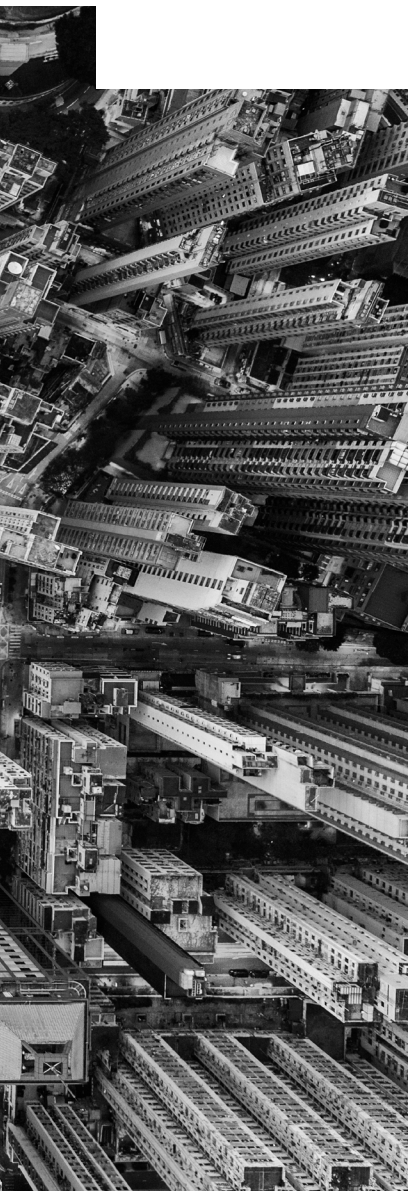
# Maximizing your Microsoft Defender value with Red Canary Managed Detection and Response (MDR)

