proofpoint | IBM QRadar



SOLUTION BRIEF

Proofpoint + IBM QRadar

Email threat visibility in the SIEM your SOC already runs.

Investigate Email–Borne Threats Where Your SOC Already Works

Human-targeted attacks often begin in email, but the investigation usually continues in the SIEM. Credential phishing and business email compromise are malware-free threats that leave little for endpoint or network tools to catch, so the email-side record is often the evidence analysts need. When that record lives in a separate console, analysts leave QRadar to find out what arrived and who clicked, and correlation is manual.

Proofpoint and IBM QRadar close that gap with two integrations. Proofpoint email threat detections and message logs flow into QRadar, so your SOC can investigate email-borne attacks and trace messages next to every other event source without switching consoles.

Key Benefits

- See email-borne threats beside every other event source
- Quickly identify which users were affected by delivered and clicked threats
- Trace messages with standard QRadar searches, dashboards, and reports
- Keep the SIEM workflows your SOC already runs

Make Email Threats Searchable in Your SIEM

Proofpoint Core Email Protection detects, blocks, and extracts intelligence from external email attacks. Through the SIEM API, it sends threat and click events to QRadar, including blocked and delivered messages as well as blocked and permitted URL clicks. QRadar ingests those events to support investigation, alerting, and reporting.

Email Threat Detection	Search, Alert, Report
Core Email Protection → SIEM API Proofpoint detects and blocks external email attacks, then sends threat and click events, including delivered and clicked threats, to QRadar. This helps analysts see which users were affected by credential phishing, BEC, and other malware-free threats.	**Ingest in IBM QRadar** QRadar ingests the events so SOC teams can investigate, alert, and report on email threats next to the rest of their event data. The Proofpoint app for QRadar also provides dashboards and reports based on the SIEM API data.

©Proofpoint, Inc. 2026

Trace Any Message Without Leaving QRadar

The Proofpoint Email Security app for QRadar gives SOC and email administrators visibility into email activity and message tracing. The Email Protection Log API streams message logs and mail logs as structured JSON, and the app extracts and normalizes them so teams can use standard QRadar searches, dashboards, reports, and alerts.

Log Streaming	Normalized Events
Email Protection Log API For Proofpoint on Demand deployments, the Log API streams message logs and mail logs as structured JSON. Data is delivered over standard TCP 443 with token authentication.	**Proofpoint Email Security App for QRadar** The app extracts and normalizes both log types, so teams build dashboards, reports, and alerts. Analysts use the standard QRadar searches they already know.

See Email Alongside Every Other Event Source

Proofpoint supplies the email evidence, and QRadar supplies the investigation. QRadar is only as complete as its sources, and without Proofpoint data it has no view of what Proofpoint detected or delivered, or the click that followed. Proofpoint has rich email telemetry, and QRadar gives analysts a place to join it with identity, host, and network events. Together, email becomes one more source in the investigation, not a separate one. Analysts can see what arrived, who clicked, and how that connects to the activity they already monitor in QRadar.

Email as one more source	Visibility, not response
Threat, click, and message-level data sits alongside identity, host, and network events in QRadar, so analysts investigate email-borne attacks in the same place as everything else.	Both integrations send Proofpoint data into QRadar for investigation, alerting, and reporting. They don't return verdicts or trigger actions in Proofpoint, so your SOC keeps the workflows it already runs.

Extend the SIEM You Already Run

Both integrations build on the Proofpoint and QRadar deployments your team already operates. The SIEM API feed requires Proofpoint Core Email Protection with SIEM API access. The message-tracing app requires Email Protection on Proofpoint on Demand and a Remote Syslog license. Both integrations cover email data only. Together, Proofpoint and IBM QRadar help you bring email threat detections and message logs into the SIEM your SOC already runs, so email-borne attacks are searchable where your team works.

Learn More

For more information, visit **proofpoint.com/us/partners/ibm-qradar**

proofpoint.

About Proofpoint, Inc. Proofpoint, Inc. is a global leader in human- and agent-centric cybersecurity, securing how people, data and AI agents connect across email, cloud and collaboration tools. Proofpoint is a trusted partner to over 80 of the Fortune 100, over 10,000 large enterprises, and millions of smaller organizations in stopping threats, preventing data loss, and building resilience across people and AI workflows. Proofpoint's collaboration and data security platform helps organizations of all sizes protect and empower their people while embracing AI securely and confidently. Learn more at **www.proofpoint.com**

Connect with Proofpoint: **LinkedIn**

Proofpoint is a registered trademark or tradename of Proofpoint, Inc. in the U.S. and/or other countries. All other trademarks contained herein are the property of their respective owners.