IBM Security

IBM

IBM QRadar

Sense and detect modern threats with the most sophisticated security analytics platform

IBM Security White Paper

Conquer the unknown

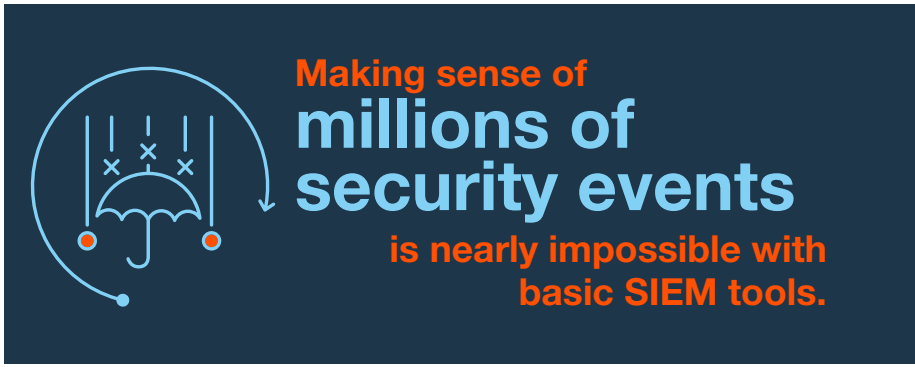
Security professionals live in a world of constant suspense. Threats and attacks hit their organizations from every angle, every minute of every day. When persistent attackers break in, they move slowly and quietly. They hunt for valuable data and they cover their tracks. In fact, a recent survey found that the mean time to identify an attack was 256 days, while the mean time to contain it was 82 days.[1] Consequently, life in a Security Operations Center (SOC) is stressful; many teams just don't know what they don't know.

Gone are the days when security teams could just lock down the perimeter, ban many forms of Internet access and fight the latest fire. Today's organizations demand near-ubiquitous connectivity in order to keep the business moving while simultaneously stopping advanced threats, identifying fraud and rogue insiders, and ensuring continuous compliance. New requirements call for analyzing as much information as possible to detect threatening activities that lurk under the surface—and respond more rapidly. SOC analysts must develop a keen ability to detect deviations from normal activities, and the solutions they choose must be able to scale, reaching every nook and cranny of the enterprise with a single, cohesive platform.

[1] "2015 Cost of a Data Breach Study: Global Analysis," *Ponemon Institute Research Report*, May 2015.

Sense threats and act

To stay ahead, organizations need to be able to "sense" chains of malicious activities in the same way that people sense danger when they see, hear, smell or feel troublesome conditions. They need a security platform that can:

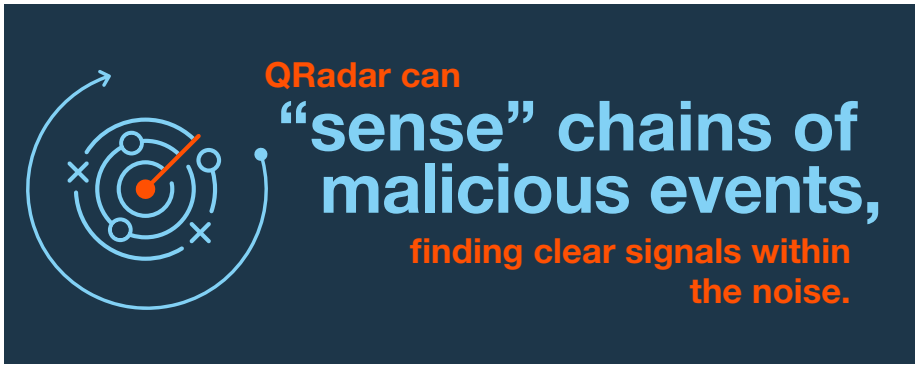


- Deploy rapidly across an entire network, including cloud-based resources
- Detect subtle differences in the environment, such as lurking intruders or rogue insiders
- Discover attacks without depending upon a few highly trained specialists
- Collect, normalize and correlate billions of events, prioritized to a handful of issues
- Identify the important vulnerabilities and risks to prevent a breach

