IBM Security QRadar Network Detection and Response

Detect hidden threats with network visibility and analytics

Highlights

Help eliminate blind spots on your network where threat activity can go undetected

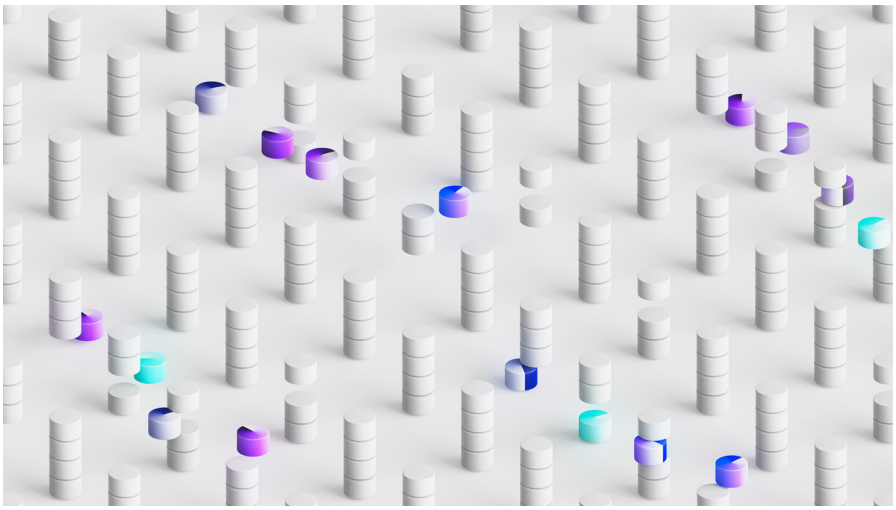
Automatically detect suspicious behaviors and activity using advanced analytics

Respond quickly with automated response actions, playbooks and case management

Streamline workflows with a unified solution that scales to meet your needs

The increased sophistication of cyberattackers combined with changing IT environments and ever increasing network activity can allow threat actors to go undetected. The need to eliminate blind spots and detect unknown threats drive demand for network detection and response (NDR) solutions.

IBM Security® QRadar® Network Detection and Response (NDR) includes multiple integrated technologies so customers can tailor detection and response capabilities for their environment, priorities and budget. QRadar NDR addresses use cases including lateral movement, data exfiltration, advanced threats and compromised asset detection. It also brings together network flow telemetry from your network device, full packet reconstruction and analysis, advanced machine learning based network analytics, threat intelligence, and AI-powered investigations into a single solution. QRadar NDR is integrated with IBM Security QRadar SIEM and IBM Security QRadar Security Orchestration, Automation and Response (SOAR) for comprehensive detection and incident response across on-premises, cloud and hybrid environments.



IBM **Security**

QRadar NDR helps organizations tailor their NDR capabilities to provide the visibility, detection and response they need to quickly detect and respond to network threats:

IBM QRadar Flows
Flow data provides comprehensive network visibility by ingesting Netflow, J-flow, S-flow and IPFIX from devices across your network. Cloud-based flows packaged as logs—such as Amazon Web Services (AWS) VPC Flow logs—are converted to native flow records for analysis, enabling seamless visibility across on-premises and cloud environments.

IBM QRadar Network Insights (QNI)
Reconstruct and analyze network sessions in real time using full packet streams for greater depth of visibility. QNI extracts vital metadata and application content to extend the detection capabilities for QRadar NDR. This telemetry provides deep insights to attackers' precise behaviors.

IBM QRadar Network Threat Analytics (NTA)
Leverage the latest innovations in machine learning to continuously baseline your network environment and analyze network activity as it happens, automatically identifying new or unusual behaviors that may otherwise go unnoticed. QRadar NTA enhances the detection capability of your QRadar environment while enabling "threat hunting" across your networks.

IBM QRadar Network Packet Capture
Provides highly scalable full packet capture capabilities to store and retrieve full packet data for in-depth investigations.

