Red Canary

Voice of Customer (VOC) Fieldwork

MSSP / MDR Security Vendors

December 2024

A Crossover Catalyst Report

Table of Contents

Respondent Overview | General Profile

60
RESPONDENTS

Primary Software Vendor

- 30 red canary
  - 2 Enterprise
  - 14 Mid-Market
  - 14 Commercial
- 11 CROWDSTRIKE
- 3 SentinelOne
- 5 Microsoft Defender
- 2 pwc, Deloitte., KPMG, EY, eSENTIRE, Secureworks, RELIAQUEST
- 1 paloalto NETWORKS, deepwatch

All Vendors | General Profile

Internal SOC Status | Do you have a 24/7 internal Security Operations Center (SOC) at your organization?

41%	59%
Yes	No

Red Canary | General Profile

Internal SOC Status | Do you have a 24/7 internal Security Operations Center (SOC) at your organization?

31%	69%
Yes	No

Respondent Overview | General Profile

Security Tech Stack | Which security vendors do you use in each of the following areas?

Application Security

snyk, f5, Checkmarx

Cloud Security

Microsoft Defender, paloalto NETWORKS, zscaler

Data Security

Purview, VARONIS, Symantec

Email Web Security

Microsoft Defender, proofpoint, mimecast

Endpoint Detection

Microsoft Defender, CROWDSTRIKE, SentinelOne

Identity Access Mgmt.

Microsoft Entra ID, okta, CYBERARK

Mobile Security

Microsoft Intune, jamf, vmware

Network Security

paloalto NETWORKS, cisco Meraki, FORTINET

Security Training

KnowBe4, proofpoint, mimecast

Security Info/Event Mgmt.

splunk>, Microsoft Sentinel, red canary

Security Orchestration

splunk>, paloalto NETWORKS, Microsoft Sentinel

Vulnerability Mgmt.

tenable, RAPID7, Qualys.

SECTION 1

Voice of Customer (VOC) Takeaways

Executive Summary | Voice of Customer Takeaways

Procurement Process Feedback	Red Canary has established itself as a leading player in the MDR space due to a combination of technical expertise, commercial flexibility and strong integration capabilities. The company's ability to seamlessly integrate with Microsoft's security ecosystem, while supporting multiple EDR/XDR platforms has proven to be a crucial differentiator, particularly for organizations heavily invested in Microsoft technologies. Customers also pointed to Red Canary's (1) superior threat detection capabilities versus Darktrace & CrowdStrike, (2) automated playbooks and dual-analyst review process [which has significantly reduced false positives while enabling rapid threat response], and (3) competitive pricing model / flexibility in seat count requirements, as reasons why they were chosen over other vendors in the procurement process.
Selection Rationale	Red Canary was praised for its platform-agnostic approach and superior integration capabilities, which resonates well with organizations seeking to avoid vendor lock-in and maintain flexibility in their security stack. The company's ability to provide enterprise-grade security expertise while maintaining high-touch customer service has proven especially attractive to mid-market customers who feel underserved by larger providers like Microsoft. Customer feedback consistently highlights Red Canary's technical excellence, evidenced by low false positive rates and comprehensive detection capabilities, while also emphasizing the value proposition of competitive pricing combined with premium service quality. The platform's ability to support multiple EDR/EPP solutions and diverse technology stacks positions it well for sustainable growth in an increasingly complex security landscape.
Security Posture Improvement	Red Canary drives a significant positive improvement (8.6) on customers' security operations, particularly for organizations lacking internal 24/7 security coverage. The service consistently delivers value through workload reduction, improved response times, and enhanced threat detection accuracy, with multiple customers reporting substantial decreases in false positives compared to previous solutions. The platform's strength lies in combining automated monitoring with expert analysis, though some sophisticated customers note limitations in automated detection capabilities compared to native tools like Microsoft Defender. The service shows particular effectiveness for mid-market organizations transitioning from basic security tools to comprehensive MDR coverage, with customers highlighting improved security posture through better incident response processes and security expertise.
MDR / MSSP Replacement Difficulty	The consensus amongst Respondents was that it would be "very difficult" (8.8) to replicate the efficiency of your MDR / MSSP provider with an in-house team. Red Canary customers had a slightly more positive feedback on their overall value-add than the broader Respondent pool, with the average characterization of displacement difficulty by an in-house team coming in at an 8.4. When asked to characterize the cost savings, the majority (67%) of Red Canary customers suggested that it was significantly less expensive than in-house (>25% savings).
Threat Identification Capabilities	68% of Red Canary customers suggested that they have seen a significant improvement in their organization's ability to accurately detect threats. Customers suggested that Red Canary (1) often detects sophisticated threats missed by native tools (2) significantly reduces false positives and noise (3) provides effective 24/7 coverage with rapid response times (4) offers value-add services beyond basic EDR through behavioral and contextual analysis. Similarly, 64% of Red Canary customers suggested that the accuracy/false positive rate was "much better" than alternative vendors they've used or evaluated in the past.

Executive Summary | Voice of Customer Takeaways

Likelihood of Recommending	The majority of customers voiced positive feedback on Red Canary's core MDR offering citing detection accuracy and low false-positive rates as a basis for recommending the platform to other organizations (9.0). The combination of automated detection and human expertise receives consistent praise, with many customers noting significant improvements over previous security solutions. While there was some negative feedback from smaller organizations on service quality inconsistencies and pricing, mid-market organizations with moderate security maturity tend to have the easiest time extracting value from the platform.
Vendor Benefits	Red Canary delivers substantial value through effective security team augmentation, particularly benefiting organizations with limited internal security resources. Customers consistently highlight the combination of reduced workload and enhanced security capabilities, with many noting the ability to reallocate internal resources to strategic initiatives rather than alert investigation. The service provides multiple layers of value beyond basic MDR functionality, including security education, strategic guidance, and access to security expertise.
Feature Requests	Red Canary customer feedback reveals several key areas for potential product enhancements, including: (1) broader integration support across network security tools, cloud services (particularly AWS and Azure), and identity management systems (2) enhanced log management capabilities (3) an expansion beyond pure MDR into broader security advisory services, including proactive security posture reviews and threat intelligence sharing (4) reporting improvements and dashboard customization capabilities.
Security Stack Consolidation Preference & Vendor Integration Feedback	Our fieldwork suggests that organizations prefer working with several core security vendors (5.2 on a 10-point scale) rather than consolidating with a single vendor or spreading across multiple best-of-breed solutions. There is a clear correlation with team size and resources with larger organizations with dedicated security teams favoring a best-of-breed approach and prioritizing specialized capabilities over operational simplicity, whereas smaller teams strongly prefer vendor consolidation to manage complexity and resource constraints. There is universal recognition that complete reliance on a single vendor creates dangerous security and operational risks. The emerging consensus appears to be a balanced approach using several core vendors (typically 3-5) that excel in their respective domains, providing sufficient security coverage while maintaining manageable operational complexity. This strategy allows organizations to mitigate single-vendor risk while avoiding the operational overhead of managing too many specialized solutions.