www.redcanary.com



# Table of contents

**MAXIMIZING YOUR MICROSOFT DEFENDER VALUE WITH RED CANARY MDR**

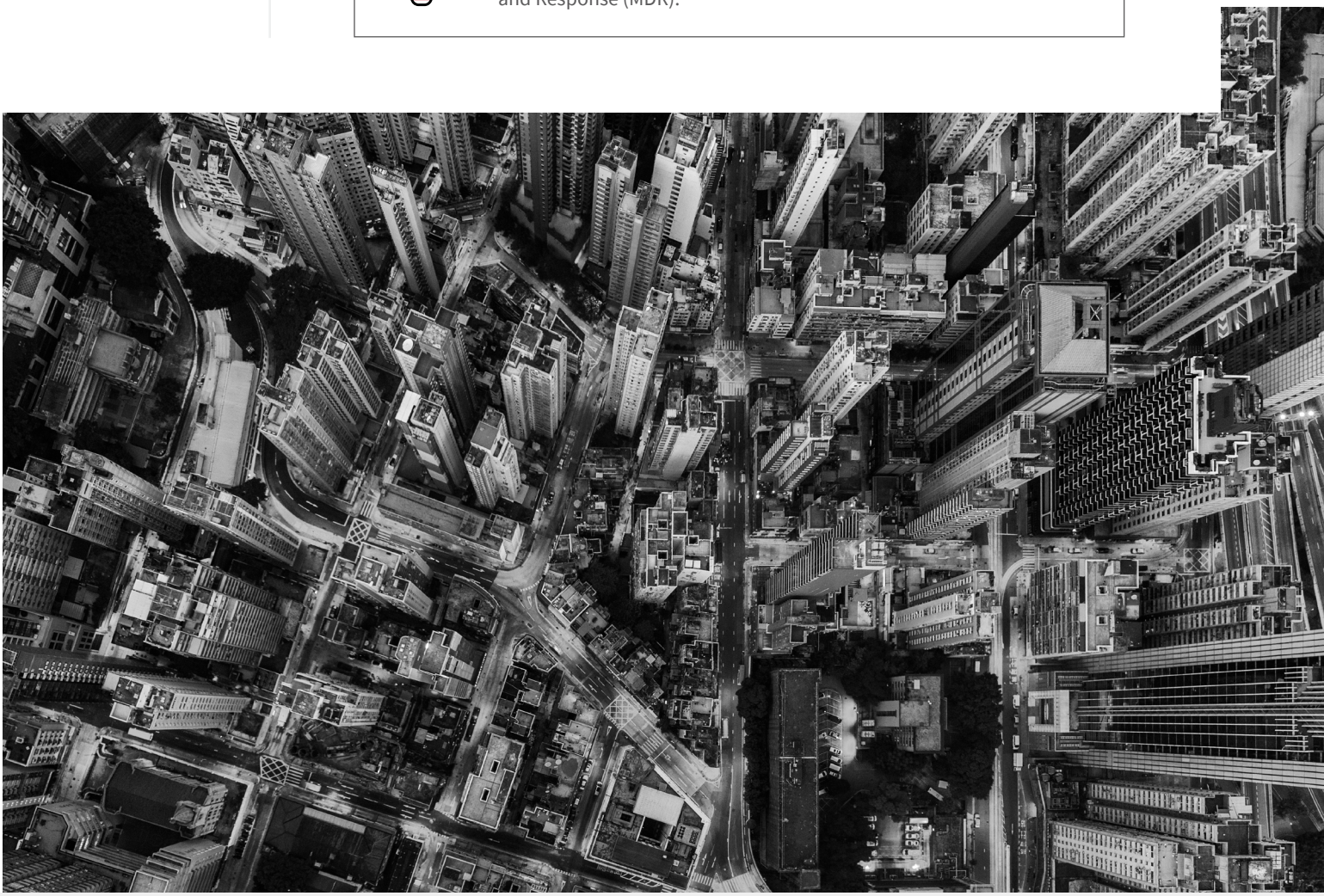


red canary

# Introduction

It's never been more important for security leaders to be well-armed in the battle to protect valuable information. As business systems evolve to employ emerging technical capabilities (both on-prem and in the cloud), security operations teams must grow and adapt to stay ahead of the modern enterprise's inherent complexity and risk. Teams also need to stay ahead of increasingly sophisticated adversaries whose tactics enable them to access networks and stay undetected for extended periods, leading to extensive damage and bountiful payouts. But how can security leaders balance the value of ever-improving tools and technology with the resources that are needed to manage evolving threats and IT risk?

This guide walks you through how you can maximize your Microsoft Defender investment by tapping into Red Canary Managed Detection and Response (MDR).



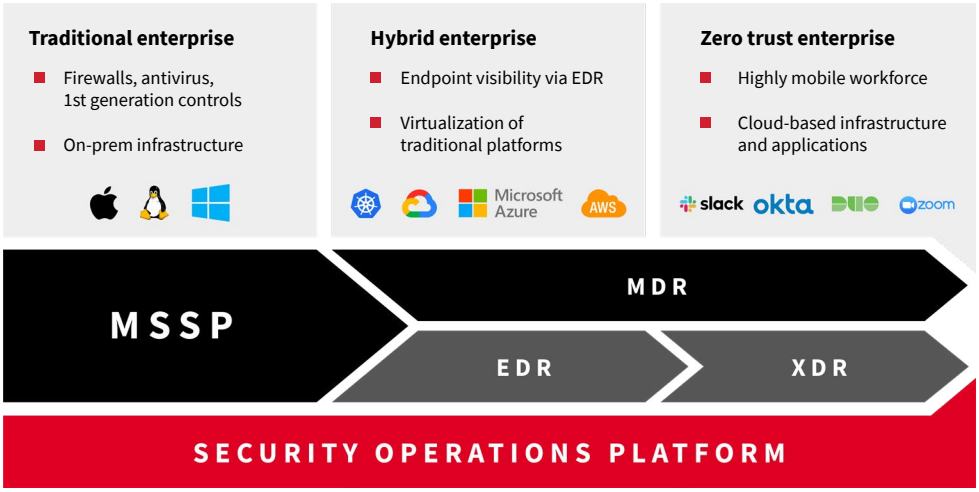
# Adapting to a changing technology and security landscape

End users and the endpoints that they depend on are increasingly under attack, particularly in light of today's mobile and distributed workforce. Endpoint security telemetry is the primary source of threat data in your environment and enables Endpoint Detection and Response (EDR) as a foundational element of threat detection and mitigation. The most common endpoints that EDR solutions protect include laptops, desktops and servers running Windows or macOS.

As organizations move to adopt "zero trust" principles that assume threat conditions are already being exploited, active management through MDR offers important solutions to address those threats.

## Security operations teams need MDR solutions to stay ahead of today's rapid pace of change

For years, Red Canary has been a trusted advisor for security operations teams through their MDR solutions. As companies evolve and expand their infrastructure, the detection and response market itself is evolving. Extended Detection and Response (XDR) is the result of that evolution, expanding threat monitoring, and detection and response across modern security operations.




