# IBM Security QRadar

## Visibility, detection, investigation, and response

There is no shortage of challenges facing security teams: an increase in the volume and sophistication of cyberattacks, an explosion of data, an expanding attack surface, disjointed security tools and a shortage of skilled security staff. In fact, organizations are spending hundreds of hours a week investigating suspicious alerts and yet, despite this time spent, close to 17% of alerts are not being investigated.[1] Organizations seeking to protect their customers' identities, safeguard their intellectual property and avoid business disruption need to proactively monitor their environment so that they can rapidly detect threats and accurately respond before attackers are able to cause financial and reputational damage.

IBM Security QRadar®, a market-leading SIEM solution, helps defend against growing threats while modernizing and scaling security operations through integrated visibility, detection, investigation, and response. QRadar provides security teams with centralized visibility into enterprise-wide security data and actionable insights into the highest priority threats. Security analysts can work from one pane of glass to quickly understand their security posture, identify the most critical threats, and drill down to get more details, helping to streamline workflows and eliminate the need to pivot between tools. With QRadar's anomaly detection capabilities, security teams can

### Highlights

- Gain complete visibility into security data from a single pane
- Reduce events into a prioritized list of the most important alerts
- Leverage automated, advanced analytics and threat intelligence to speed investigation time
- Scale rapidly with out of the box use cases and integrations
- Drive compliance and manage regulatory risk

[1] IDC, Insights from IDC's EDR and XDR 2020 Survey: Operational Challenges and Initiatives Are Abundant, Doc #US47357921, January 2021

quickly identify changes in user behavior that could be indicators of an unknown threat.

The solution ingests a vast amount of data throughout the enterprise to provide a comprehensive view of activity throughout on-premises and cloud-based environments. As data is ingested, QRadar applies real-time, automated security intelligence to quickly and accurately detect and prioritize threats. Actionable alerts provide rich context into potential incidents, enabling security analysts to swiftly respond to limit the attackers' impact. QRadar is purpose-built to address a broad spectrum of security use cases and easily scale with limited customization effort required.

## Gain comprehensive, centralized visibility

Enterprise networks can span across traditional on-premises IT, cloud-based and operational technology (OT) environments, all of which require some level of oversight to effectively protect assets, accurately detect threats and maintain compliance. Before security teams can start analyzing data to detect and manage threats, they must first have centralized visibility into disparate security data. QRadar enables organizations to gain centralized, comprehensive visibility into siloed environments by collecting, parsing, and normalizing both log and flow data. From a single pane, security analysts can monitor on-premise, cloud, and hybrid environments.

The solution includes more than 450 pre-built Device Support Modules (DSMs), which provide default setting integrations with other security investments. Customers can simply point logs to QRadar, and the solution can automatically detect the log source type and apply the correct DSM to parse and normalize the log data. As a result, QRadar customers can get up and running much faster than customers of alternative solutions. Additional integrations can easily be added via apps in the IBM Security App Exchange. QRadar also offers a simple DSM Editor with an intuitive graphical user interface

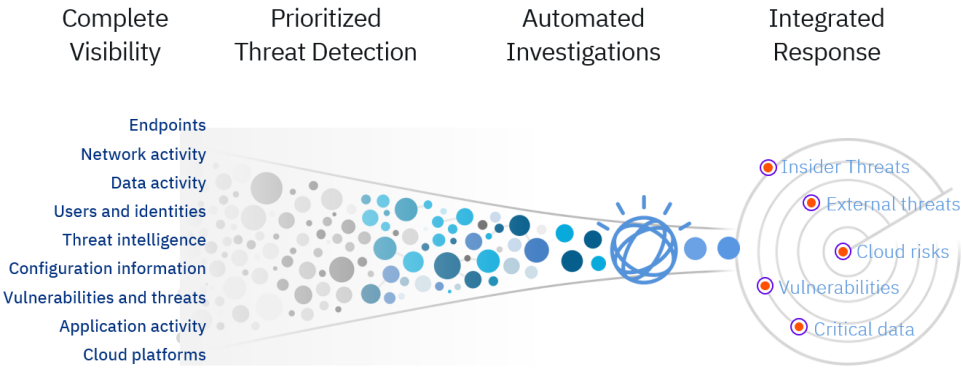
(GUI) that enables security teams to easily define how to parse logs from custom applications.