IBM QRadar Incident Forensics
Post-incident network forensics reconstruct and analyze full packet capture data, facilitating both investigation and incident response. QRadar Incident Forensics and QRadar Network Packet Capture complement the real-time network analysis and detection provided by QRadar Network Insights and QRadar Network Threat Analytics. This capability supports detailed forensic investigations and historical analysis of incidents.

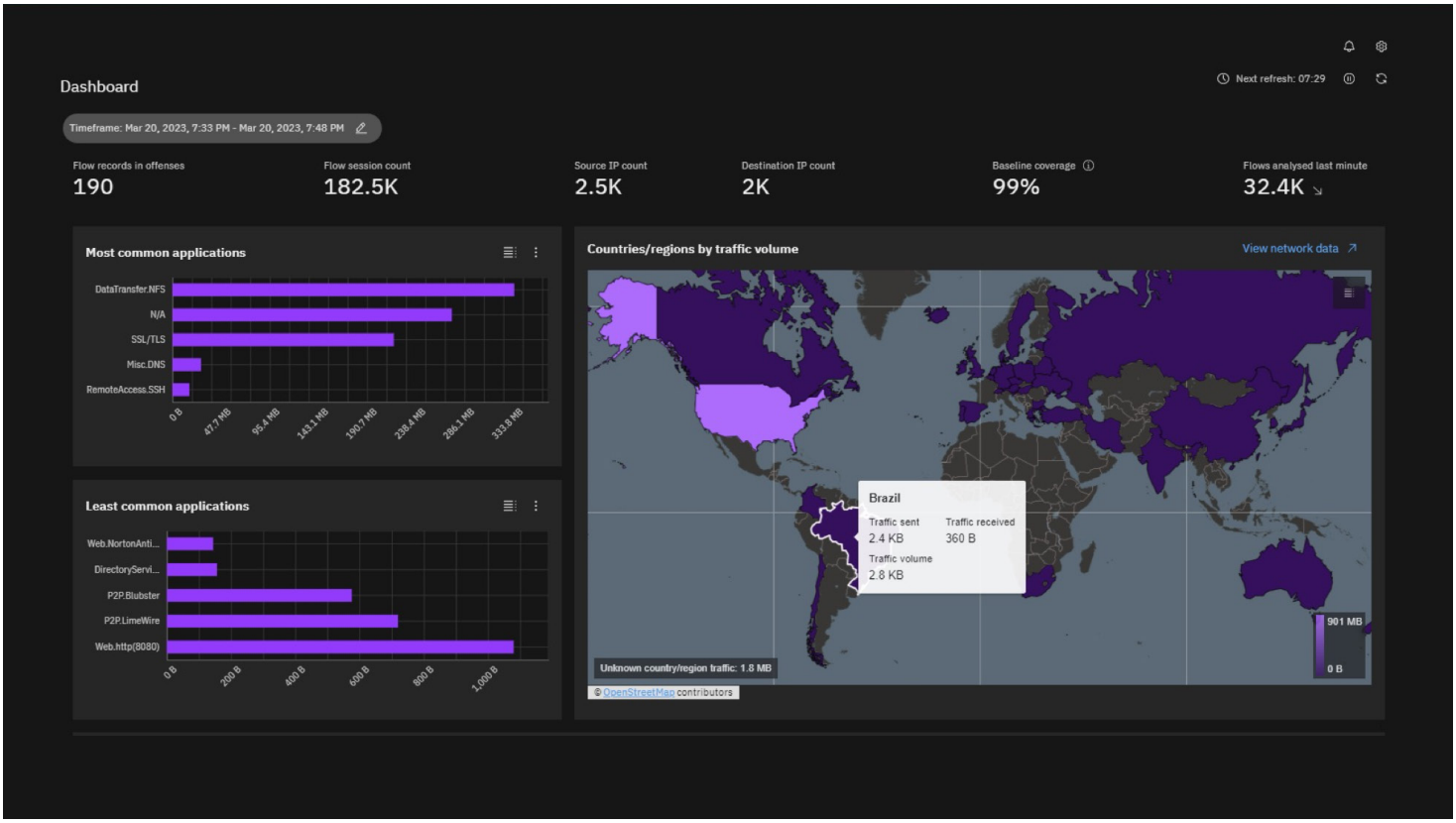


Figure 1. IBM QRadar NDR dashboard.