Executive Summary | Vendor Comparison

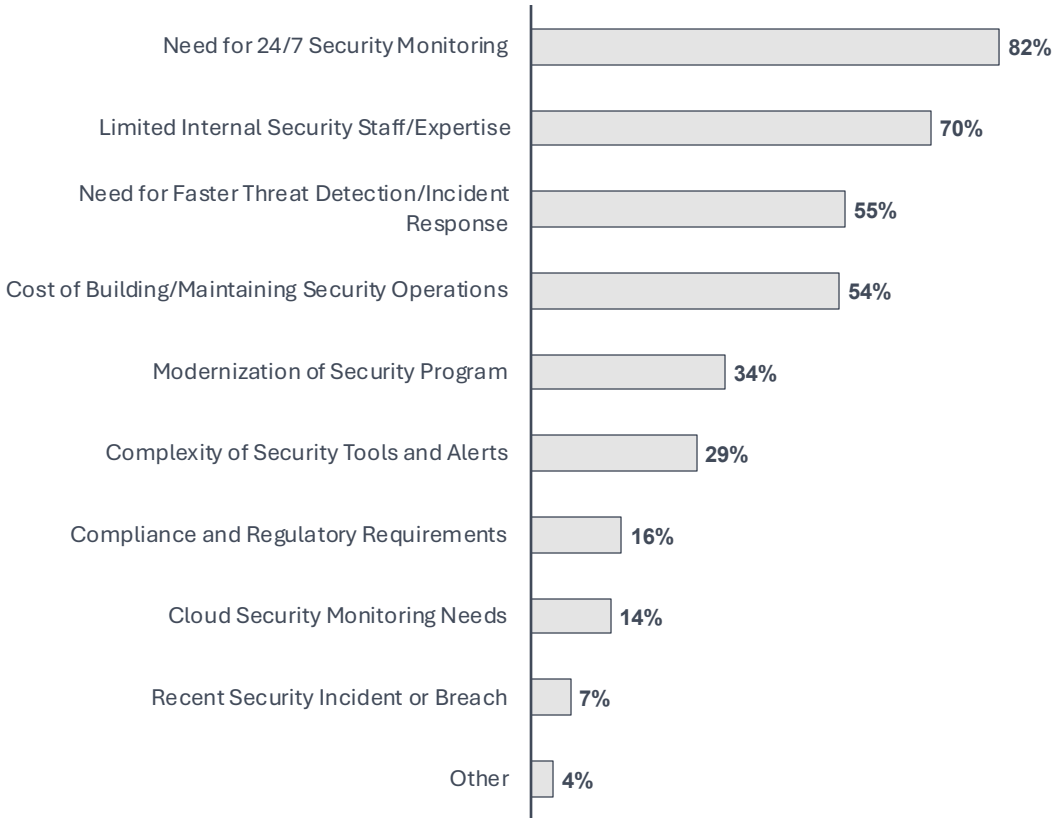
	Improvement to Security Posture	Difficulty of Replicating In-House	Likelihood of Recommending	Integration	Vendor Consolidation Preference
	1=Limited Improvement 10=Significant Improvement	1=Not Difficult 10=Very Difficult	1=Very Unlikely 10=Very Likely	1=Poorly Integrated 10=Well Integrated	1=Single Vendor 10=Best of Breed
All Vendors	8.2	8.4	8.6	7.5	5.2
CROWDSTRIKE	9.0	8.5	8.8	7.3	5.8
SentinelOne	8.3	8.0	8.7	9.3	4.3
red canary	8.6	8.8	9.0	7.2	5.5
Microsoft Defender	7.0	8.2	7.4	7.4	3.6
eSENTIRE	10.0	9.0	10.0	9.5	2.0
RELIAQUEST	8.7	9.7	9.3	7.7	6.3
deepwatch	8.3	8.0	7.0	8.0	7.0
Secureworks	6.5	5.5	5.5	6.5	4.0
paloalto NETWORKS	4.0	6.0	-	8.0	6.0

SECTION 2

Voice of Customer (VOC) Fieldwork

Key Challenges Prompting Adoption	01	Need for 24/7 Security Monitoring	02	Limited Internal Security Staff/Expertise	03	Need Faster Threat Detection/Response

What specific challenges led you to engaging a MDR / MSSP provider?



