IBM Security QRadar Log Manager

Real-time log management for defending IT infrastructures and meeting compliance mandates

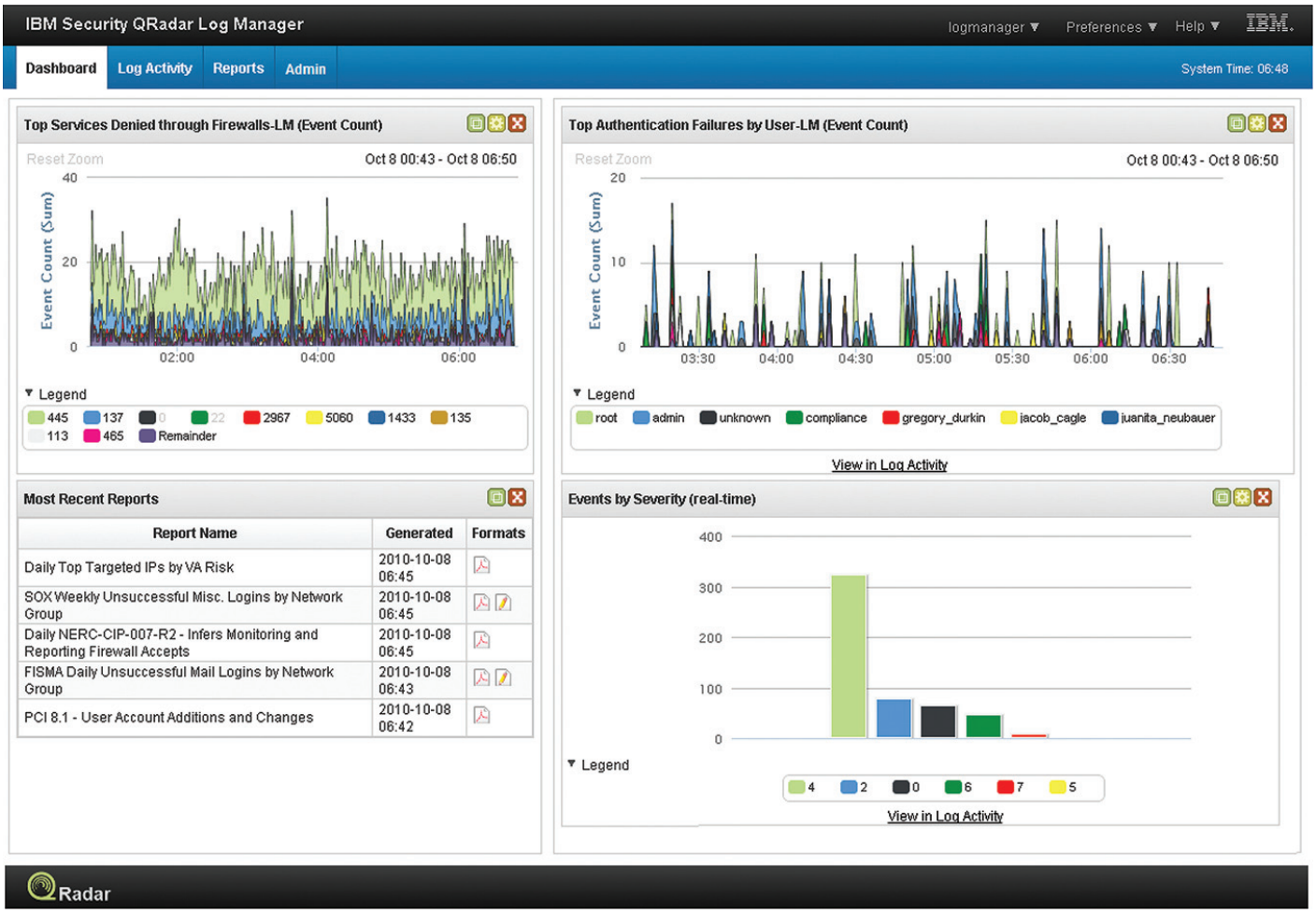
Highlights

- Generate actionable IT forensics by aggregating and correlating a diverse set of logs and events
- Capture event data from security and network devices, servers, endpoints and applications within a federated repository with a single global view
- Easily perform forensics, application and network troubleshooting across normalized data for simplified searching
- Scale to support hundreds of thousands of events per second, per system
- Help exceed regulatory mandates with rich compliance-reporting capabilities
- Preserve investments by enabling the addition of integrated security information and event management (SIEM) technology

Organizations looking to collect, analyze, archive and securely store large volumes of network and security event logs need a high-performance, easy-to-use, comprehensive log management system. This is especially important on today's smarter planet, where instrumented, interconnected and intelligent businesses generate and store more information than ever before. IBM® Security QRadar® Log Manager analyzes all the data from various network and security devices, servers and operating systems, applications, and a wide assortment of endpoints to provide near real-time visibility into developing threats and to meet continuous compliance-monitoring requirements.