Many enterprises rely on business applications and cloud-based offerings from Microsoft, such as Microsoft 365, and that relationship often extends beyond IT to include Microsoft Defender.

Microsoft has pioneered the development of endpoints for nearly 50 years, and their combined endpoint expertise and commitment to security is reflected across their XDR offerings. In fact, in 2021 Gartner named Microsoft as a leader in the Endpoint Protection Platform Magic Quadrant, for their Defender for Endpoint solution. They also place a priority on the integration of security and operations. In fact, for customers with large academic (A5) or enterprise (E5) licenses in place, Microsoft Defender is included in the licensing.

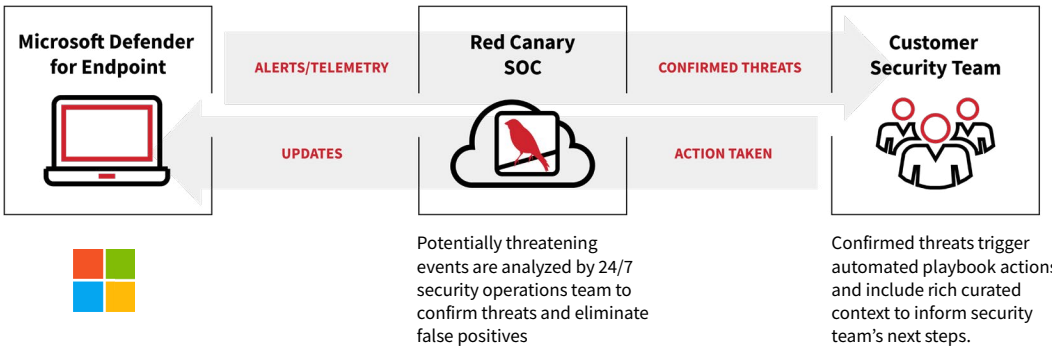
Taking advantage of these licensing opportunities can be fiscally and operationally beneficial to replace existing (and potentially redundant) security products with Microsoft's own comprehensive solutions.

# Red Canary MDR + Microsoft Defender for Endpoint

Red Canary was Microsoft's first MDR partner and is strongly aligned and connected with the Microsoft security product and threat intelligence teams.

Defender provides valuable security information, but even the most accurate and informative telemetry doesn't help unless you can turn that data into action. In today's high-stakes environment, you need an ally that can supercharge that telemetry with a leading edge security operations platform.

## HOW IT WORKS:




Potentially threatening events are analyzed by 24/7 security operations team to confirm threats and eliminate false positives

Confirmed threats trigger automated playbook actions, and include rich curated context to inform security team's next steps.

Red Canary MDR with Microsoft Defender for Endpoint together provide a powerful combination for effective security operations. Red Canary's MDR solutions extend across the entire enterprise estate, from endpoint to on-prem and cloud Linux infrastructure.

"Red Canary serves as an extension of our customers' security teams, providing managed detection and response using Microsoft Defender. I first reached out to explore working together, given Red Canary's reputation and position in the industry. Their strategic thinking is steeped in industry knowledge and they have deep threat detection experience and expertise. They are a true security ally to their customers and the greater security community."

**Rob Lefferts, corporate VP of Microsoft 365 security,**
**"Microsoft Security Roadmap for Defending Against Advanced Threats"**
**keynote at the 2021 Microsoft Ignite conference**

Red Canary's security operations platform—the technology engine of their MDR solutions—extends detection and response beyond the endpoint and aligns with Microsoft's XDR security strategy. For example, the Red Canary platform integrates with Microsoft Defender for Identity to enable all customers to instantly understand if a confirmed threat includes an identity dimension, enabling faster and more complete response.

The integration and implementation of this combined solution are cost-effective and deliver quick time to value. The solution can be implemented within minutes (quite often with only a few clicks), transforming thousands of Defender alerts into meaningful XDR answers.

# Challenges and opportunities for today's security operations

As the enterprise diversifies and modernizes, there is a growing list of assets to secure. Historically, staff and IT might have been neatly housed within a single perimeter, but today's users, systems, and data might be anywhere in the world. These distributed workforces and systems increase the risk of a breach. As a result, many teams are adopting a zero trust approach that assumes cyber adversaries are already somewhere within that infrastructure.