Gain visibility across your networks

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. QRadar Network Insights enables deeper network visibility by analyzing each network session to identify the true application being used, then analyzes the content within the context of that application. QRadar Network Insights records application activity, 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 associated with compromised hosts, compromised users, data exfiltration attempts and other malicious activity. QRadar Network Insights assists short-staffed security teams by providing automated suspect content detection to identify potential threat activity.

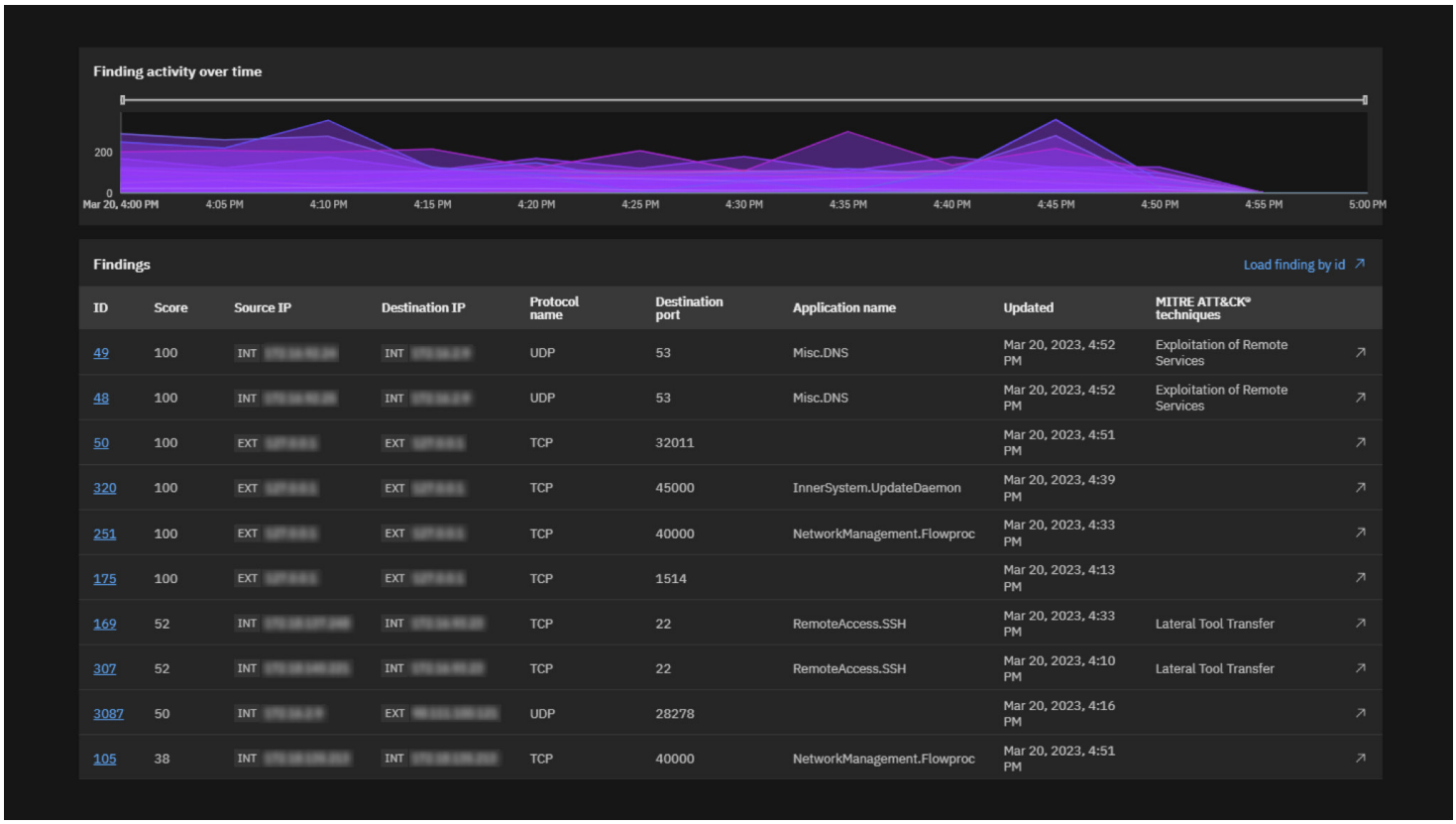


Figure 2. IBM QRadar Network Threat Analytics findings identify and track new or unusual network behavior. Risk scores are continuously updated for prioritized investigation and response.

Detect suspicious behavior quickly to stop advanced threats

As attackers become more sophisticated in their techniques, IOC and signature-based threat detection is no longer adequate on its own. Instead, organizations must also be able to detect subtle changes in network, user or system behavior that may indicate existing unknown threats while minimizing false positives. Advanced analytics are critical for automatically detecting new or unknown threat activity across networks.

QRadar Network Threat Analytics leverages network visibility to power innovative machine learning analytics that help automatically uncover threats in your environment that otherwise may go unnoticed. QRadar Network Threat Analytics learns the typical behavior on your network and then compares your real-time incoming traffic to expected behaviors through network baselines. Unusual network activity is identified and then monitored to provide the latest insights and detections. QRadar Network Threat Analytics also provides visualizations with analytic overlays for your network traffic, enabling your security team to quickly understand, investigate and respond to unusual behavior across the network.