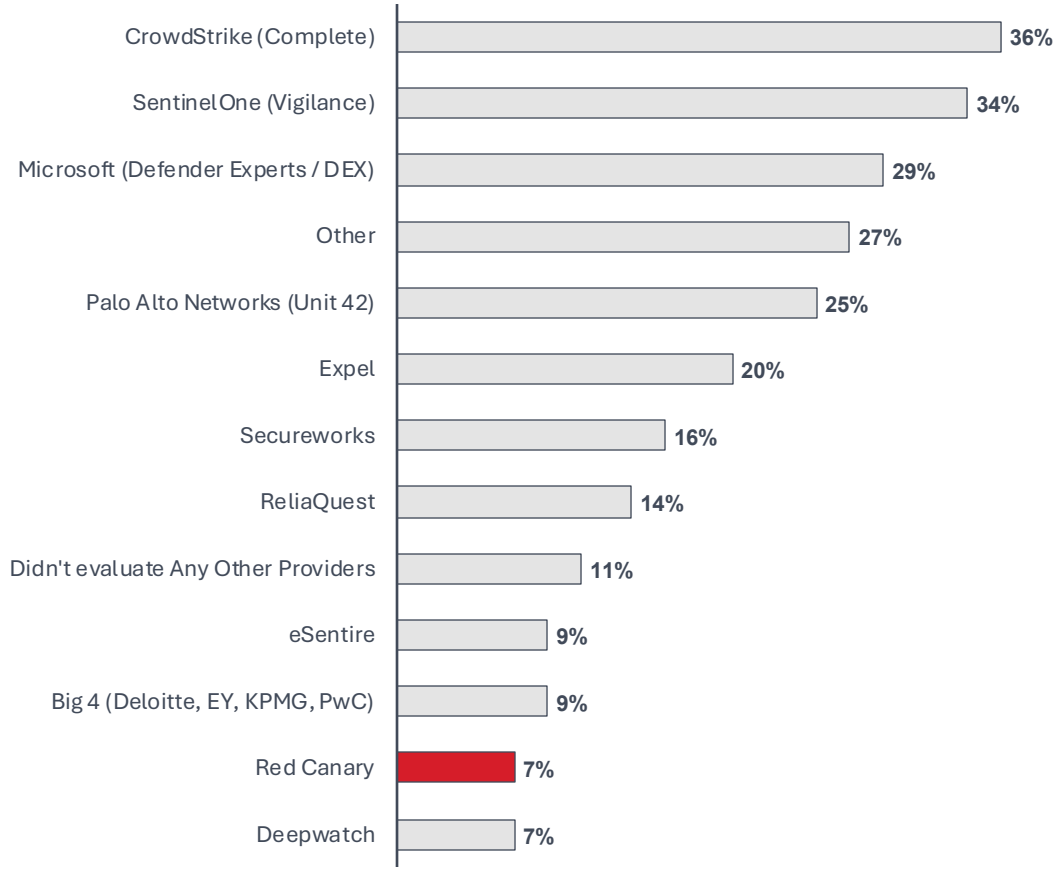
red canary — Customer Responses Only

Onboarding Drivers (Factors)	
Need for 24/7 Security Monitoring	81%
Limited Internal Security Staff	77%
Faster Threat Detection/Response	65%
Cost of Building/Maintaining Security Ops	58%
Complexity of Security Tools and Alerts	35%
Modernization of Security Program	35%
Compliance and Regulatory Requirements	15%
Cloud Security Monitoring Needs	15%
Recent Security Incident or Breach	8%
Other	4%

Most Evaluated Vendor(s)

01 CROWDSTRIKE 02 SentinelOne 03 Microsoft Defender

Did you evaluate any other MDR / MSSP providers?



red canary **Customer Responses Only**

Top Solutions Evaluated	
CrowdStrike	42%
SentinelOne	31%
Expel	31%
Other	31%
Microsoft Defender	23%
ReliaQuest	19%
Secureworks	15%

Insights | Procurement Process

Red Canary has established itself as a leading player in the MDR space due to a combination of technical expertise, commercial flexibility and strong integration capabilities. The company's ability to seamlessly integrate with Microsoft's security ecosystem, while supporting multiple EDR/XDR platforms has proven to be a crucial differentiator, particularly for organizations heavily invested in Microsoft technologies. Customers also pointed to Red Canary's (1) superior threat detection capabilities versus Darktrace & CrowdStrike, (2) automated playbooks and dual-analyst review process [which has significantly reduced false positives], and (3) competitive pricing model / flexibility in seat count requirements, as the primary reasons why they were chosen over other vendors in the procurement process.

red canary	Walk us through the procurement / selection process. Why did you end up choosing Red Canary? What specific aspects stood out?
	Cost, though Red Canary was not the cheapest, was the first driver, followed by the quality and quantity of their alerts. Lastly, having their own SIEM greatly assisted. Red Canary has a very smart team, and I must say a good salesperson as well. **-CISO at Second Wave Delivery Systems**
	They are recommended by Microsoft and are an established vendor. Interviewed two of their customers who gave raving reviews. They have a great team of experts that do in-depth research on attacker techniques. **-CISO at Virtual Vaults**
	Contacted vendors, went through dog/pony show, selected four to go through a deeper review with, developed an RFI questionnaire that each vendor completed indicating their capabilities across MDR/XDR capabilities and our requirements, received pricing proposal, reviewed results of the questionnaire and proposal for fit, coverage, and budget, and selected Red Canary as the best fit. Their pricing is in the same ballpark as other vendors. **-Head of Information Security and Privacy at Ovative Group**
	Overall reputation and customer service. We sent out request for proposals and found that Red Canary's work would be better suited for our company. **-Tech Lead at First Citizens Bank**
	The integration with Carbon Black and the depth of expertise. The automation playbooks were very intuitive too. **-Vice President, Technology Security, Risk & Compliance at FTI Consulting**
	Good technology that was recommended strongly by our local security solutions VAR. Strong contributions to opensource and security community. Was cost competitive to Arctic Wolf and simpler to stand up vs using a Microsoft solution. **-IT Director at Dynamic Brands**
	We did a pretty extensive bake-off using real malware and a collection of fileless malware scripts. Our decision-making criteria was constrained to the speed at which our IR team could escalate IOCs, detection coverage, and the speed at which detected threats were escalated to our IR team. We specifically did not make decisions based on the managed service offerings, "single pane of glass," what our peers are doing, complexity of the tool, out-of-the-box rules, or false positives. **-CISO at Sittadel**
	Highly knowledgeable staff, dedicated "pods" of individuals, strong contributor to security community with free tools, articles, insight. They integrated with all our data sources and were a Microsoft partner with experts in that area. We were also happy how alerts were reviewed by two analysts before a "threat" is published. This cut down on false positives significantly. **-Information Security Manager at Nashville Electric Service**
	There was a well-established partnership between Carbon Black and Red Canary. As a district near a Cyber Centers of Excellence, recommendations from peers also helped point us in the direction of Red Canary. **-CIO at Columbia County School District**