To help easily establish the asset database, which enables organizations to define critical assets or network segments, QRadar can inspect network flow data to automatically identify and classify valid assets on the network based on the applications, protocols, services and ports they use.

QRadar supports a wide variety of technologies, applications, and cloud services to help customers gain comprehensive visibility into enterprise-wide activity. Once this data is centralized, it can be automatically analyzed to identify known threats, anomalies that may indicate unknown threats and critical risks that may leave sensitive data exposed.

## Automate security intelligence to rapidly detect threats

QRadar is designed to automatically analyze and correlate activity across multiple data sources including logs, events, network flows, user activity, vulnerability information and threat intelligence to identify known and unknown threats.

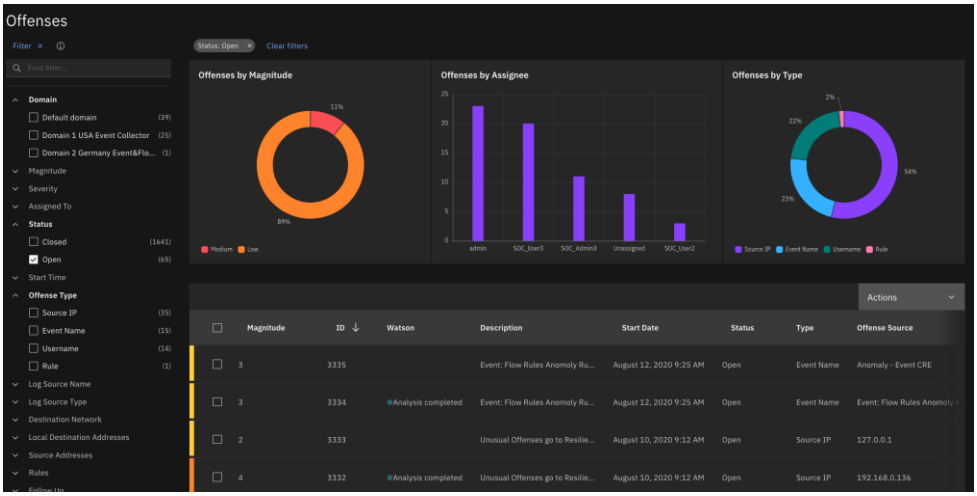



QRadar collects, analyzes, and correlates data from a wide variety of sources to detect and prioritize the most critical threats that require investigation.

QRadar intelligently correlates and analyzes a variety of data types from a wide range of sources, including the following:

- Endpoint data: from the Windows event log, Sysmon, EDR solutions and more
- Network activity data: from firewalls, gateways, routers, or sensors
- Vulnerability data: From antivirus tools, vulnerability scanners, intrusion detection systems, intrusion prevention systems, data loss prevention systems and more
- Cloud activity: From SaaS and IaaS environments, such as Office365, SalesForce.com, Amazon Web Services (AWS), Microsoft Azure and Google Cloud
- User and identity data: Ingested from Active Directory, LDAP, or other identity and access management solutions
- Application data: From enterprise resource planning (ERP) solutions, application databases, SaaS applications and more
- Threat intelligence: From sources such as IBM X-Force® and third-party threat intelligence feeds
- Container activity data: from container management and orchestration technologies software such Kubernetes

QRadar includes hundreds of pre-built security use cases, anomaly detection algorithms, rules, and real-time correlation policies to detect known and unknown threats. As threats are discovered, the solution aggregates related security events into single, prioritized alerts known as “offenses.” Offenses are automatically prioritized based on both the severity of the threat and the criticality of the assets involved.




The Offenses view in QRadar provides a prioritized list of threats

Within each offense, security analysts can see the full chain of threat activity from one single screen. From here, analysts can easily drill down into specific events or network flows to start an investigation, assign the offense to a specific analyst, or close it out. Offenses are automatically updated as new related activity occurs so that analysts can see the most up-to-date information at any given time. This unique approach helps security analysts easily understand the most critical threats in the environment by providing end-to-end insight into each potential incident while simultaneously reducing the total alert volume.

