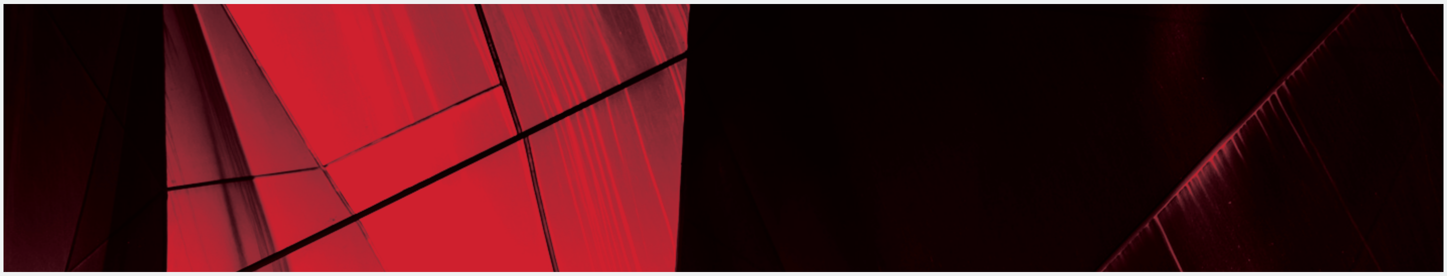


RED CANARY THREAT INVESTIGATION

MDR beyond the endpoint

red canary

MDR beyond the endpoint with Red Canary Threat Investigation

MDR services used to focus exclusively on the endpoint. The world has changed.

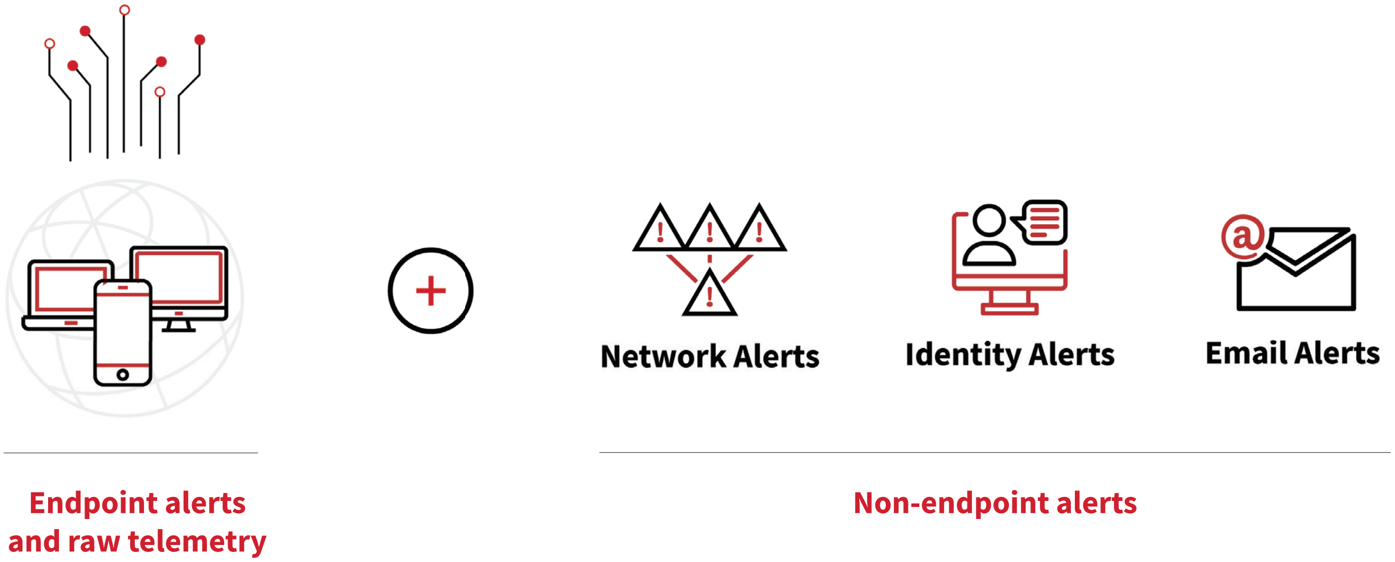
In many attack scenarios today, the initial entry point into an environment is via a non-endpoint vector and throughout the attack chain adversaries move throughout the network. Email, network, and identity security tools may very well pick up signals that detect this suspicious activity, but it is not easy for security teams to identify the threats that really matter across disparate tools and the avalanche of alerts.

For many organizations, their security stack is complex and noisy, and their teams struggle with managing the multitude of security solutions and alert fatigue. Security operations teams seek a solution that provides a single pane of glass, and informed guidance around which threats require immediate response to effectively protect their organization from a breach.

What is Red Canary Threat Investigation?

Red Canary MDR goes beyond the endpoint with Red Canary Threat Investigation. In addition to ingesting raw endpoint data and telemetry, Threat Investigation allows Red Canary to process non-endpoint alerts from network, identity, and email tools. Alerts sent from these data sources are investigated by Red Canary analysts. They will determine which can be ignored and which need to be addressed right away.

Customers can rest easy knowing that they will not be overwhelmed by noisy alerts while ensuring that they are addressing the most critical threats to the business with the context they need, in a single pane of glass, to appropriately remediate.