Microsoft Defender for Endpoint brings powerful capabilities, but some key challenges remain:

### LIMITED EXPERTISE

It's difficult to master in-house tools and deep detection expertise required to review and respond to endpoint security threats internally.

### BUDGET LIMITATIONS

It's not cost-effective to hire dedicated security personnel to manage all endpoint security alerts.

### ENDLESS ALERTS

Security solutions like Defender for Endpoint identify thousands of issues and alerts daily—many of which are not immediate or urgent threats to the organization. Trying to keep up with the volume can be exhausting.

### BROKEN PROMISES FROM PRODUCT VENDORS

SIEM tools that aggregate security data yet leave the work of interpreting that data to the security team have paid poor dividends. Teams are left with increased licensing and maintenance costs; agents and sensors that increase network and system complexity; and time spent learning how to operate the tools instead of responding to incidents.

## Addressing challenges through automation and endpoint telemetry

Other products often require installation of software agents to provide endpoint monitoring data. Since those agents consume resources and add risk and complexity, the fact that Defender for Endpoint requires no special agents or sensors is highly valued by IT and security teams alike.

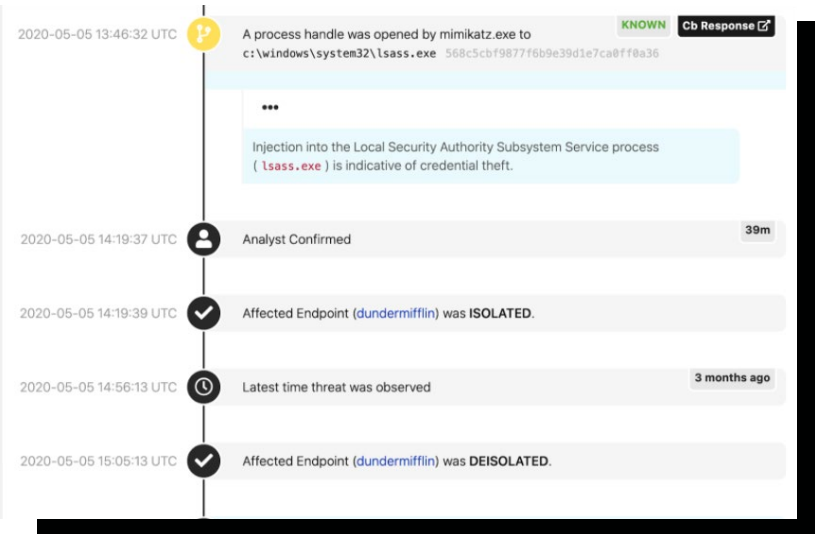
But a high volume of raw information and alerts are insufficient for a complete defense. Security leaders must still ask some tough questions and need to be prepared to provide answers to their own stakeholders. Some of these questions might include:

- How can I best apply strategy and playbooks to turn a flood of information into proactive defense?
- Is my security team investing more capital and operating expenses on running security tools than on managing security?
- In my small organization, does our security staff have the time and expertise to manage the thousands of alerts and reports?
- Do my analysts spend their days chasing down unconfirmed events, wasting company resources to determine which alerts represent real threats? Are they able to provide real-time analysis on a 24x7 basis?

## Red Canary's solution was designed to answer these exact questions

Paired with Defender for Endpoint, Red Canary MDR provides full analysis while virtually eliminating anything that's irrelevant to detection and response. Since every confirmed detection from Red Canary includes full context and is always validated by a second detection engineer, the organization's security team deals with fewer false positives so they can focus valuable resources on enterprise needs.