## Identify anomalous network, user and application activity

As attackers become more sophisticated in their techniques, known threat detection is no longer sufficient on its own. Instead, organizations must also have the ability to detect slight changes in network, user or system behavior that may indicate unknown threats, such as malicious insiders, compromised credentials or fileless malware.

QRadar contains a variety of anomaly detection capabilities to identify changes in behavior that could be indicators of an unknown threat. QRadar User Behavior Analytics analyzes user activity to detect malicious insiders and determine if a user's credentials have been compromised. Security analysts can easily see risky users, view their anomalous activities, and drill down into the underlying log and flow data that contributed to a user's risk score.

By optionally using QRadar Network Insights as part of the SIEM deployment, organizations can gain insight into which systems communicated with each other, which applications were involved and what information was exchanged in the packets. By correlating this information with other network, log and user activity, security analysts can uncover abnormal network activity that may be indicative of compromised hosts, compromised users, or data exfiltration attempts.

While QRadar ships with numerous anomaly and behavioral detection rules as default settings, security teams can also create their own rules, tailor anomaly detection settings, and download over 265 pre-built apps from the IBM Security App Exchange to augment their deployment.

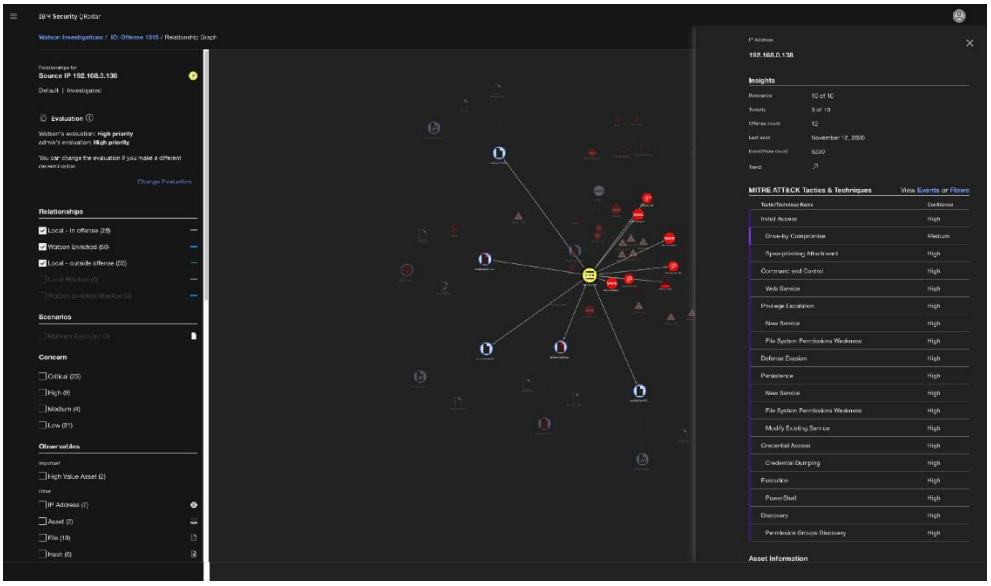
## Reduce investigation time with AI and automation

Security teams are burdened with a high volume of alerts, manual tasks, and limited staff, often leading to burnout and weakening of the organization's security posture. QRadar Advisor with Watson™ uses AI and automation to significantly reduce the time spent investigating threat alerts from days and weeks down to minutes or hours. Advisor provides prioritized alert research and correlated data to help analysts focus on more impactful, strategic analysis and threat hunting – all while using industry-standard MITRE ATT&CK mapping to improve root-cause analysis. This enables faster

remediation, shorter dwell times, fewer missed critical incidents, less analyst fatigue, and improved SOC/analyst efficiency.

QRadar groups and prioritizes all related events under a single offense, providing security analysts with a full view of a potentially evolving attack scenario. The cross-investigation analysis provides rich context on alerts by automatically linking investigations through connected incidents, which reduces duplication of effort and extends the investigation beyond the current probable incident and alert.