On the bright side, today's SOC analysts no longer have to go it alone. Just as the attackers have banded together to share their insights and techniques, the security community has responded with similarly shared resources. The emergence of these new threat intelligence and application sharing facilities helps limit the effectiveness of new malware and exploit kits, and the impact of zero-day or one-day vulnerabilities. Yet many SOC analysts are still limited by aging log management systems or basic security information and event management (SIEM) solutions that generate excessive alerts using a single instance of suspicious behavior.

Use analytics to eliminate threats

The most serious security breaches don't begin with a big bang. Instead, cybercriminals launch "low and slow" attacks that can persist for months. Wouldn't it be great if you could identify subtle and related changes in the environment, and then alert security teams when weird stuff starts to occur?



IBM® QRadar® Security Intelligence Platform is the only security solution powered by IBM Sense Analytics™, which can:

- Develop user and asset profiles to baseline legitimate activities
- Detect abnormal behaviors across people (including insiders, partners, customers and guests), networks, applications and data
- Relate current and historical suspicious activities, increasing the accuracy of identified incidents
- Retrieve and replay network activity and investigate packet content in its original form
- Find and prioritize weaknesses before they're exploited

Point products that perform moment-in-time analyses are unreliable; they can't associate new network activity with "risky" users, such as those who are known to have previously visited websites with poor reputations. Sense Analytics helps eliminate threats by matching user behavior with log events, network flows, threat intelligence, vulnerabilities and business context. It enables organizations to focus on their most immediate and dangerous threats by finding clear signals within the noise—and guides them through remediation efforts to minimize any potential damage.

How does Sense Analytics work?

Without data, analytics are useless, and without lots of data, they're simply weak. Some of this data comes from the operation of your network, some of it is stored in applications, some of it is derived from previous analyses, and some of it arrives as a feed from an external source. QRadar collects raw security data from every device, application and user within the network—whether on an organization's premises or hosted within a cloud environment.

Sense Analytics can:

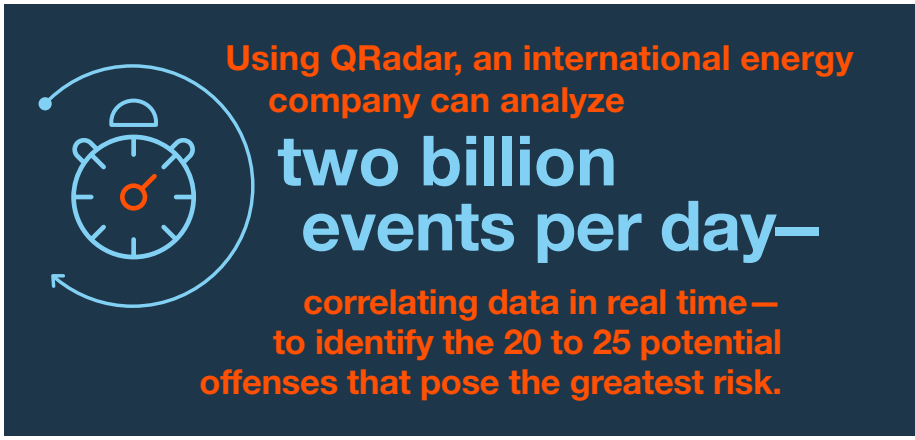
- Analyze security data
- Understand context
- Profile usage

Once the data is collected, QRadar appliances perform real-time analyses to search for immediate signs of danger, and then further infuse the results with other stored intelligence about any of the involved network, user or file metadata. QRadar allows security teams to understand how current activities are related to what's occurred in the past, and one key aspect of sensing change is having the right parameters for baseline activity.

