Red Canary Managed Detection and Response

Red Canary Managed Detection and Response (MDR) monitors your environment to detect and respond to threats so you can focus on your mission. Thanks to our unique blend of human expertise and security, you can have confidence knowing you’re prepared for modern adversaries as your team works remotely, moves to the cloud, or adopts new cybersecurity and IT technologies.

Led by humans, powered by automation

Our teams of detection engineers, threat researchers, intelligence analysts, and incident handlers are aided by a powerful set of automation tools to decrease mean-time-to-detect (MTTD) and mean-time-to-respond (MTTR). Unlike other solutions that only focus on alerts, Red Canary applies advanced analytics to volumes of raw security telemetry helping detect threats that would otherwise go unnoticed. This approach allows us to detect five times more threats on average than endpoint security tools can find on their own. Our technology is so strong that over 97 percent of the threats detected by Red Canary are machine-driven. However, humans still confirm the threats reported to our customers.

Red Canary eliminates noise with a 99.9 percent reduction in false positives, allowing your team to focus on the tasks that really matter. Additionally, detections are shared across our entire customer base. This means that when we detect a threat to any of our customers, we immediately hunt for it across your environment.

In addition to powering detection with automation, Red Canary customers benefit from automated response. Customers can take advantage of a security automation orchestration and response (SOAR) platform that is included in the service. Pre-built and highly customizable automated playbooks allow you to quickly notify the right people, contain threats, and begin remediation automatically when confirmed threats are found. For customers wishing to gain even more speed, human-led, hands-on-keyboard response is available with Red Canary Active Remediation.

When we find suspicious activity, our team of incident handlers work side by side with your team, providing detailed but digestible explanations of everything we find—using language anyone on your team can understand.
MDR everywhere

We go where the adversary goes—across endpoints, identities, network, email, and beyond. MDR everywhere is achieved with our built-in extended detection and response (XDR) platform that we use to deliver our MDR service.

Red Canary MDR processes data from corporate (endpoint, server, network), SaaS (identity, email), and cloud applications (AWS, Azure). Alerts and Red Canary detections from these data sources are investigated by analysts who determine which can be ignored and which need to be addressed right away. Customers can view investigations in a unified timeline, making it easy to understand the root cause as well as the scope and impact of an attack. For organizations with production Linux workloads, Red Canary Linux EDR can also be deployed. The lightweight Linux EDR agent provides the visibility needed to deliver MDR for your infrastructure.

Built for security outcomes, not feature comparisons

Red Canary works closely with our customers to create features that are designed for the operators who will use our product every day. For example, our “by the numbers” reporting tracks mean time to response (MTTR) and return on investment (ROI) and provides metrics so you and your leadership team know exactly how Red Canary is working on your behalf and how your security program is improving over time.

Being built for security outcomes not only applies to our product but the way we treat our customers. We work relentlessly as a security ally for the organizations that entrust us with their protection. You can contact us at any time without any caps or restrictions, including access to Red Canary subject matter experts. Incident handling is included as a standard part of the service, as are all professional services.

“Red Canary operates as a security ally for its clients… [and] truly understands what its MDR clients need and want from a provider.”

Forrester

The Forrester Wave™: Managed Detection And Response, Q1 2021

HIGHLIGHTS

- 24/7 monitoring, investigation, and response
- 5x increase in confirmed threats identified
- 99.9% decrease in false positives
- 10x reduction in mean-time-to-response (MTTR)
- Vendor and platform neutral
- MDR delivered across endpoint, network, identity, email, and more
- Unlimited access to subject matter experts
- Professional service included at no additional cost
- Deploys in hours