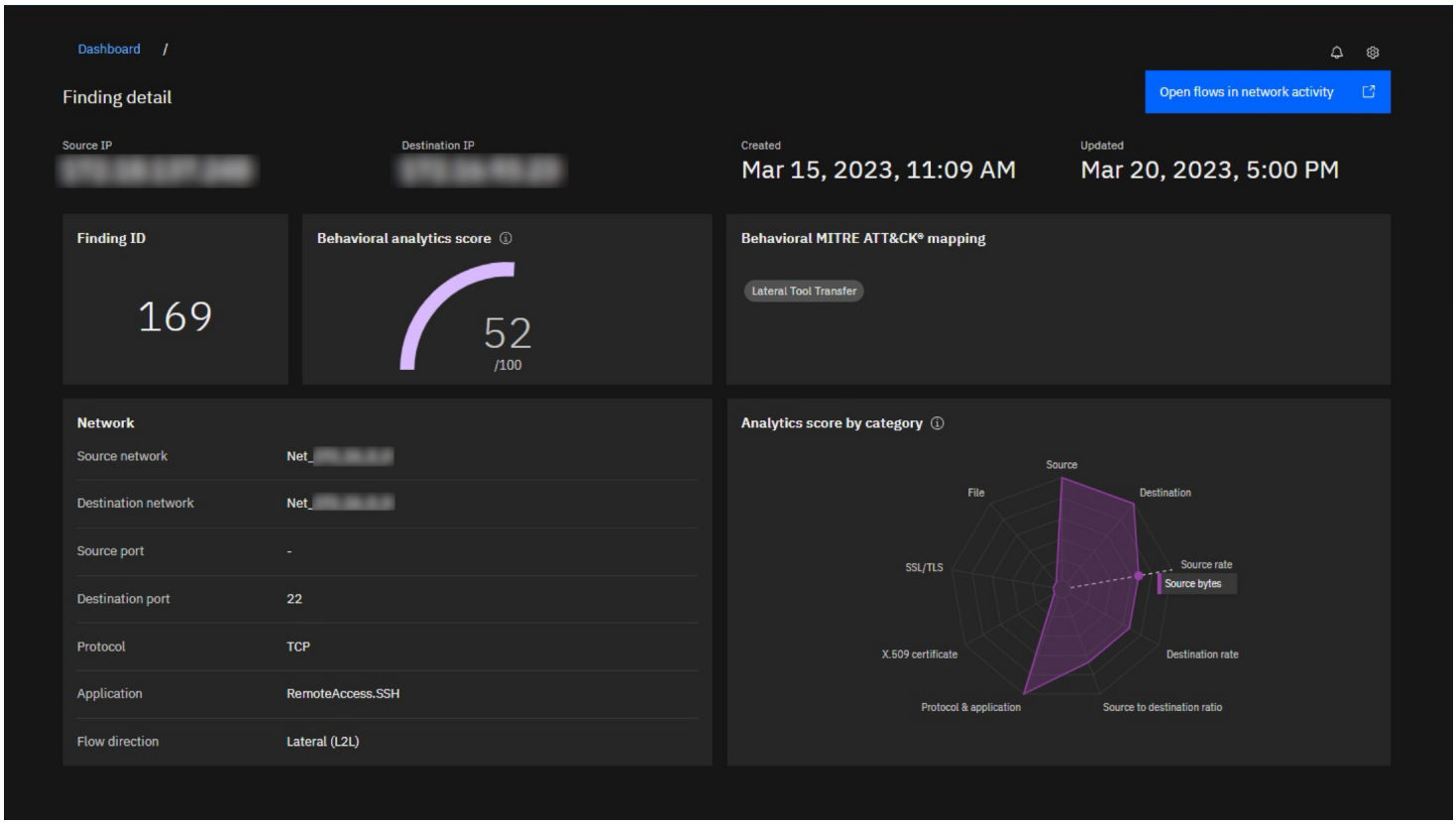


Figure 3. QRadar Network Threat Analytics uses detailed information to analyze suspicious network activity.

The QRadar Network Threat Analytics dashboard provides an overview of what's happening across your network with a prioritized list of analytics findings that are continuously updated. These findings are automatically mapped to relevant MITRE ATT&CK categories—such as Lateral Tool Transfer, Encrypted channels and other categories—when network activity is observed that resembles those behaviors. Each finding contains a detailed breakdown of the analytics results with access to more details into specific network activity. These specifics on what occurred are then compared to what is expected for the given type of network activity.