Analyze security data to sense threats

Powered by Sense Analytics, QRadar uses advanced, state-based analysis to transform current security data into meaningful insights. Security teams can define multiple types of conditions to help them sense potentially malicious activity, including:

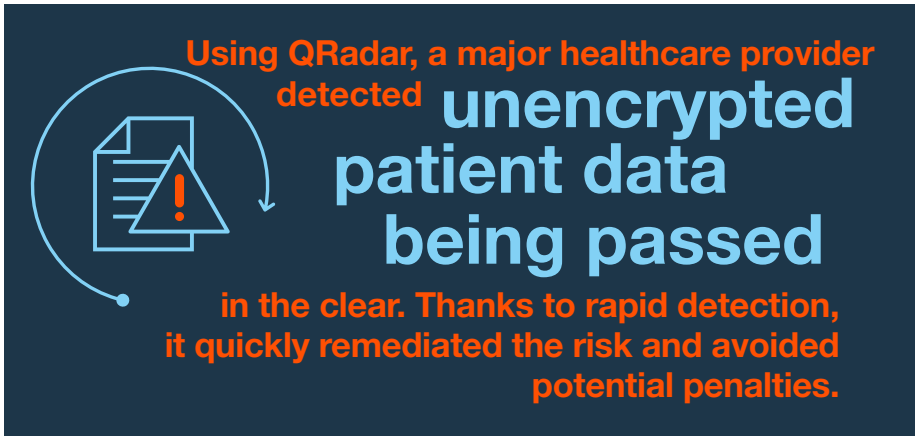
- Behavioral changes to catch deviations from regular patterns
- Anomalies that can uncover new network traffic or traffic that suddenly ceases
- Threshold violations to find occurrences of an activity that exceeds a defined level



A change in the regular behavior of users or identities is often one of the first signs that the network's been breached and, perhaps, someone's credentials have been compromised. Sense Analytics not only compares real-time activity to historical patterns, but it also detects new application usage, new website visits and new file-transfer activities. It can also help rule out false-positive results by pulling data from organizational identity systems, allowing SOC analysts to see a recent reporting or role change for the individual.

Understand context by analyzing events to flows to packets

One powerful and often overlooked source of context can be derived from native network flow data—the data that identifies IP addresses, ports, protocols, and even application or "payload" content crisscrossing the network—all captured through immediate deep-packet inspections or the post-incident recovery of full packets. This enables security teams to:



- Profile "normal" network traffic and get alerts when conditions change
- Find new or compromised hosts communicating with malicious IPs
- Detect new security threats without the use of signatures
- Replay the step-by-step actions of a detected intruder or malicious user
- Get visibility into the application layer and detect suspicious content or inappropriate use

Sense Analytics uses network data to provide context for every event, incident or correlated offense. It can detect if a web server stops responding to communications, identify a significant change in the activity level of commonly used services, and generate alerts when new services or protocols appear on the network. This analysis also reveals application types and identifies port and protocol mismatches—which can help expedite investigations.

Profile usage to store insights and help manage risk

A security solution designed to quickly search through real-time data is going to miss a lot of incidents that require prior knowledge of key applications, the people who use them, their typical performance levels, their associated hosts, and when they experience fast and slow periods of activity. Knowledge of these parameters is crucial for actionable intelligence.

QRadar can help a credit card firm **protect its critical data** and infrastructure from advanced threats—while also achieving deployment, tuning and maintenance cost savings up to 50 percent.

The ability to store knowledge by profiling assets and individuals is a foundational characteristic of Sense Analytics. QRadar automatically discovers assets and creates asset profiles, using network flow data and vulnerability scans. Profiles define what an asset is, identify how it communicates with other assets, list the permissible applications and outline the presence of any known vulnerabilities. QRadar then uses all of this context to reduce noise and provide highly accurate incidents.