Walk us through the procurement / selection process. Why did you end up choosing Red Canary? What specific aspects stood out?
We were users of Darktrace. We had a number of instances when we discovered that Darktrace had no knowledge of the intruder attacks but yet we did. We received the same attacks and found that Red Canary was a much better partner. **-Director of Product & Solutions at BCC Collaboration Company**
We worked with our procurement team to develop requirements for the RFP. We then evaluated the proposals we received and scored them based on a set of criteria. From the finalists, we selected 3 top contenders to interview and conducted a proof of value to evaluate their capabilities and features. Our internal team commenced security testing to test the vendor's detection and response time and efficacy. From there, we selected the solution. Red Canary won because they have a good threat intelligence team, their technology integrated well with our EDR provider, and they are a local company. **-Director of Information Security at Denver Water**
We tested all three vendors in the following areas: (1) Customization and Flexibility (2) Integration with existing systems (3) Log Management and Analysis (4) Incident Response Capabilities (5) Communication and Transparency. Red Canary had the fastest response time, and their active remediation worked flawlessly. **-CISO at Wash Laundry**
There is parity across all the vendors, so this came down to price & ability to fit into our MSFT ecosystem of Defender and Sentinel. Red Canary provided the most complete end-to-end service and were able to naturally integrate with our support team. **-Vice President of IT & Security at Allucent**
We were an early adopter of Red Canary. They were able to alter their tool to suit our needs and they had a competitive price. **-Security Engineer at Wide Open West**
We chose Red Canary because they provide an automated playbook to isolate host and notify specific people of threats. Additionally, they integrate with multiple products that we already own, not just the EDR. **-CIO at Rushmore Electric Power Coop**
Red Canary was selected for expansion because they already had a presence in our environment. We had them monitoring a small subset of computers/servers and expanded out to cover the entire campus. They are on state contract which is important for state/local government orgs. As one of the first managed responders to market, they are well-known, and their reputation is good. **-CIO at Southern Arkansas University**
I did a 30-day trial of each solution. UncommonX required a VM server and was agent-less. I liked the platform but was concerned about post breach abilities such as network isolation and remediation. Red Canary won the day with their framework and playbooks for remediation. The playbooks are very flexible, and I can create my own. The other important aspect is the integration options. Red Canary allows me to integrate our Cisco Umbrella in to the scan and detection process. We experienced a breach, and Red Canary detected it and shut it down immediately. **-Director of IT at Rollie Williams**
Aligned with our security objectives at a reasonable price point. Also felt we would not get "lost" as a client and would get good customer service. **-CTO at Sun Auto**
We wanted a MDR that did not depend on agents and could enhance our use of the Microsoft platform investments we were making. Red Canary stood out as a tool that leveraged existing capabilities with strong support and analytics that matched our price point and technical sophistication. While evaluating, we looked at other services that included agents and determined that their approach did not provide adequate coverage or increased the complexity of our security environment, especially as we have a heavy identity / SAAS profile. **-Vice President of IT Operations at Kilbourne Group**

Walk us through the procurement / selection process. Why did you end up choosing Red Canary? What specific aspects stood out?
I created detailed requirements and used negotiated RFP approach. Red Canary was able to natively support our EDR/XDR platform and our Cloud Identity provider. They were also able to ingest more data sources from different vendors without requiring a dedicated SIEM tool. Red Canary provides some SOAR capabilities via portal and were more flexible with automating response actions. Red Canary was competitively priced too and did not require multiple add-on subscriptions. Their price model was less complex compared to other vendors. Red Canary's sales team and sales engineers were very professional and paid attention to our use case. They were responding faster than some other vendors. **-Director of Cybersecurity at Mercer International**
We leveraged Red Canary on a conditional basis for one of our business units in the immediate aftermath of a major incident. We needed a quick way to increase our ability to detect and respond to threats coming from our EDR and had limited internal resources. Red Canary provided immediate threat detections and automated playbooks to ease the burden on our internal Incident Responders. In only a few months Red Canary was able to detect and stop several threats that would have lead to incidents with potentially major business impacts. This data allowed us to put together a business case to expand Red Canary MDR services to all our business units on a multi-year contract. **-Global Director, Cybersecurity Services & Engineering at Bridgestone**
Reviewed overall capabilities and was looking for a way to avoid adding more agents to the workstation. Since we already had O365 E5 seats, we needed to find a partner that would integrate with Defender and also other systems that would simplify what we needed to analyze in the SIEM. **-Head of Cybersecurity at PGA TOUR**
1. Alignment with our existing technology stack. Microsoft and SentinelOne EDR 2. Reputation and previous experience with vendor. Used Red Canary at another organization 3. Cost was competitive 4. Ease of implementation CrowdStrike Complete was our runner-up. Cost was a big factor as CrowdStrike seat count started at 300 where Red Canary was priced at our actual seat count of 200. **-Head of Technology and Security at VuePoint Diagnostics**
1. We first go through vendors to determine fit, functionality, and price. Once there we select the top three. 2. We go through full demos of the three chosen vendors to grade usability, current and future functionality, scalability, and implementation. 3. We select the vendor that best meets our needs and start the negotiation process. As for Red Canary: the aspect of them that tipped the selection to them was their team assigned to us. We were impressed with the team selection and how each member filled the functionality needs. We were/are confident in them and that trust relationship is a must. **-Director of IT at Pikes Peak Regional Building Department**
In this instance we understood we needed better coverage of our endpoints with 24/7 access and remediation when any event might occur. Normally we would research the marketplace and have multiple conversations with various vendors including pricing info. In this case we relied on the references of peers that were happily using Red Canary, so I reached and had the discussions. We then moved forward without additional competitive due diligence. It happens. We chose them as the integration was straightforward and the pricing was reasonable. We trusted our peers who had been using them for a while after they had actual security related events. **-CIO at Revere Electric Supply Co.**

What were the shortcomings of Red Canary's offering?

