log Manager provides a seamless migration path from simple Log Management to full SIEM through a license upgrade.

High Availability for Automatic Failover

By adding on QRadar High Availability, an organization can take advantage of automatic failover and full disk synchronization between systems - a capability that is typically only available with costly, manually-implemented software and storage solutions. High availability of data storage and analysis is easily deployed through architecturally-elegant plug-and-play appliances.

Q1 Labs
890 Winter Street, Suite 230
Waltham, MA 02451 USA
1.781.250.5800, info@Q1Labs.com

The specifications and information contained herein are subject to change without notice.