Building knowledge about what network users are doing is equally valuable for attack and breach detection. QRadar can track IP and MAC addresses, email IDs and chat handles, for example, and it can leverage other IBM or third-party identity and access management programs to provide valuable context to incident investigations. It can use all of these associations to qualify the scope of its analytics, and include or exclude individuals or personas associated with suspect activity—happening currently or observed in the recent past.

Explore use cases that show the power of Sense Analytics

In many environments, complacency and lapses in security practices mean that critical assets aren't necessarily as secure as they can—or should—be. Organizations need to limit the downside of an inevitable breach. They need solutions that cover the complete environment without any blind spots.

From the moment it's installed, QRadar begins building actionable security intelligence that can help strengthen an organization's defenses. The use cases in which the solution delivers rapid value include:

- Advanced threat detection
- Critical data protection
- Insider threat monitoring
- Risk and vulnerability management
- Unauthorized traffic detection
- Forensics investigation

Use cases:

Advanced threat detection

Using real-time analytics, security teams can detect if a host visits a potentially malicious domain, but an alert might not be required for just a visit. However, if that same host starts demonstrating beaconing behavior—detected by using historical long-term analysis—and it also starts transferring abnormally high data volumes deviating from behavioral baselines, the combination of all three conditions enables QRadar to produce a single, heightened alert.

QRadar can also sense a sudden change in network traffic, such as the appearance of a new application on a host or the termination of a typical service, capturing it as an anomalistic condition. Anomalies are not easily spotted by security teams as they search through system logs—unlike malware signatures or other defined attacks against known vulnerabilities. By definition, an anomaly is an oddity, and is only discoverable by a security solution that monitors and profiles the actions of all users and entities.

Use cases:
Critical data protection

Overnight, a new application begins operating on a network host. This activity might be the result of a new business requirement or someone simply installing a chat application. But if that host has access to critical data, and also has a known vulnerability associated with it, QRadar can create a high-priority alert to prompt security teams to investigate the incident.

QRadar quickly detects when event traffic exceeds a specific activity level and generates an alert. The threshold or limit can be based on any data that is collected in QRadar, such as network device configurations, servers, network traffic telemetry, applications, and end users and their activities. And like a behavioral change or anomaly, QRadar can enrich the alert with the context of user identities, ports and protocols in use, IP reputations and reported threat activities to provide security teams with a deeper perspective about the incident.

Use cases:

Insider threat monitoring

A customer service representative suddenly begins downloading twice the normal amount of data from a client information system, which might be part of some new sales analysis activity. But if QRadar knows that representative recently visited a potentially suspicious website, and is now seeing small amounts of data being sent to a competitor's site, the security staff can be informed before a large amount of information is leaked.

By profiling entities and individuals, QRadar stands out from other security products. The combination of a comprehensive set of data, business context and threat intelligence—coupled with the ability to detect deviations from normal behavior as well as recognize what behavior is not allowed or is inappropriate—provides for an extremely powerful incident detection capability.

Use cases:

Risk and vulnerability management

When a new entity appears on the network, QRadar automatically senses its existence through passive profiling of logs and flow data. With its seamlessly integrated vulnerability scanner, QRadar can trigger a scan of this new entity to discover if it has any urgent or high-risk vulnerabilities that are exposed to potential threat sources.

For example, when a new server is added to the network, QRadar can detect if it is missing critical patches or has default administrative credentials. QRadar can then notify the appropriate team to remediate and/or schedule a patch, and then escalate the issue if that task hasn't been performed in a timely manner.

What's more, new vulnerability disclosures are automatically correlated with existing data without needing a rescan, which helps improve the speed and accuracy of detection. The resulting operational savings also allows security analysts to spend more time focused on proactive tactics, such as risk analysis and vulnerability patching activities.