I felt the cost and connectivity into our current tech stack was lacking. **-CIO at Peloton Consulting Group**

Red Canary's managed detection and response product was fine. We didn't like their identity product as much. We also felt they were doing too much by working with so many other companies and maybe had lost focus on the core security field we were interested in. **-CTO at Florida State University**

CROWDSTRIKE	Walk us through the procurement / selection process. Why did you end up choosing your vendor? What specific aspects stood out?
	Arctic Wolf was in place when a breach occurred. CrowdStrike was engaged to perform forensics, and with the level of detail they provided, we made the strategic decision to move our EDR/MDR service to them. **-CIO at Independent Living Systems**
	CrowdStrike was the best value overall and had the biggest market brand name. It was recommended by peers and it's in the top left of Gartner's quadrant. **-CISO at Owens & Minor**
	We have the most internal expertise and familiarity with CrowdStrike's tools and offerings. The logic was that outsourcing incident response to the vendor whose tools we use would help us identify and resolve any potential issues or threats in a timely manner. **-Deputy CIO at Oppenheimer & Co. Inc.**
	KPCs are interoperability, cybersecurity and compliance, costs and pricing model, UX/UI of the platform used, talents and support, innovation including AI, scalability and reversibility. We either launch a formal RFP or go through a value-added reseller. **-CIO at Région Ile de France**
	We initially went through a VAR to help us identify the top 3-4 vendors that would best suit our business segment and size. From there, they helped to foster the introduction and schedule various demos with each and worked to obtain quotes from each. With CrowdStrike, we needed the "white-glove" treatment where they will detect, respond, and remediate as needed. Other firms could handle the first two areas but Falcon complete is what we needed for our specific use case. **-CIO at Outreach Health Services**
	Most of the systems were similar but we went with CrowdStrike since it's industry leader and provided us with full hands-off approach and guarantee insurance. **-CTO at Alliance Ground International**
	Reviewed whitepapers and received feedback from other CISO's which came up with the shortlist of 3 vendors. Microsoft was included because we had E5 licenses. SentinelOne and CrowdStrike were comparable, but the services provided by CrowdStrike were deemed to be stronger. **-CISO at Constellis**
	We felt CrowdStrike had the best track record for managing security in this space. We also thought their identity product went well in our space. Finally, we were looking for a company that could provide recovery assistance if we had a breach and CrowdStrike has an excellent reputation in that space. We looked at a couple of other providers but none of them had the complete package. Price was a consideration and CrowdStrike was the most expensive we looked at, but we felt the value was there. **-CTO at Florida State University**
	I brought in Expel, SentinelOne, CrowdStrike and Artic Wolf. We got down to SentinelOne and CrowdStrike with whom we did proof of concepts. After that, I asked for a best and final offer and CrowdStrike brought a good proposal and so I went that route. **-CIO at Marian University**
	Global reach, support for our toolsets, ability to meet our timeframes/SLAs, breadth of services, responsiveness, costs and scalability. **-CIO at Gallagher Bassett**

Microsoft Defender	Walk us through the procurement / selection process. Why did you end up choosing your vendor? What specific aspects stood out?
	Did research via Google, then went to Gartner to see how the solutions I found ranked against each other. The Microsoft offering stood out as being one of the best options available. Since we are a MS shop, the solution was priced well and since it's part of the same MS ecosystem, it seemed like a no brainer. Then I reached out to my distributor, CDW, to get the best pricing. **-CIO at Spitzer Autoworld**
	Microsoft's integration with our mainly Windows environment but also their surprisingly good tooling for Mac, Linux etc. **-CISO at GlobalSign**
	We ended up using Microsoft and Sophos after looking at various vendors and running through various demos. Since we have already standardized on Sophos and Microsoft, this additional offering was basically built into our workflows and process so it made a lot of sense for us. We really liked and started off with the Sophos MDR offering years back and are currently testing the waters with the Microsoft offering. I really liked the responsiveness and the ability to allow the Sophos SOC to real-time interaction with an endpoint for remediation capability. The reporting, dashboarding and real-time outreach from the Sophos team is top-notch and gives me an additional level of comfort running a global footprint with over 1000 endpoints. **-CIO at Peloton Consulting Group**
	We assess the market for the leaders and then outline what our requirements are according to our security frameworks. We then assess each of the products to ensure that they can meet our needs. When this is narrowed down we then approach the vendors and ask them for pricing and a demo of their product to gain an understanding of their security levels and accuracy in detection. We then take this information and decide on the solution for us. **-CIO at Dementia Australia**
	It made sense to us as we have tried to centralize as much on Microsoft as we could. We looked at CrowdStrike, and they had that huge screw up. We also looked at Arctic Wolf, but they ended up being too expensive. Our core competence is Microsoft tooling, so it was an easier transition. **-CTO at Immunotec**

SentinelOne	Walk us through the procurement / selection process. Why did you end up choosing your vendor? What specific aspects stood out?
	Great level of proactivity and engagement from the vendor. Their teams were very knowledgeable and were able to work seamlessly with our other vendors and partners. They complemented our other services well. **-CIO at Trafalgar Entertainment Group**
	The major reason we selected them was because our cyber insurance provider recommended them, following a breach in the company, and remediation. **-IT Manager at BMT Tax Depreciation**
	SentinelOne delivers a solid product and with Vigilance we expected a fast response time on incidents and/or threats that occur on our devices. The combination between automated response / sandboxing and their good warning system. **-CISO at Den Helder**

Insights | Vendor Selection Rationale: Red Canary

Red Canary was praised for its platform-agnostic approach and superior integration capabilities, which resonates well with organizations seeking to avoid vendor lock-in and maintain flexibility in their security stack. The company's ability to provide enterprise-grade security expertise while maintaining high-touch customer service has proven especially attractive to mid-market customers who feel underserved by larger providers like Microsoft. Customer feedback consistently highlights Red Canary's technical excellence, evidenced by low false positive rates and comprehensive detection capabilities, while also emphasizing the value proposition of competitive pricing combined with premium service quality. The platform's ability to support multiple EDR/EPP solutions and diverse technology stacks positions it well for sustainable growth in an increasingly complex security landscape.