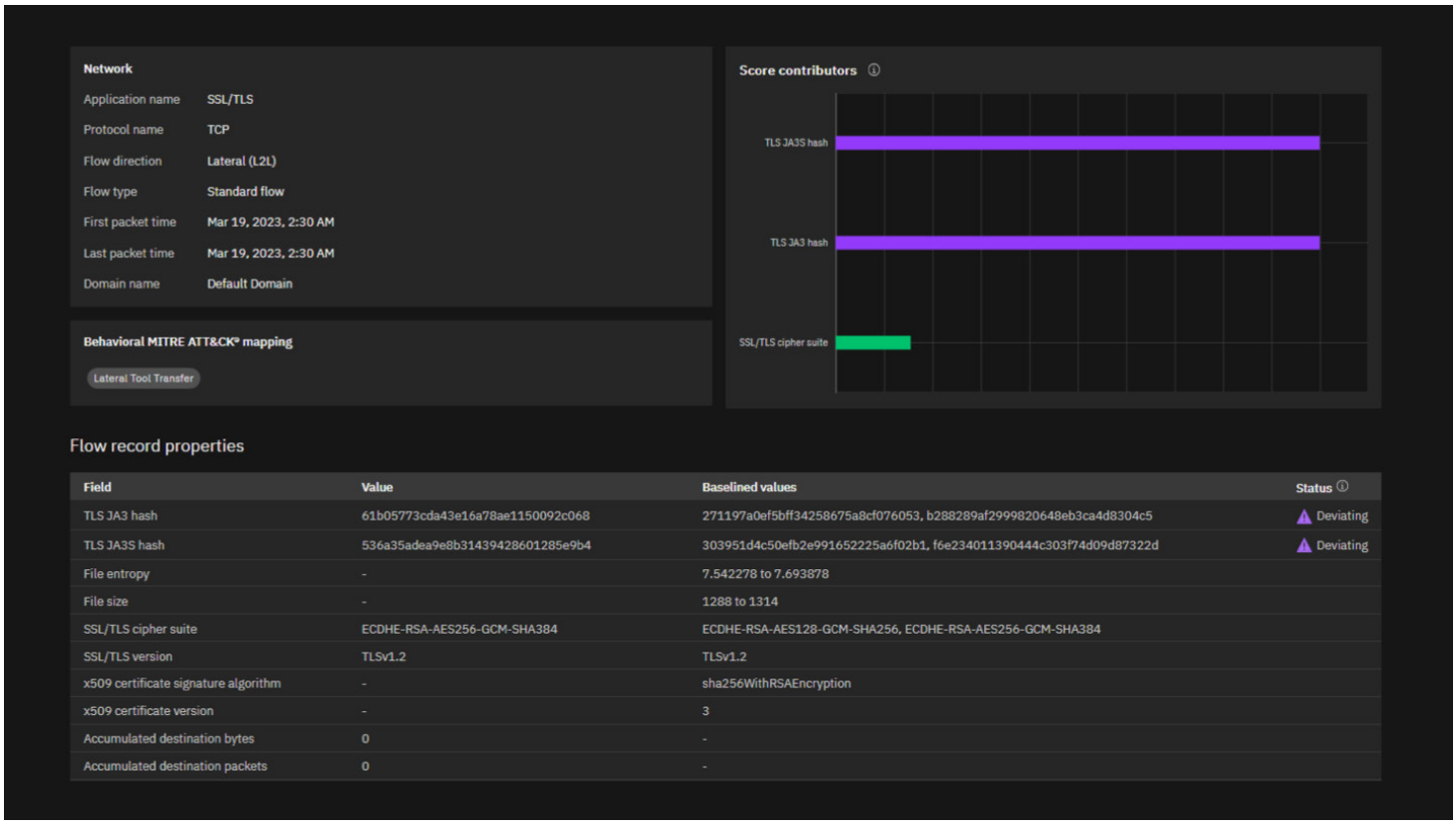


Figure 4. QRadar flows represent network activity by normalizing IP addresses, ports, byte and packet counts, and other data, into flow records, which effectively are records of network activity between two hosts.

Accelerate response times to reduce dwell time

Time is critical when an attack has been identified. Security teams can also leverage automation and orchestration as part of their incident response process. The seamless integration of QRadar SIEM and QRadar NDR 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, information is synchronized between QRadar SIEM and QRadar SOAR, helping safeguard full data integrity. Any new information uncovered by QRadar SOAR is fed back into QRadar NDR to improve the detection process.

As information is being synchronized between QRadar SIEM and QRadar SOAR, IBM Security QRadar Incident Forensics with IBM Security QRadar Network Packet Capture is capturing and storing full packet data. This helps provide context and visibility to the attack information. This capability can be used during investigations to help determine the root cause of the attack and identify gaps in security. This determination allows security analysts to reconstruct and visualize content after an incident has occurred to see exactly what happened, help validate proper remediation of the threat and help prevent similar events in the future.

Easily scale with changing needs
The flexible, scalable QRadar architecture 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 your needs grow. 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 give security analysts actionable insight into hidden threats so they can make better, faster triage and response decisions.

QRadar NDR provides broad threat visibility, detection and response in a unified solution so you can do more with what you have without pivoting between tools. The centralization and visualization of data helps avoid data silos and quickly provides critical context and insights into threats. QRadar NDR works with your existing network infrastructure and easily scales to keep pace with growth in network activity over time, whether on-premises or in the cloud. QRadar NDR optimizes existing security investments without network vendor lock-in so there's no need to disable or 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.

For more information
To learn more about the IBM Security QRadar portfolio, contact your IBM representative or IBM Business Partner, or visit ibm.com/products/qradar-ndr.

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the
United States of America
July 2023