



---

## Highlights

- Increase visibility into activities across virtually all your IT platforms
  - Tap into the expertise you need to help improve your security posture
  - Rapidly identify and resolve operational and security issues
  - Help meet regulatory compliance requirements
  - Operationalize your security investments and avoid capital expenditures
- 

# IBM Managed Security Services – intelligent log management

Log data can provide critical insights to help support your compliance, security and overall business objectives. But midsized organizations face challenges around shrinking IT staffs and budgets along with increasing complexity in their environments. What's more, the growing sophistication of cyber attacks and the need for robust defenses to counter them means that you can no longer look to log management for simple aggregation, display and storage—especially in a hybrid environment with multiple IT platforms.

IBM® Managed Security Services – intelligent log management can provide improved visibility and insight into your network and IT infrastructure using the IBM Threat Insight Platform. With a more automated and proactive approach to security management, IBM can help you better manage compliance requirements for various regulations such as Payment Card Industry Data Security Standards, the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act and the Sarbanes-Oxley Act—while also supporting a more informed defense strategy against sophisticated attacks, even in a hybrid environment.

## Helping improve visibility across your existing and evolving infrastructure

Intelligent log management is a cloud-based service designed to provide you with around-the-clock log management that includes time stamped collection, normalization and correlation. Powered by IBM QRadar®



technology, it uses hosted, multi-tenant technology to provide intelligent log management capabilities. It can provide you with a single view of your security posture across the enterprise, with flexible service options to consume the right amount of service for the right devices, and make changes as and when your security capabilities mature or your needs change.

Intelligent log management supports more than 450 platforms to help ensure that you capture logs from nearly any device that your business requires, including servers, applications, databases and networking nodes, and has a number of pre-built reports to help support your business management requirements.

Midsized organizations need the ability to invest in an option that allows them to scale and grow over time as they seek to advance their security posture. Intelligent log management is an entry-level service—a gateway to a suite of increasingly sophisticated security information and event management (SIEM) capabilities that IBM offers. As your requirements and budget change, you can seamlessly upgrade to get additional features and functionality—all the way to full IBM QRadar SIEM capabilities.

### **Providing expertise whenever you need it**

To meet the growing business demands of your security program, intelligent log management can supplement your staff with the expertise of IBM threat managers and analysts. Managed security services can be added at any time through IBM Threat Insight Platform cloud-based technology. You can chat with an IBM Security specialist to help resolve issues at any time during the year. You can also get top-level security information with IBM X-Force® Exchange—a threat

intelligence-sharing platform that supports research on security threats, aggregation of intelligence and collaboration. Logged-in users have integrated access to all the functionality of the site—including search, commenting, collections and sharing. The IBM Managed Security Services online portal facilitates real-time search, reporting and auto alert capabilities.

### **Making your security investment an operating expense**

Intelligent log management lets you “pay as you go”—with a reduced-cost operating expenditures model, virtually eliminating the need for hardware and other capital expenditures for log management. Billing is based on required events per second and retention periods, with scaling and deployment options designed to meet the needs of dynamic, hybrid IT environments. Other features can include:

- Flexible service tiers
- Around-the-clock log collection
- Automated policy-based event alerting
- More rapid scale and deployment options
- Scalable log retention—one year online (up to seven years archival available)
- Health and availability monitoring
- High-availability service level agreements (SLAs)
- Configurable rules and thresholds, with critical content updates within 72 hours

Intelligent log management helps you get the security expertise and insight you need, as you need it, to help safeguard your organization—all from a company committed to protecting your critical assets and giving you peace of mind.



IBM operates one of the broadest enterprise security research, development and delivery organizations, with 34 IBM Security locations worldwide.

## Why IBM?

Integrated security intelligence from IBM helps protect businesses from cyber threats around the world. IBM consultants are certified by many leading security associations in penetration testing, analysis, and incident response and forensics. With 10 security research centers, 10 security operations centers and 14 security development laboratories, IBM also has more than 1,000 security patents and manages tens of thousands of security devices for thousands of clients worldwide. IBM systems monitor 15 billion network events for our clients each day across 133 countries.<sup>1</sup>

## For more information

To learn more about IBM Managed Security Services – intelligent log management, please contact your IBM representative or IBM Business Partner, or visit:

[ibm.com/services/security](http://ibm.com/services/security)

Additionally, IBM Global Financing provides numerous payment options to help you acquire the technology you need to grow your business. We provide full lifecycle management of IT products and services, from acquisition to disposition.

For more information, visit: [ibm.com/financing](http://ibm.com/financing)



---

© Copyright IBM Corporation 2017

IBM Security  
New Orchard Road  
Armonk, NY 10504

Produced in the United States of America  
September 2017

IBM, the IBM logo, ibm.com, QRadar, and X-Force are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at [ibm.com/legal/copytrade.shtml](http://ibm.com/legal/copytrade.shtml)

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

**Statement of Good Security Practices:** IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

<sup>1</sup> Current as of April 2015



Please Recycle

---