IBM Security QRadar Network Detection and Response

Detect hidden threats with network visibility and analytics

The increased sophistication of cyber-attackers combined with sprawling IT environments and remote workers can allow threat activity to go undetected. Eliminating blind spots and detection of subtle or unknown threats is driving demand for Network Detection and Response (NDR) solutions, an emerging market which helps security teams quickly detect and response to network threats. NDR solutions analyze network data using non-signature-based techniques like machine learning to baseline what is normal for the network. NDR tools can provide manual or automatic actions that teams can take to remediate security incidents.

QRadar NDR applies machine learning analytics to vast amounts of network data in real time to provide security analysts with actionable insight into hidden threats, enabling them to make better, faster triage and response decisions. QRadar NDR addresses use cases such as lateral movement, date exfiltration, advanced threats, and compromised assets. QRadar NDR brings together open-standard network flow data, full packet analysis, advanced machine learning based network analytics, threat intelligence and AI-powered investigations into a single solution – integrated with QRadar SOAR for incident response – all with comprehensive visibility across on-premises, cloud, and hybrid environments.

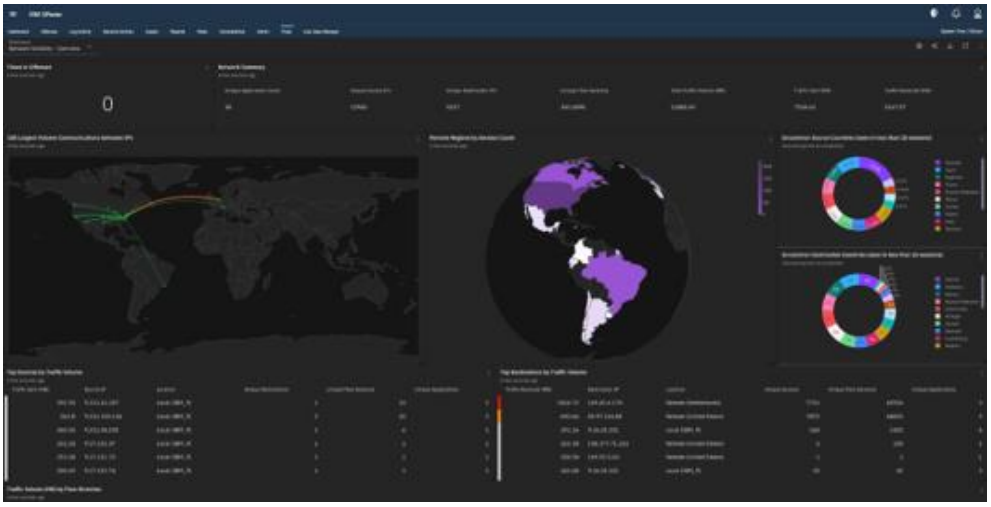
Highlights

- Gain deep and broad visibility across the network to help eliminate blind spots
- Baseline normal network traffic in order to quickly detect suspicious activity
- Investigate network activity to understand the cause of deviations and gain more context
- Respond quickly with automated response actions, playbooks, and case management
- Streamline workflows with a unified solution that scales to meet your needs

QRadar NDR combines several capabilities to provide the visibility, analytics, and response needed to quickly detect and respond to network threats. QRadar Flows provides broad network visibility across a wide range of network devices. QRadar Network Insights (QNI) provides deep visibility into network content that is analyzed in the context of an application, allowing security analysts to gain actionable insights during an investigation. QRadar Network Threat Analytics (NTA), available in the IBM App Exchange, baselines normal network activity and identifies suspicious behavior with machine-learning-based analytics and visualizations.

Gain deep and broad visibility

Network visibility is critical to identifying threats quickly. QRadar NDR provides breadth of network visibility by ingesting network data from a wide range of sources and network devices. QNI enables deep network visibility by analyzing each network session to identify the true application being used and then analyzes the content within the context of that application. QNI records application activities, captures key artifacts, and identifies assets, applications, and users that participate in network communications. 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. Furthermore, QNI helps short-staffed security teams by providing automated suspect content detection to identify potential threat activity.



QNI provides depth and breadth of visibility across your network.