red canary	Why did you choose Red Canary over the first-party offering of your endpoint provider?
	Cost plus a feeling of not being lost in the shuffle. We valued Red Canary's expertise. I would also say they have a great interface as well. **-CISO at Second Wave Delivery Systems**
	The expected quality of their offering was better than we would have received with the other providers. **-CISO at Virtual Vaults**
	Best set of integrations, acceptable pricing via our budget, great customer service and engagement through the sales process, great integration support. **-Head of Information Security and Privacy at Ovative Group**
	Keeping all your eggs in one basket is not a good idea. Plus distributing services ensures there is no one point of overall failure. **-Tech Lead at First Citizens Bank**
	Carbon Black did not offer a first party offering and still does not. We were using Carbon Black prior to engaging Red Canary. **-Vice President, Technology Security, Risk & Compliance at FTI Consulting**
	I wanted to have separation of endpoint tool and monitoring & detection. It has been helpful in preventing false positives from native AI. Red Canary provides leading edge enhancements to detection methods. **-IT Director at Dynamic Brands**
	It all came down to the detection timeline - the way Red Canary presents the most relevant data. Engaging different teams was as simple as copy and pasting. There is some unquantifiable philosophical comfort we get from the MDR platform being somewhat tool agnostic. A bespoke MDR platform is concerned with your outcome, while a first-party offering is rightfully only concerned with their scope. As an example: a first-party service that detects execution of password-stealing malware can be trusted to remove the malware, but if we "set and forget" the first-party monitoring service, our team might miss that a password needs to be reset. Because we are running the MDR platform without Red Canary's first-party monitoring service, Active Remediation, our own team measures the impact of each threat, so we know that an expert is always determining when the threat is remediated. S1 Vigilance will detect mimikatz, remove mimikatz, and consider the matter resolved. **-CISO at Sittadel**
	Expertise in Microsoft products and integrations. Extremely low amount of false positives during our PoC. Additionally, during third party pen test (during PoC) they detected more actual threats than any other provider tested. **-Information Security Manager at Nashville Electric Service**
	Due to the reputation of Carbon Black, market share and price points. **-CIO at Columbia County School District**
	We were too small for Microsoft as a client. Others either were too pricey or did not integrated, well with our existing technology stack. **-Director of Information Security at Denver Water**
	There were two main reasons: 1. They were able to use our existing Microsoft EDR (Defender) 2. Pricing. **-CISO at Wash**

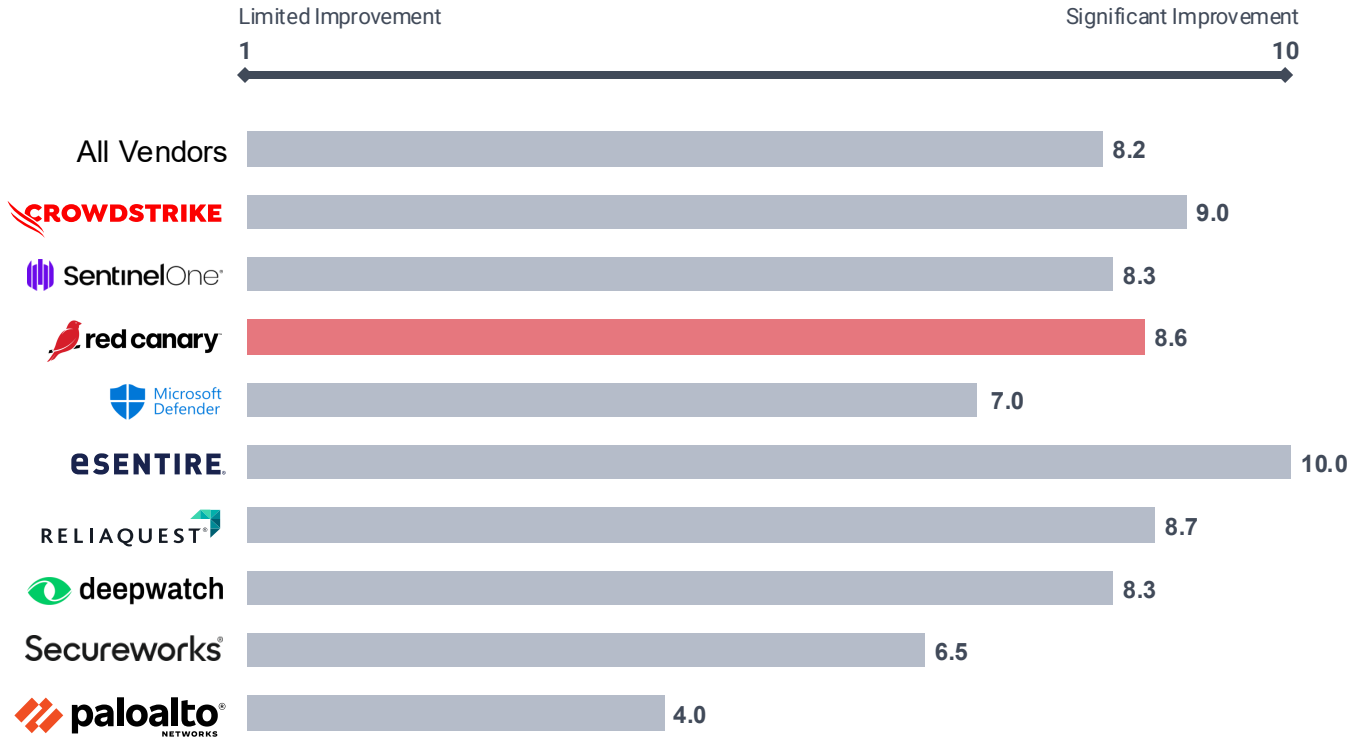
Insights | Vendor Selection Rationale: Red Canary