**RED CANARY DETECTION TIMELINE**



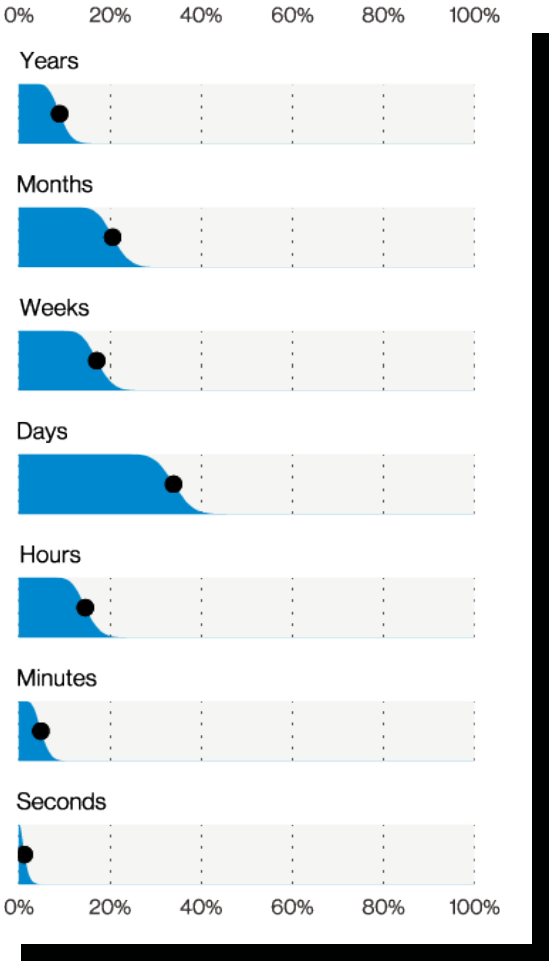
# Staying ahead of attack evolution

While more than one-third of threats are discovered in 30 days or less, and nearly 15% are discovered within hours, no security leader will be satisfied with the notion of an attacker roaming around their infrastructure for any period of time.

While enterprises are transforming, the adversaries are evolving, too. Each day, attackers find new ways to adapt behavior to evade detection, enabling them to stay within the infrastructure for a longer time. The **Verizon 2021 Data Breach Investigations Report (DBIR)** points out that at least half of the incidents observed were able to avoid detection for weeks, months, or even years.

The Data Breach Investigation Report also shared that many organizations learned of a compromise from an external source. That means the tools, sensors, agents, and analysts they had invested in still missed a large number of intrusions. And, in these days of increased ransomware activity, their first notice of a compromise might be a demand for payment from a cyber-criminal.

**BREACH DISCOVERY TIMELINE**

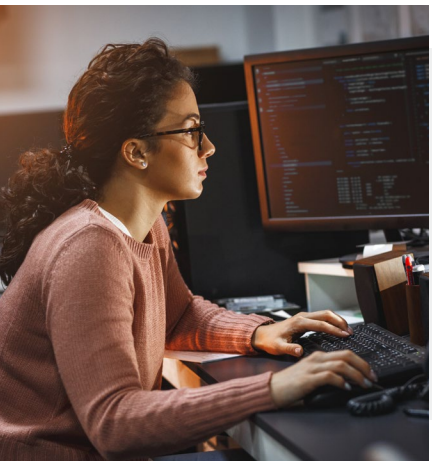



Source: Image from Verizon Data Breach Incident Report 2021

# Improving response to advanced threats with Red Canary MDR

Red Canary's customers report a tenfold reduction in mean time to respond (MTTR), a key risk indicator for many security leaders and a much different story than the one told above.

Faster detection matters because it reduces the impact on your organization and customers. Red Canary customers boast a 75% reduction in realized risk per endpoint over time, a statistic made possible by a significant investment in adversary behavior research.

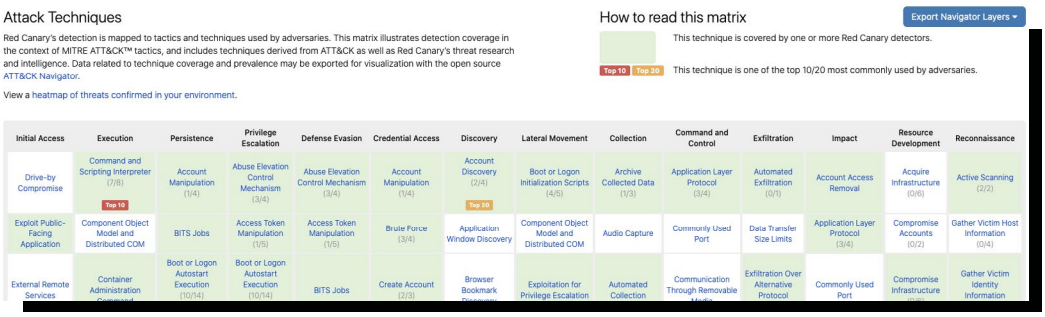


**Red Canary response engineers are engaged in thousands of incident responses each year and use that experience to continuously update behavior-based detection from endpoint telemetry. Their analytic rules significantly extend Defender's threat detection coverage, doubling the number of confirmed threats detected. Red Canary's platform continuously feeds those lessons learned back to the customer Defender portal to improve ongoing monitoring.**

# The role of MITRE ATT&CK® in detections

Red Canary's Security Operations Platform describes activity by using the MITRE ATT&CK framework of tactics, techniques, and procedures (TTPs) that adversaries use for everything from reconnaissance to persistence to impact. That translates to real-time reporting on 203 of the 244 observable ATT&CK techniques. In fact, to help the security community to better characterize detection and response, Red Canary invested the effort to painstakingly map its extensive library of behavioral analytics to a list of thousands of adversary sub-techniques. That behavior understanding and methodology is an example of how Defender for Endpoint is better when paired with the Red Canary MDR solution.