Use cases:
Unauthorized traffic detection

With most organizations now supporting bring-your-own-device (BYOD) endpoints, security teams are seeing more network traffic associated with social media applications. Users often access their corporate email systems and stay connected with friends through Facebook, LinkedIn, Twitter and other services—all with the same device. QRadar collects and analyzes this data, and notices when, for example, Internet chat sessions start connecting through port 80, the port normally reserved for HTTP traffic. Further connections with known botnet servers quickly verify the injection of malware and prompt the security team to take action.

QRadar collects and analyzes data from mobile and BYOD devices both from the network layer and from endpoint management systems. It can detect potential threats—such as a jailbroken device, suspicious applications installed on a device, or potentially malicious Internet communications—and then trigger quarantining of the device and/or escalation to the appropriate security team for action.

Use cases:

Forensics investigation and threat hunting

During the investigation of an offense, a security analyst discovers that one or more employees have succumbed to a phishing scam and the attacker has latched on and expanded to an internal server host. The pattern matches one identified by X-Force and is known to inject remote-access Trojan (RAT) software, which is difficult to detect.

With a few mouse clicks, QRadar recovers all network packets associated with the incident and reconstructs the step-by-step movements—showing the security analyst with crystal-clear clarity exactly where and when the RAT software was installed. The forensics workflow enables the analyst to quickly and easily build a rich profile of the malicious software and piece together the infection paths through link analysis to identify “patient zero” and any other infected parties. As a result, the security team can quickly remediate the damage and help minimize recurrences.

IBM delivers actionable intelligence for an active offense and stronger defense

Information security is a boardroom priority, but many organizations still depend upon dozens of point products for moment-in-time insights. Highly trained personnel are using search engines to comb through mountains of data, but more and more often, attackers evade detection by switching IPs, protocols, ports and applications to latch on, expand and gather valuable data after a successful breach.

IBM QRadar is different. It deploys rapidly regardless of a network's scale and begins delivering results in mere hours. Its cognitive-like capabilities and stored intelligence can associate related attacks emanating from the same source or corresponding to the same targeted data. QRadar delivers these actionable insights to meet both current and future needs—from advanced threat detection to insider threat monitoring, fraud detection, risk and vulnerability management, forensics investigations, and compliance reporting.

Key reasons why security leaders choose QRadar include:

- An easy-to-use security dashboard that highlights the most important threats and supports fast, effective investigation and remediation workflow
- Near-limitless scalability, backed by X-Force threat intelligence and the collaborative power of IBM X-Force Exchange
- The IBM Security App Exchange, featuring IBM and partner-developed applications (apps) that extend the capabilities of QRadar without added complexity
- The single, integrated platform with global visibility, providing insights about network, application and user activity

Bring the most important threats to life

Once the threat, attack or breach is detected, then it's time to take action. QRadar empowers security teams with a web-based user interface that has a common look and feel across the entire platform. Switching between monitoring log activity, watching network activity, reviewing highly correlated offenses, running risk and vulnerability analyses, or performing forensics analysis is as easy as clicking on a tab to display an information-rich dashboard screen. Each dashboard has extensive security intelligence information, organized into highly visual displays of recent activity that's easily investigated with just a few mouse clicks.

Spend a few minutes looking at the spikes or drilling down into the details underlying a reported offense. Security teams can quickly understand the nature of the highlighted problem; any vulnerabilities exploited; the injection of any botnet, RAT or other malware programs; and the extent of any lost data. Now it's time to act before any real damage is done.