Why did you choose Red Canary over the first-party offering of your endpoint provider?
Comprehensive detection capabilities across all devices/assets. Advanced capabilities with behavioral based analytics. The team was very organized and easy to implement. **-Vice President of IT & Security at Allucent**
At the time, Carbon Black did not have an MSSP option. **-Security Engineer at Wide Open West**
Red Canary felt like a better product and a better user interface. **-CIO at Rushmore Electric Power Coop**
N/A. There is no first-party offering for Carbon Black. **-CIO at Southern Arkansas University**
Red Canary beat the first party offering because it was agent-based and allowed us to choose our preferred agent CrowdStrike. The competitor was agentless and required a physical server or a virtual server. Red Canary proved to be more powerful with the MITRE framework, integrations and powerful playbooks. **-Director of IT at Rollie Williams**
Value for price point. Additionally felt we would get improved customer service as a more boutique provider. **-CTO at Sun Auto**
First-party offering from Microsoft was not advertised. We did consider consultants that would work within Microsoft, but the relative complexity of the implementation was much higher. **-Vice President of IT Operations at Kilbourne Group**
Red Canary had much better integration support for products from other vendors compared endpoint providers offerings. It allowed us to integrate and monitor more standalone tools in our cyber stack. **-Director of Cybersecurity at Mercer International**
We have multiple EDR/EPP platforms within our environment, Red Canary offers multi-platform integration and ingests telemetry data from all of these sources. It allows us to get the same baseline protection regardless of the endpoint provider and offers us flexibility in the ability to switch EDR solutions and maintaining the same threat detection in the future. **-Global Director, Cybersecurity Services & Engineering at Bridgestone**
We didn't want all of our eggs in one basket. **-Director of Product & Solutions at BCC Collaboration Company**
We're mostly an AWS shop, so we wanted to get additional analyst visibility into GuardDuty and other logs coming out of AWS. There were also other playbooks that we wanted to run so that issues could be routed to the correct groups when security issues were identified. **-Head of Cybersecurity at PGA TOUR**
Red Canary's focus is on detection and response whereas S1 is more of an add-on to their product. We do have a diverse set of integrations with Red Canary that S1 did not offer, particularly the ingestion of our network traffic/logs. The Red Canary MDR offering was also more mature than S1's Vigilance. **-Head of Technology and Security at VuePoint Diagnostics**
Red Canary has a very good reputation and since we switched to them, they have always been available. They also provide insight via their monitoring of possible issues we should be checking out. We don't have the security expertise and Red Canary has become a trusted partner with this. They have also been around a while and we felt they offered the best solution for us. **-Director of IT at Pikes Peak Regional Building Department**
My first party XDR is Microsoft. I don't see their offering as actually being competitive. We certainly have some overlap considering the logs feeding Red Canary are from our Microsoft security tools but having the hands-on touch that we would actually have access to sold us on their offering. **-CIO at Revere Electric Supply Co.**

Insights | Security Posture Improvement Since Adoption

Red Canary drives a significant positive improvement (8.6) on customers' security operations, particularly for organizations lacking internal 24/7 security coverage. The service consistently delivers value through workload reduction, improved response times, and enhanced threat detection accuracy, with multiple customers reporting substantial decreases in false positives compared to previous solutions. The platform's strength lies in combining automated monitoring with expert analysis, though some sophisticated customers note limitations in automated detection capabilities compared to native tools like Microsoft Defender. The service shows particular effectiveness for mid-market organizations transitioning from basic security tools to comprehensive MDR coverage, with customers highlighting improved security posture through better incident response processes and security expertise.

How would you characterize the level of improvement your vendor has had on your security posture?



red canary	Please explain your 'Posture Improvement' ranking and the ways in which your vendor has had an impact.
10	At the time, we had no detection and response around endpoint telemetry. Red Canary filled a gaping hole in our new security program. **-Security Engineer at Wide Open West**
10	We now have real 24x7 security monitoring and alerting, better log collection and coverage, which offloaded at least half an FTE of workload (which never would have included 24x7 coverage) enabling us to take on additional responsibilities and support additional projects to further grow our security program. **-Head of Information Security and Privacy at Ovative Group**
10	Red Canary is like many tools that are used to improve security coverage, but they're one of the only tools that has improved communication among our teams. **-CISO at Sittadel**
10	There is a little matrix that can be used to define how Red Canary has improved our posture. As a school district, security is not on the forefront of most districts radars which becomes a concern when incidents do occur. Personally speaking, when an anomaly has occurred at our district, Red Canary has taken immediate action, and notification has resolved the issue nearly immediately. **-CIO at Columbia County School District**
9	We were using a more traditional MDR prior and their skills and time to respond were bad. After hours team really seemed asle ep. Red Canary has done well for us, much more consistent and efficient. I've been impressed with their detection and response so far. No additional tools to use (AlienVault, Sumo Logic, etc) which keeps costs lower. They don't analyze KnowBe4 logs yet, though they do ingest them, so, that is a minor gripe. They also don't have 2nd-level analysts on the weekends though, which can cause some delay on escalation. **-CISO at Second Wave Delivery Systems**
9	We are confident in their ability to find attacks on our devices. The level of insight in our endpoint devices has drastically increased. **-CISO at Virtual Vaults**
9	I no longer worry about pawing through vulnerability logs, updates to EDR or worry about removal tools. It has freed up my time and reduced the required skill for support. We have had zero incidents that impacted business since implementing. **-IT Director at Dynamic Brands**
9	It provides 24/7 monitoring services that we cannot simply do with internal to team. This led to a significant improvement to our mean time to detection and response. **-Director of Information Security at Denver Water**
9	24/7 monitoring and security automation for our smaller, short-staffed company. **-CIO at Rushmore Electric Power Coop**
9	Prior to Red Canary we did not use an MDR/EDR we just relied on Sophos antivirus for protection. We added Sophos MDR but the calls normally came hours after an issue. Red Canary is near real-time and allows me to respond much quicker. Red Canary has a process in place to determine if the incident is an attack and not a false positive. We had a lot of false positives with Sophos. Red Canary really made me feel much better about our security. **-Director of IT at Rollie Williams**
9	We saw significant improvement in our security posture after implementing the Red Canary MDR. Prior to Red Canary we did not have 24/7 coverage, suffered from alert fatigue and false positives and saw threats go undetected until very late in the Attack kill chain. Through Red Canary's threat detection engine, automation and expert analysts to review the threats, we were able to expand our coverage, reduce our false positive rate to near zero and stops threats before there was a major impact. We also gained additional visibility to enhance our posture by removing riskware/adware with the environment. **-Global Director, Cybersecurity Services & Engineering at Bridgestone**
9	1. They educated us on security aspects we didn't think about. We thought we were looking at our security holistically be we weren't. Red Canary filled in the gaps to solidify our attack surfaces. 2. Red Canary ingests data from our endpoints and suing this data has allowed them to report on attack trends which helps us move quicker to eliminate our weaknesses. 3. Red Canary's service just works**. -Director of IT at Pikes Peak Regional Building Department**