## MITRE THREAT MAPPING




Together, all of these elements illustrate how the Red Canary + Microsoft approach to threat detection and response translates to a maximum return on investment and improved security outcomes.

# Red Canary + Microsoft: Delivering the best managed XDR solution

Some MDR solutions simply take in the raw Defender alerts from security products, perform some basic investigation, and send them back to you.

Today's security leaders have many choices for threat detection and response services, including Managed Security Service Providers (MSSPs) who seemingly offer a one-stop-shop for many of an organization's security needs. MSSPs can share alerts but may oversell their detection and response capabilities.

Red Canary's security engineers are backed by leading-edge security research, behavior analysis techniques, and advanced analytic capabilities that far exceed those of MSSPs (and other MDRs). Poor detection and response from selecting the wrong partner could have severe impact, in the balance sheet, in reputational damage, and in customer trust.

## Your security ally:

- Red Canary + Defender for Endpoint means that all alert data and raw telemetry is fully analyzed 24x7x365—never suppressed—and only confirmed detections of real threats are issued. The result: better security outcomes including up to 96% reduction in Defender for Endpoint non-critical "noise."
- Proactive response and detection analysts do more than simply respond to investigation and remediation calls. They serve as independent security consultants for general security engineering concerns. And in the event of a critical threat in a customer's environment, the response engineers proactively contact the customer to spur immediate action and guide the response activities every step of the way.
- Outcome-focused analysis helps organization stakeholders understand what happened, how it occurred, and how to improve. Unlike competing solutions, Red Canary enables their customers' enterprise security teams to concentrate on responding to confirmed threats, freeing them up to focus on security issues unique to their organization.

## Better outcomes

Thycotic, a leading privileged access management (PAM) company, measured the following improvement after deploying Red Canary MDR with Microsoft Defender:

**95%**

productivity increase

**90%**

reduced alert fatigue

**55+**

daily alerts to 1x per week

# Complete transparency. Continuous improvement.

Today's security leader depends upon full transparency to ensure the team's effectiveness, to inform management about progress, and to ensure compliance with legal, regulatory, and contractual needs. In addition to the fact that those leaders have on-demand access to real-time threat and timeline information through the Red Canary SOC portal, Red Canary's engineers also provide proactive, regular security program reviews for customers to support continual improvement and to help stay a step ahead of the adversaries.

The value of Red Canary's MDR offerings are affirmed by global analysis reports. For example, the **2021 Forrester Wave™ Report** for Managed Detection and Response scored the strategy and offerings of more than a dozen MDR providers, and declared Red Canary as an industry leader.

**RED CANARY IS AN MDR MARKET LEADER**

**The Forrester Wave™**
Managed Detection And Response
Q1 2021


Source: 2021 Forrester Wave Report for Managed Detection and Response

# Conclusion

Red Canary's security operations platform and extensive threat detection expertise and experience enable customers to shut down and respond to threats quickly. Experienced analysts, a strong intelligence team, and skilled response engineers focus on the "hard stuff"—churning through billions of telemetry records every day to turn data into intelligence, and intelligence into action. They ensure that your security operations personnel only need to focus on confirmed security events and the threats that matter to them.

Security operations is hard, especially during today's state of rapid change. This guide outlines why organizations of all sizes and security maturities have turned to Red Canary to be their security ally. Red Canary's technology and expertise informed Microsoft's move into EDR and were key reasons why Red Canary was their inaugural MDR partner. However, it's a shared security ethos and vision for improving security outcomes for customers that set the stage for this powerful, ever-evolving partnership, and combined security solution.

"I view Red Canary as an extension of my internal team. I communicate with them 24 hours a day, seven days a week. I feel like they care about our security as much as my internal team does. And that's why I call them my 'easy button."

**Terence Jackson, Chief Information Security & Privacy Officer, Thycotic**

## Better security starts with a better conversation

redcanary.com/contact-us