In addition, Advisor with Watson provides a combination of cognitive insights and local data mining designed to uncover related indicators of compromise (IOCs). QRadar can graph relationships within an investigation to visualize enriched investigation data and explore connections to other IOCs, assets, users, or investigations.




QRadar can graph relationships between IOCs, assets, users, or other investigations

Advisor also maps the investigation to the MITRE ATT&CK framework, so security teams can visualize attacker tactics and

techniques, drill into events and flows by ATT&CK stage and make more confident decisions.

## Accelerate response times with guided response and case management

The integration of IBM Security QRadar with IBM Security SOAR allows security teams to accelerate incident response times with step-by-step playbooks, automation of manual tasks, and consistent collaboration and coordination with case management. Security analysts can quickly and efficiently escalate suspected offenses from QRadar to IBM Security SOAR, trigger additional automated enrichments, and drive the full investigation process. As the incident evolves, all information is synchronized between QRadar and IBM Security SOAR, ensuring full data integrity. Any new information uncovered by IBM Security SOAR is fed back into QRadar to improve the detection process.

## Better manage compliance with pre-built content, rules and reports

QRadar provides the transparency, accountability, and measurability critical to an organization's success in meeting regulatory mandates and reporting on compliance. The solution's ability to correlate and integrate threat intelligence feeds yields more complete metrics for reporting on IT risks for auditors. Hundreds of pre-built reports and rule templates can help organizations more easily address industry compliance requirements.

Profiles of network assets can be grouped by business function—for example, servers that are subject to Health Insurance Portability and Accountability Act (HIPAA) compliance audits—to help teams more easily report on relevant activity as needed.

QRadar has the experience and resources needed to help organizations address risk and regulatory exposure by providing default setting compliance packages for General Data Protection Regulation (GDPR), the Federal Information Security Management Act (FISMA), Sarbanes-Oxley (SOX), HIPAA, ISO 27001, Payment Card Industry Data Security Standard (PCI DSS) and more. These packages are included free of charge with a QRadar license and are available in the IBM Security App Exchange.

## Easily scale with changing needs

The flexible, scalable architecture of QRadar is designed to support both large and small organizations with a variety of needs. Smaller organizations can start with a single all-in-one solution that can be easily upgraded into a distributed deployment as needs evolve. Larger enterprise organizations can deploy dedicated components to support global, distributed networks with high data volumes.

IBM Security QRadar includes the following components: event collectors, event processors, flow collectors, flow processors, data nodes (for low-cost storage and increased performance) and a central console. All components are available as hardware, software, or virtual appliances. Software and virtual appliance options can be deployed on-premises, in IaaS environments or distributed across hybrid environments.

Regardless of deployment model, organizations can optionally add in high availability and disaster recovery protection where and when needed to help ensure continuous operations. For organizations seeking business resiliency, QRadar delivers integrated automatic failover and full-disk synchronization between systems without the need for additional third-party fault management products. For organizations seeking data protection and recovery, QRadar disaster recovery capabilities can forward live data, such as flows and events,

from a primary QRadar system to a secondary parallel system located at a separate facility.

## Conclusion

IBM Security QRadar is a market-leading SIEM solution that applies automated, intelligent analytics to a vast amount of security data to provide security analysts with actionable insight into the most critical threats, enabling them to make better, faster triage and response decisions.

This comprehensive solution brings together log management, network analysis, user behavior analytics, threat intelligence and AI-powered investigations into a single solution – integrated with IBM Security SOAR for incident response – all with comprehensive visibility across on-premises, cloud, and hybrid environments.

## Why IBM?

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research, provides security solutions to help organizations drive security into the fabric of their business so they can thrive in the face of uncertainty.

IBM operates one of the broadest and deepest security research, development and delivery organizations. Monitoring more than one trillion events per month in more than 130 countries, IBM holds over 3,000 security patents. To learn more, visit ibm.com/security.

---



---

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice and represent goals and objectives only.

## For more information

To learn more about IBM Security QRadar, please contact your IBM representative or IBM Business Partner, or visit the following website: https://www.ibm.com/security/security-intelligence/qradar