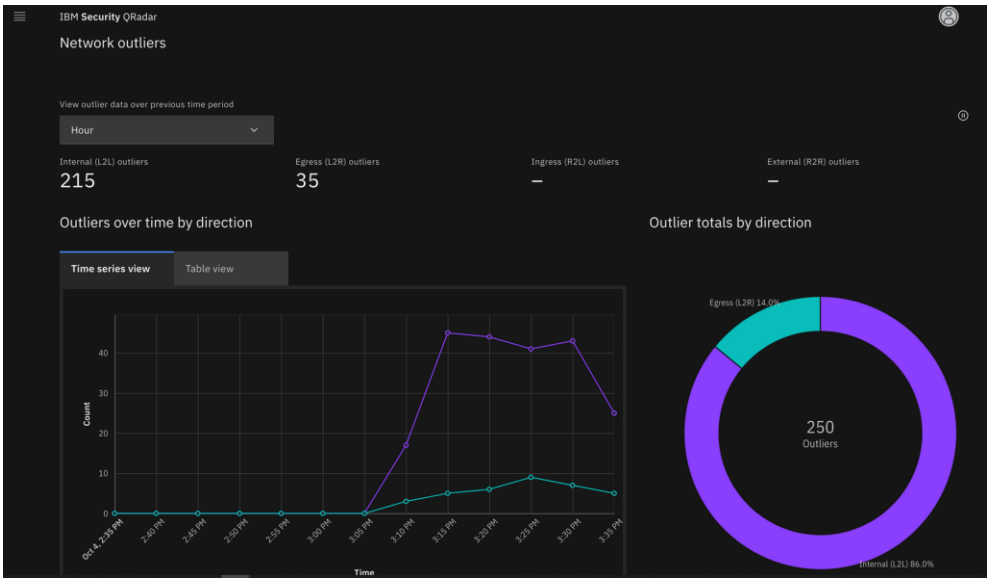
Detect suspicious behavior quickly to stop advanced threats

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. Advanced analytics are critical for detecting new or unknown threat activity across networks.

QRadar NTA provides insights into your network traffic, enabling your security team to investigate unusual behavior on the network. QRadar NTA leverages network traffic information from QRadar SIEM, including deep visibility from QRadar Network Insights, to profile and monitor activity in the environment. NTA leverages innovative machine learning techniques to uncover threats in your environment that otherwise may have gone unnoticed. It learns the typical behavior on your network and then compares your real-time incoming traffic to activity from the past via network baselines.

Unusual network activity, also called an outlier, is identified and given a score representative of how much it deviates from normal traffic.

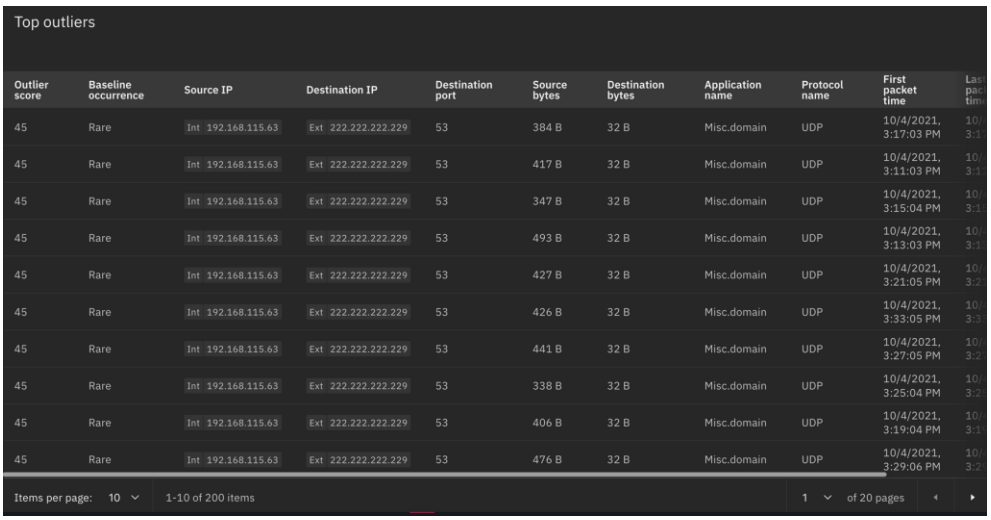
NTA visualizations allow users to quickly understand the volume of outliers by direction and time frame. NTA highlights the network activity with the highest outlier scores, helping security analysts narrow in quickly on potential threats. Security analysts can set the time frame of the flows to be examined, ranging from the last week, day or hour, as well as the direction of the flows. The flow direction may indicate whether there is lateral movement (internal) or data exfiltration (egress).



The Network Threat Analytics dashboard shows network traffic by direction and time frame.

