

# Your guide to operationalizing Microsoft Security

---



# A different path to a security operations center (SOC)

Many organizations want help harnessing the power of the Microsoft Security's product portfolio. Organizations turn to security services for assistance, and these days there are a lot of 'SOC-as-a-service' providers that say they'll manage threat detection and response for you. But there's a problem.

These services leave you with a lot of the work. They largely regurgitate the alerts they see back to your team, leaving your staff to do the hard part: distilling signal from noise. Doing so in-house is time consuming and prone to missed threats, slower response times, and resource expenditure.

There's a better way to handle this. A security service provider should take work off your plate, not add to it.

## Microsoft provides the foundation for an effective SOC when you add Red Canary.

Using the right Microsoft workloads and adding Red Canary will save your team time—and get you more value from your Microsoft investments.

In this e-book, we'll show you how Red Canary MDR + Microsoft Security is different and how it works.

## Not just a subscription—an entire SOC team

Red Canary combines Security Engineering-as-a-Service cost efficiency with topflight SOC expertise. There's no need to go looking for full time employees (FTEs) with the right skills—Red Canary provides them. So you can:

- **Gain the talent you need** for a 24/7/365 SOC
- **Save thousands to millions of dollars** depending on your organization's size

# Microsoft gives you a solid SOC foundation

---

Using your Microsoft license investment (E5 or other license) as a foundation, Red Canary can provide you with the security depth and coverage you need. It instantly gives you economies of scale with a seasoned army of analysts who provided managed detection and response (MDR).

## Who is this army?

They're the Red Canary experts who coached Microsoft as they developed the EDR elements of Defender; they can help you move to or get maximum value from your current Microsoft license. Deploying a combination of this human expertise and automated detection, Red Canary detects threats that Microsoft Defender does not on its own. It also reduces false positives by over 99%, freeing your security teams from risk and stress.

**Instantly onboard the experts who coached MSFT in developing the EDR elements of Defender.**



# Measurably improve security outcomes:

---

**96%**  
Reduction

**96% reduction** in false positives from Defender.

**3.8x**  
Increase

**3.8x increase** in confirmed detections beyond what you're already getting from Microsoft Defender for Endpoint.

**10x**  
Reduction

**10x reduction** in the mean time to respond.



# More than Managed Detection and Response: Support across the Microsoft ecosystem

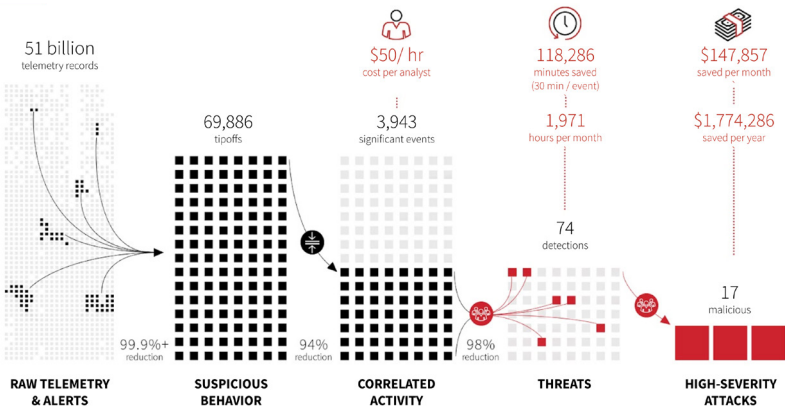
It's all about the ratio.

How many people do you need in-house to detect and foil a growing number of attacks while minimizing the number of false positives? Red Canary helps you reduce that ratio. By outsourcing the expertise and lowering that ratio, you're improving your defenses while freeing up more time for your internal IT and security personnel. This enables them to invest more time on business-specific risks that they are best positioned to handle. You're also achieving a higher return on investment when each attack your team foils costs you less time, fewer resources, and less money. That's a win for IT security and business.

Red Canary both reduces the number of threats your IT and security teams needs to deal with and increases the number of seasoned security experts working on your behalf. Red Canary effectively knocks the amount of threats you deal with to a very manageable number, while saving you money every month.

Additionally, by reducing false positives by over 99%, Red Canary saves your team time while boosting morale.

## Red Canary ROI:



# Supercharge Microsoft Security

---

The Red Canary approach expands on the traditional MDR model. With Red Canary MDR plus Microsoft Security, you get a “better together” solution that supercharges your Microsoft security tools. It’s more than a technology integration. Together, Red Canary and Microsoft give you a powerful combination to protect your organization with:



**Alert investigation** and custom Microsoft-specific detection engineering



**Greater value** from Microsoft Defender and Sentinel



**More threats stopped** across your enterprise and Microsoft ecosystem




**Bi-directional Microsoft Sentinel** and Microsoft Defender for Endpoint support



**Email, identity, and cloud threat visibility** for Microsoft Office 365, Microsoft Azure Active Directory Identity Protection, Microsoft Defender for Identity, Microsoft Defender for Cloud Apps, and more