Gain the power to act—at scale

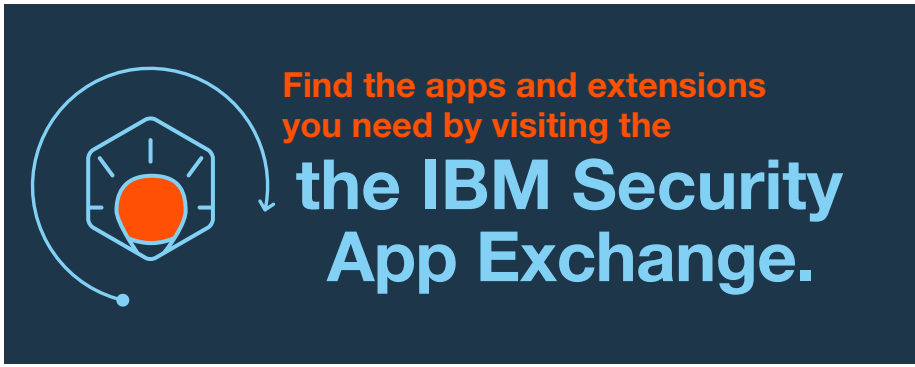
Using the greater QRadar platform, security teams can clearly understand both what has happened and what's at stake if they don't act—quickly. Key capabilities such as threat monitoring, risk and vulnerability management, and compliance reporting are typically a click away, and can pass relevant data to each other. Plus, QRadar includes tight integration with X-Force threat intelligence for hourly updates on global attack techniques and malware strains.

In the event of a breach, QRadar integrated forensics technology provides SOC analysts with packet data for an associated offense, detailing the step-by-step actions of intruders with exact clarity. Defeating some threats simply requires blocking communications with an external IP address, but others require the mobilization of emergency response teams to isolate and reconfigure hosts, disable malware and patch vulnerabilities. But what if your team doesn't know exactly what to do? It's time to ask for help, collaborate with peers, seek a solution or even hire a professional services team.

The QRadar open framework—as well as the IBM Security App Exchange—helps facilitate tighter integrations with IBM and third-party solutions. For example, one of the apps on the site passes QRadar offense data to Resilient Systems' Incident Response Platform for immediate action. Another app provides a similar data sharing capability with the Carbon Black Enterprise Response endpoint management solution.

Expand capabilities with the IBM Security App Exchange

The IBM Security App Exchange expands the flexibility of QRadar exponentially. This premier collaboration site allows customers, developers and business partners to share apps, security app extensions and enhancements to IBM Security products.



With the IBM Security App Exchange, organizations can:

- Obtain apps that extend the capabilities of IBM Security solutions
- Share best practices and learn from others
- Find solutions and use cases that enhance the strategic value of security operations

All code is reviewed by IBM against set criteria before it appears on the site. And security teams can download and install the solutions independently—outside of official product release cycles. This way, they can apply new security use cases without adding unnecessary solution complexity.

In particular, QRadar users can download industry-, threat-, device- and vendor-specific content from the IBM Security App Exchange. Plus, they can access custom reports, dashboards, specialty analytics and threat information.

Deploy one platform with global visibility

Today's security environments are full of complexity—often, security data is distributed across multiple offerings from different vendors, all with different interfaces and data storage formats. To effectively detect existing and emerging threats, security teams need a consolidated view of this data, combined with comprehensive threat detection analytics and response capabilities. QRadar uses a single, federated database for all security data that is specifically designed for scalable collection from on-premises and cloud systems, storage, reporting and very fast investigation search performance. In addition, QRadar is optimized for real-time and historical incident analysis, detecting incidents in a matter of seconds after they occur—not hours, days or weeks.

QRadar also provides a highly integrated set of security use cases, with additional ones available via the IBM Security App Exchange. Security teams can use a single, dashboard-based console for all functions, including real-time security monitoring; proactive risk and vulnerability management; and incident detection, forensics and remediation. This one hub for security operations and response fuses intelligence from IBM and third-party products—backed by a consistent user interface and workflow—making your security operations team far more effective.

For more information

To learn more about IBM QRadar Security Intelligence Platform powered by Sense Analytics, please contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/security

About IBM Security

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned X-Force research and development, provides security intelligence to help organizations holistically protect their people, infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. These solutions enable organizations to effectively manage risk and implement integrated security for mobile, cloud, social media and other enterprise business architectures. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 15 billion security events per day in more than 130 countries, and holds more than 3,000 security patents.

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
April 2016

WGW03211-USEN-00