



Highlights

- Integrate security information and event management (SIEM), log management, anomaly detection, and configuration and vulnerability management into a unified solution
 - Leverage a single architecture to analyze log, flow, vulnerability, user and asset data
 - Use real-time correlation and behavioral anomaly detection to identify advanced threats
 - Identify high-priority incidents among billions of data points
 - Gain 360-degree visibility into network, application and user activity
 - Automate regulatory compliance with collection, correlation and reporting
-

IBM QRadar Security Intelligence Platform

Providing actionable intelligence for enterprise security and compliance

IBM® QRadar® Security Intelligence Platform integrates SIEM, log management, anomaly detection, and configuration and vulnerability management into a unified solution. By using intelligence, integration and automation to provide 360-degree security insight, this solution delivers superior threat detection, greater ease of use and lower total cost of ownership.

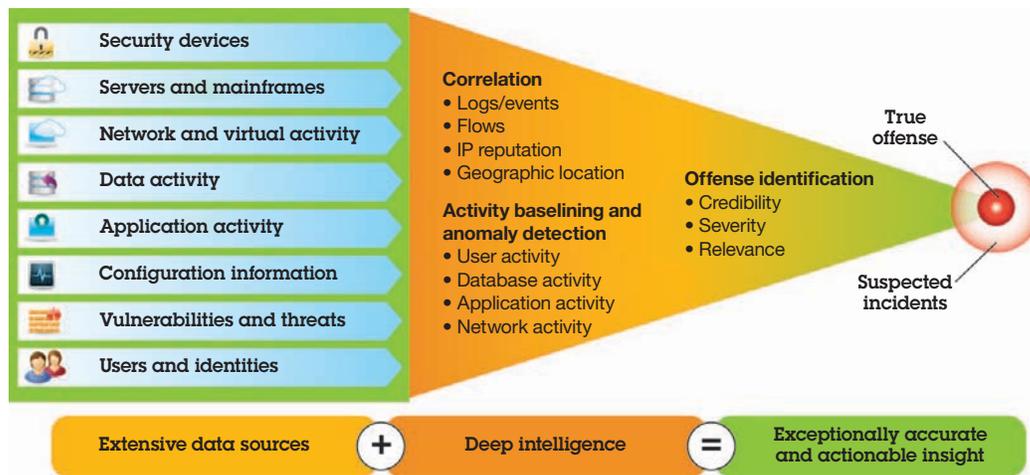
Delivering intelligence, integration and automation

The QRadar Security Intelligence Platform delivers security and compliance benefits that are invaluable on today's smarter planet, where instrumented, interconnected and intelligent businesses collect, process, use and store more information than ever before.

Detect threats that might otherwise get missed

Organizations today are exposed to a greater volume and variety of attacks than in the past. Advanced attackers are clever and patient, leaving just a whisper of their presence. The QRadar Security Intelligence Platform is an integrated family of products that helps detect and defend against threats by applying sophisticated analytics to more types of data. In doing so, it helps identify high-priority incidents that might otherwise get lost in the noise.





IBM QRadar Security Intelligence Platform delivers 360-degree security intelligence.

Consolidate data silos

Although a wealth of information exists in organizations' log, network flow and business process data, this information is often held in silos and ignored or underutilized. QRadar converges network, security and operations views into a unified and flexible solution. It breaks down the walls between silos by correlating logs with network flows and a multitude of other data, presenting all relevant information on a single screen. This enables superior threat detection and a much richer view of enterprise activity.

Detect insider fraud

Some of the gravest threats to an organization come from the inside, yet organizations often lack the intelligence needed to detect malicious insiders or outside parties that have

compromised user accounts. By combining user and application monitoring with application-layer network visibility, organizations can better detect meaningful deviations from normal activity, helping to stop an attack before it completes.

Predict and remediate risks with vulnerability management

Security, network and infrastructure teams strive to manage risk better by identifying vulnerabilities and prioritizing remediation before a breach occurs. The QRadar Security Intelligence Platform integrates configuration and vulnerability management with SIEM capabilities, including correlation and network flow analytics, to provide better insight into critical vulnerabilities. As a result, organizations can remediate risks more effectively and efficiently.

Address regulatory compliance mandates

Many organizations wrestle with passing compliance audits while having to perform data collection, monitoring and reporting with increasingly limited resources. To automate and simplify compliance tasks, QRadar provides collection, correlation and reporting on compliance-related activity, backed by numerous out-of-the-box report templates.

Leveraging easier-to-use security analytics

The QRadar Security Intelligence Platform provides a unified architecture for storing, correlating, querying and reporting on log, flow, vulnerability, user and asset data. It combines sophisticated analytics with out-of-the-box rules, reports and dashboards. While it is powerful and scalable enough for Fortune 500 corporations and major government agencies, it is also intuitive and flexible enough for small and midsize organizations. Users benefit from faster time to value, lower cost of ownership, greater agility, and enhanced protection against security and compliance risks.

Intelligence

By analyzing more types of data and using more analytics techniques, QRadar can often detect threats missed by other solutions and provide network visibility that others cannot.

Integration

With a common application platform, database and user interface, this platform delivers massive log management scale without compromising the real-time intelligence of SIEM and network behavior analytics. It provides a common solution for all searching, correlation, anomaly detection and reporting functions. A single, intuitive user interface provides seamless

access to all log management, flow analysis, incident management, configuration and vulnerability management, dashboard and reporting functions.

Automation

The QRadar Security Intelligence Platform is simple to deploy and manage, offering extensive out-of-the-box integration modules and security intelligence content. By automating many asset discovery, data normalization and tuning functions, while providing out-of-the-box rules and reports, the solution can dramatically reduce the complexity that often cripples other products.

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 the IBM QRadar Security Intelligence Platform, contact your IBM representative or IBM Business Partner, or visit: ibm.com/security



© Copyright IBM Corporation 2013

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
January 2013

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

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.

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 or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a 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 systems and products are immune from the malicious or illegal conduct of any party.



Please Recycle