# How we work with Microsoft

 <b>Managed Detection &amp; Response (MDR)</b>	
<b>24x7</b>	Security Analytics (XDR)
	Threat Investigation & Intel
	Orchestration, Automation & Response (SOAR)
	Active & Managed Remediation



**Microsoft  
Sentinel**



## ENDPOINTS



Defender for  
Endpoint

## IDENTITIES



Defender for  
Identity

Azure AD  
Identity  
Protection

## EMAIL



Defender for  
Office 365

## CLOUD



Defender for  
Cloud Apps

Defender for  
Cloud

## The human element

Microsoft Security provides the premium technology foundation you need. Red Canary adds the human element and more. Here's how:

1. Alerts and telemetry flow from Microsoft Security into the Red Canary engine.
2. Red Canary assesses and validates any threats
3. If a threat requires further attention from your team, we pass it along to you so that it's easily visible on your console. And if it's a critical threat we get in touch with you right away.

So you're getting more than ingestion of alerts; you have a constant feedback loop of alerts, notifications, and responses. And it's all visible through a single pane of glass on your console, with access to links, notations, and any other information that's essential.

This system of integration with Red Canary within Defender can be set up and running in just minutes. There's no long implementation "process." The console itself is updated right away. And so there's no charge for implementation.

## A true security ally

Red Canary is more than a technology; we constitute a substantial human addition to your capabilities. We lock arms with you as an extension of your security team to form your security front line. And every quarter, we deliver a business review that includes an executive security review.





# Behavior-based analytics spot threat patterns

---

Red Canary is different. We used behavior-based analytics to reveal how specific actions in your environment indicate the tactics and techniques used by adversaries.

We start with deep integration with Microsoft Defender for Endpoint and a standard data exchange initially created in a partnership between our engineering teams.

## **But that was just the start.**

We now investigate alerts from Defender for Identity, Office 365 Security & Compliance, and Azure AD Identity Protection. And we apply our behavior-based analytics to Office 365 audit logs to detect email account compromise. Analyzing all this data allows us to determine which patterns of behavior are of interest and look deeper.

The result is Red Canary analyzing your endpoints, identities, email, and more, with the analytical depth to catch threats your tools and team would otherwise miss. Our analytics also help us determine the urgency and speed of response needed so that the highest severity threats are always prioritized.

# Human-led investigation and response

---

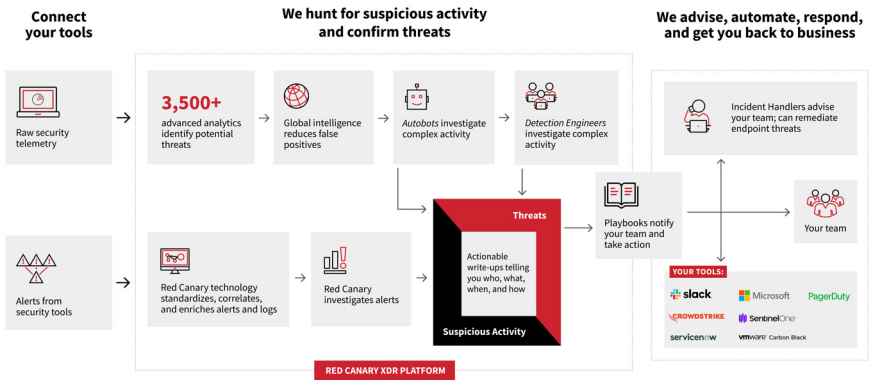
Our detection engine is at the core of our approach, yet our human experts lead the way. On the detection and investigation side, our detection engineers both create behavior-based detections and investigate threats that our engine flags. We want them involved in both detection and investigation: the result is higher-fidelity detections and more efficient investigations for our customers.

## **The best outcomes are human-led but powered by automation.**

On the response and remediation side, our incident handling experts provide real-time guidance during incidents, standing with you until you're back to business. They can remediate endpoint threats on your behalf, and they provide ongoing security program recommendations and coaching—for example, recommending automated responses to activate in Red Canary so that you neutralize threats as fast as possible.

## **Our team is your team.**

# Your Red Canary SOC in action



## Dramatically reduce IT security stress, noise, and wasted effort

- **96% fewer** non-critical alerts and noise
- **Less than 0.01%** false positives
- **Greater transparency** with relevant context presented clearly and in plain english

# Microsoft Security Trailblazer

---



At Red Canary we strive to be trailblazers, which is why we were so proud to receive Microsoft’s Security Trailblazer award.

The award—voted on by Microsoft’s security leaders and top partners—recognized Red Canary for being a “outstanding leader in accelerating customers’ efforts to mitigate cybersecurity threats.”

The award reflects the depth of integration we have with Microsoft Security tools, and the quality of outcomes we provide to Microsoft customers.



# You have a powerful security ally.

---

Find out how quickly you can start to reduce noise, improve visibility, and get more value out of your Microsoft licensing and current security tools.

**Contact us now** to see firsthand how our 24/7, end-to-end approach helps you achieve greater security outcomes—and gets you back to what matters most.

[FIND OUT MORE](#)