The outlier score will start to increase when, for example, a network session starts sending more traffic than usual or if it's using an application which is unexpected from that traffic or perhaps that type of traffic is rarely seen on the network at all. The higher the outlier score, the more anomalous the flow is. The maximum score is 100.

Once the outliers are identified, security analysts can start the investigation process by analyzing the event details to gain more context and understand what is causing the deviation. By viewing the actual traffic that correlated the network outlier score, security analysts can drill down and triage the elements that reflected the activity that has occurred on the network.



A table of the top outliers and their flow records, which can be sorted by the values shown.

A security analyst can also view the Score Contributors graph that shows what contributed to the outlier score the most. A graph indicates which network properties – such as destination packets, source packets, source IP, destination IP - weighted higher than others.

Prevent future attacks with threat hunting and historical analysis

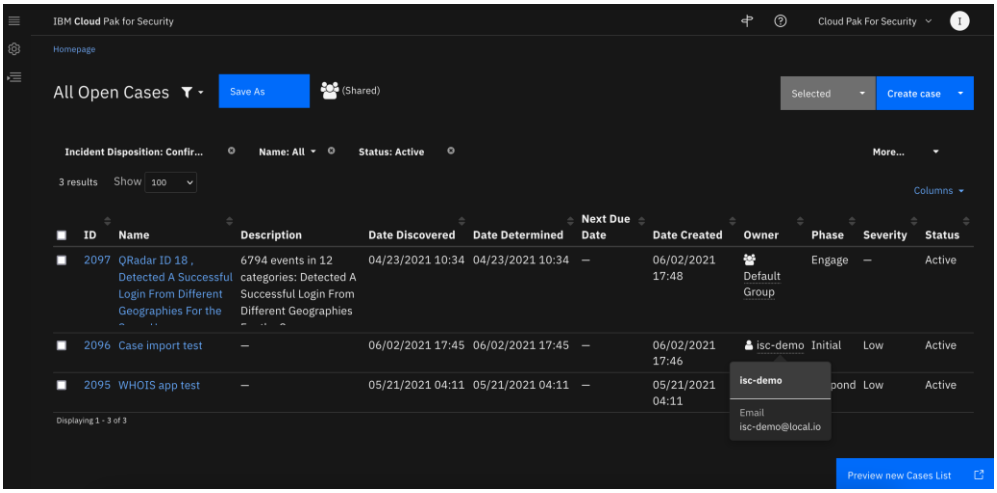
Effective threat hunting starts with having the data needed to identify and investigate unexpected activity. QRadar NTA automatically identifies unexpected network activity, providing a rich data source and guidance for threat hunters starting their analysis. The data and

insights provide input for historical analysis so that security analysts can prevent similar attacks in the future.

Accelerate response times to reduce dwell time

Time is critical once an attack has been identified. QRadar SIEM provides a number of automated and manual response actions to help security analysts respond quickly and reduce attacker dwell time. Automated response actions can include blocking an IP address or sending commands to a firewall so that it drops suspicious traffic, helping security teams stop threats quickly.

Security teams can also leverage automation and orchestration as part of their incident response process. The integration of QRadar SIEM with QRadar 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 SIEM to QRadar SOAR, trigger additional automated enrichments, and drive the full investigation process. As the incident evolves, all information is synchronized between QRadar SIEM and QRadar SOAR, ensuring full data integrity. Any new information uncovered by QRadar SOAR is fed back into QRadar to improve the detection process.



QRadar SOAR provides case management, playbooks, and automated response to help security teams respond to incident quickly.

QRadar Incident Forensics with QRadar Network Packet Capture captures and stores full packet data for use during investigations to determine root cause to identify gaps. This allows security analysts to reconstruct and visualize content after an incident has occurred to see exactly what happened, ensure proper remediation of the threat and help prevent similar events in the future.

Easily scale with changing needs

The flexible, scalable architecture of QRadar SIEM 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.

Conclusion

IBM Security QRadar NDR applies machine learning analytics to a vast amount of network data to provide security analysts with

actionable insight into hidden threats, enabling them to make better, faster triage and response decisions.

QRadar NDR provides broad threat visibility, detection, and response in a unified solution, allowing you to do more with what you have and helping to eliminate the need to pivot between tools. The centralization and visualization of data helps avoid data silos and provides critical context and insights into threats quickly. Furthermore, QRadar NDR helps optimize security investments by easily scaling as your needs change and grow. As an open solution, QRadar NDR allows security teams to leverage their existing investments, avoiding the need to rip and replace current solutions.

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