Gain visibility into log data for actionable IT forensics

Most organizations generate huge volumes of logs, but manually analyzing them can be challenging and can consume an inordinate amount of staffing resources. With the QRadar Log Manager flexible query engine, diverse log data is aggregated and correlated into actionable IT operations and security forensics to help identify patterns of attack, anomalies, access and use of confidential data and insider threats.



The customizable QRadar Log Manager dashboard offers role-based access by function and a global view to real-time log analysis, incident management and reporting.

Drill down to obtain efficient event investigations

QRadar Log Manager provides a solid, straightforward foundation for security or networking teams through a highly intuitive, centralized user interface. Default dashboards are available by function, and users can create and customize their own workspaces to monitor specific activities or drill down to a time-series view for longer-term data trending. This makes it easier to identify anomalies and possible threats or to review network usage and performance to help meet IT service-level responsibilities.

Receive comprehensive device support for capturing all network events

QRadar Log Manager collects data across a wide variety of network and security devices, including routers and switches, firewalls, virtual private networks (VPNs), intrusion detection/prevention systems (IDS/IPS), anti-virus applications, hosts and servers, databases, mail and web applications, custom devices, and proprietary applications.

Events are collected through a Device Support Module interface, in which an advanced, two-level normalization taxonomy is used to assign common terms to similar events coming from widely divergent log sources. A customized rules engine processes each incoming event in real time, assigning severity, credibility and relevance attributes and triggering an appropriate response via email notification, dashboard posting or by adding the event to a reference set of similar activity for further monitoring.

Deploy scalable appliances to expand coverage

QRadar Log Manager appliance architecture configurations range from an all-in-one hardware or software solution to an enterprise architecture using a centralized console and any number of distributed event processor and event collector appliances. QRadar Log Manager easily scales to support hundreds of thousands of events per second within a single, unified database structure.

It delivers up to 16 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 enables scalable storage of up to hundreds of terabytes. The embedded purpose-built database is self-maintaining for ease of use and lower total cost of ownership.

Administrators can establish data-retention periods based on a granular policy in order to meet specific internal requirements or regulations. A customizable event-indexing capability optimizes performance by allowing the use of any database field, and reporting features identify usage and disk space consumption. QRadar Log Manager also compresses older data to further extend retention periods.

Ease the burden of security today—and tomorrow

With more than 2,000 out-of-the-box rules and reports, QRadar Log Manager helps organizations confidently meet auditing and reporting requirements for compliance mandates, from Payment Card Industry (PCI), to Health Insurance Portability and Accountability Act (HIPAA), to Gramm-Leach-Bliley Act (GLBA). Automated alerts to security response teams also help users achieve real-time policy enforcement.

Organizations can use QRadar Log Manager to help raise their security awareness, as well as to help them discover suspicious events previously lost in the “noise” of network activities. As part of the IBM QRadar Security Intelligence Platform, QRadar Log Manager provides a seamless migration path from

log management to full SIEM technology through a simple license upgrade—easing the transition from security incident management to full-blown security intelligence.

Build security with high-availability and disaster-recovery options

Adding QRadar high-availability solutions can help organizations take advantage of automatic failover and full disk synchronization between systems—a capability typically available only with costly, manually implemented software and storage solutions. Users can easily deploy high-availability data storage and analysis through advanced plug-and-play appliances.

QRadar disaster-recovery appliances provide a means of safeguarding all collected log source data by mirroring it to a secondary, identical backup QRadar deployment.

Why IBM?

IBM operates the world's broadest security research, development and delivery organization. This comprises 10 security operations centers, nine IBM Research centers, 11 software security development labs and an Institute for Advanced Security with chapters in the United States, Europe and Asia Pacific. IBM solutions empower organizations to reduce their security vulnerabilities and focus more on the success of their strategic initiatives. These products build on the threat intelligence expertise of the IBM X-Force® research and development team to provide a preemptive approach to security. As a trusted partner in security, IBM delivers the solutions to keep the entire enterprise infrastructure, including the cloud, protected from the latest security risks.

For more information

To learn more about IBM Security QRadar Log Manager, contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/security

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
January 2013

WGD03020-USEN-00