Network Alerts

Identity Alerts

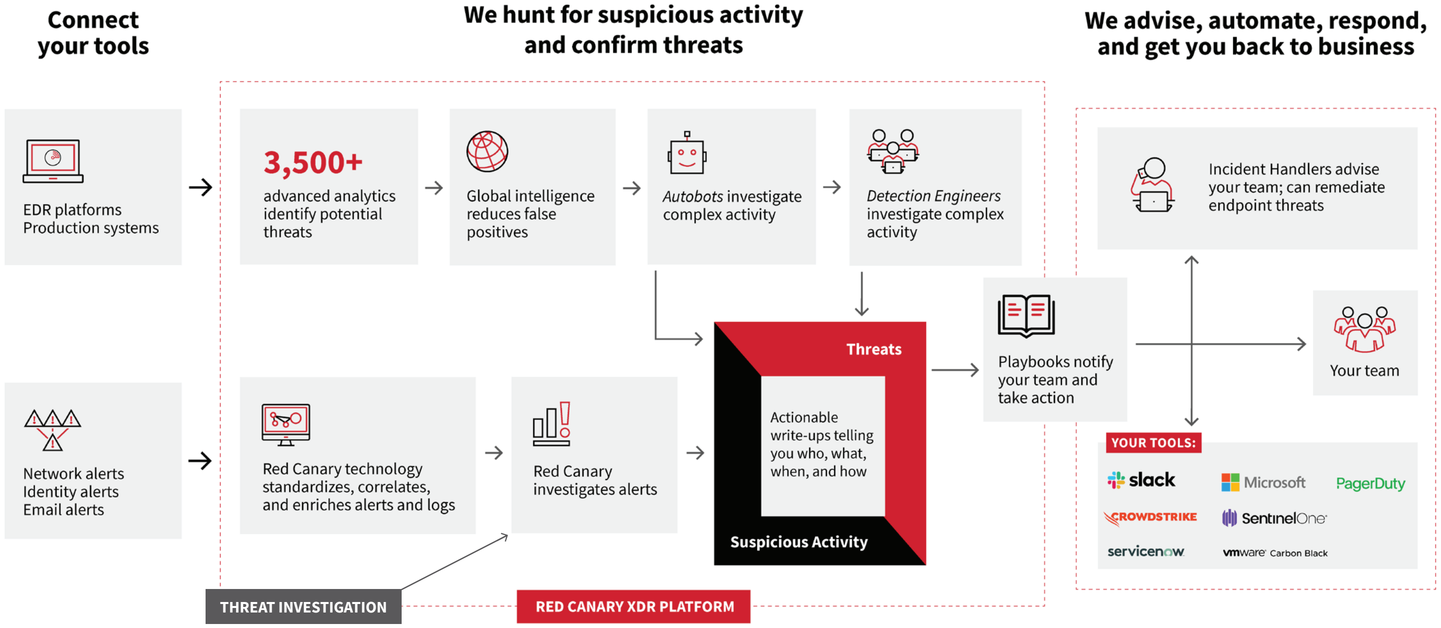
Email Alerts

Endpoint alerts and raw telemetry

Non-endpoint alerts

How Red Canary Threat Investigation for non-endpoint data sources works

1. Connect your network, email, and identity tools.
2. Red Canary ingests alerts from your connected tools into our XDR platform. We then standardize, correlate, and enrich the data.
3. Analysts at Red Canary perform human-led investigations to determine which are likely threats.
4. Red Canary provides actionable write-ups telling you the “who, what, when, and how” of the attack.



Connect your tools

We hunt for suspicious activity and confirm threats

We advise, automate, respond, and get you back to business

EDR platforms
Production systems

3,500+ advanced analytics identify potential threats

Global intelligence reduces false positives

Autobots investigate complex activity

Detection Engineers investigate complex activity

Network alerts
Identity alerts
Email alerts

Red Canary technology standardizes, correlates, and enriches alerts and logs

Red Canary investigates alerts

Threats

Actionable write-ups telling you who, what, when, and how

Suspicious Activity

Playbooks notify your team and take action

Incident Handlers advise your team; can remediate endpoint threats

Your team

YOUR TOOLS:

slack, Microsoft, PagerDuty, CROWDSTRIKE, SentinelOne, servicenow, vmware Carbon Black

THREAT INVESTIGATION

RED CANARY XDR PLATFORM

Benefits

Reduce alert fatigue across your security stack

Save time by focusing on the most important activity

Get more value out of your existing security investments

Increase visibility to better detect suspicious activity

> “ MDR services are evolving to include a larger set of technologies and coverage, beyond endpoint detection and response (EDR) ”
>
> Gartner
>
> Gartner Market Guide for Managed Detection and Response Services 25 October 2021

Integrations (as of February 2022)

Technology	Data Source Type	Threat Investigation	Advanced Threat Detection
Carbon Black Response	EDR	X	X
Carbon Black Cloud	EDR	X	X
Microsoft Defender for Endpoint	EDR	X	X
Crowdstrike	EDR	X	X
SentinelOne	EDR	X	X
Jamf	EDR	X	X
Fortinet FortiGate	Network	X	
Cisco Firepower	Network	X	
Palo Alto Networks Pan-OS	Network	X	
Darktrace Enterprise Immune System	Network	X	
Office 365 Security and Compliance	Email	X	
Proofpoint	Email	X	
Microsoft Azure Identity Protection	Identity	X	
Microsoft Defender for Identity	Identity	X	
Okta Workforce Identity	Identity	X	