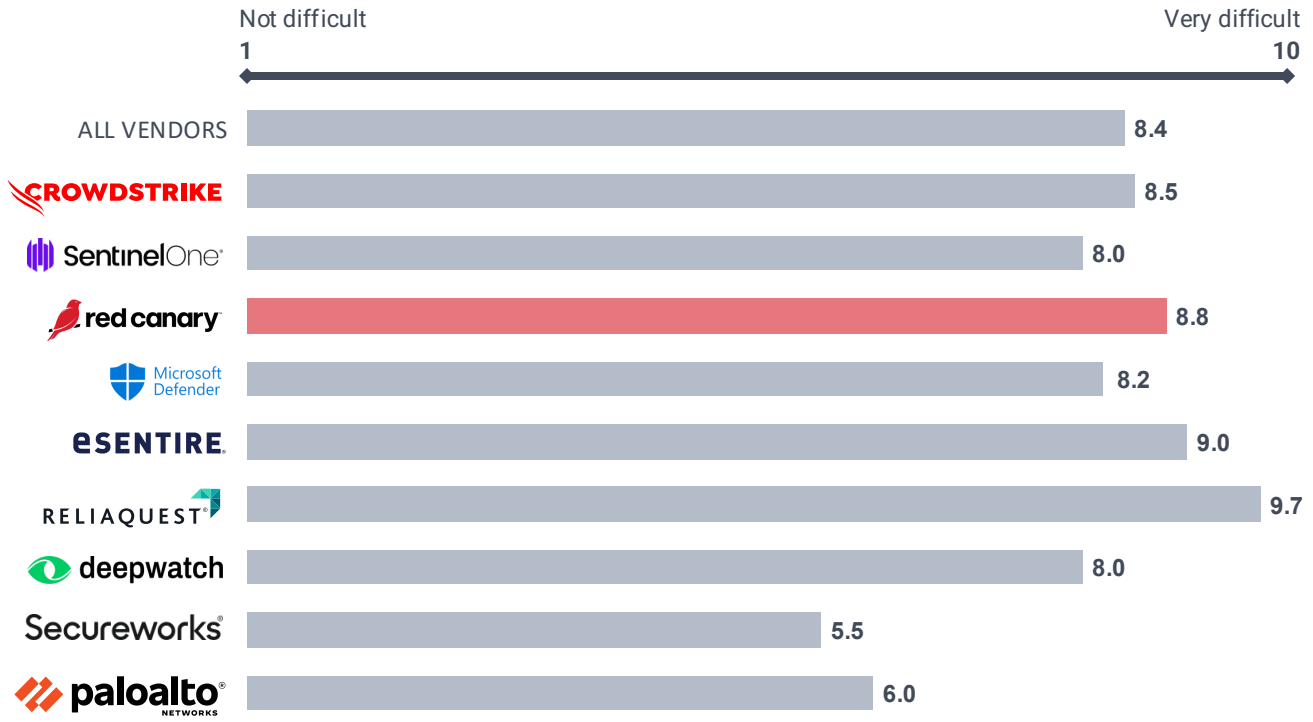
red canary	Please explain your 'Posture Improvement' ranking and the ways in which your vendor has had an impact.
9	We do not have an internal SOC. Having Red Canary in place provides for 24/7 monitoring and response to a specific set of concerns. We have significant gaps outside of normal business hours. Plus we have a skills gap as our IT department is small and we do not have dedicated security. The reactions and assistance we have had over the past year has proven to me we are in a much better place than we were prior to implementation. **-CIO at Revere Electric Supply Co.**
9	Our organization previously only had limited security support from our MSP. We felt it important to add a security vendor with 24X7 monitoring and response. **-Head of Technology and Security at VuePoint Diagnostics**
8	It has helped us monitor and ensure that we are secure. As it is an external vendor with dedicated resources, we have peace of mind. **-Tech Lead at First Citizens Bank**
8	We are not staffed 24x7, Red Canary has given us piece of mind that our environment is being monitored for threats, and those threats remediated around the clock. Additionally, we do not have dedicated SOC analysts, their ability to review and quickly triage threats has made us feel more comfortable that we are not missing anything. **-Information Security Manager at Nashville Electric Service**
8	We were moving from another MDR that fell short on detection and then the response many times. We were detecting before them. With Red Canary we no longer have to be involved as before. **-Vice President of IT & Security at Allucent**
8	Better toolset. More knowledgeable team. Provided automation we were not leveraging before. **-CTO at Sun Auto**
8	Red Canary has improved the "closed loop" nature of threat detection that was previously "noise" to our organization. We feel comfortable with the automation and managed responses provided by Red Canary, and knowing that it has full surface area to our entire device and identity environment is a huge benefit. **-Vice President of IT Operations at Kilbourne Group**
8	It's a very rough scale and 8 is somewhat of a gut feel. I would suggest previously that we had a security posture of 6. **-Director of Product & Solutions at BCC Collaboration Company**
8	Provided a better structure & response process that we hadn't had before. The additional level of analysis allows for our internal analysts to handle escalations instead of having to weed through base level issues & reports that are typically don't require actions. **-Head of Cybersecurity at PGA TOUR**
7	They have provided security expertise and clarification on security events which we need to look into. Their ticketing platform provides great audit artifacts as well. **-Vice President, Technology Security, Risk & Compliance at FTI Consulting**
7	The 24/7 monitoring of our network has ensured that any suspicious activity is detected and addressed immediately. With their dedicated security experts, they can isolate affected systems immediately. **-CISO at Wash**
7	24/7 SOC monitoring is not possible for orgs our size without a company like Red Canary. They have been able to respond to after-hours incidents and have been very communicative any time there is an alert. **-CIO at Southern Arkansas University**
7	Now we have reliable 24/7 monitoring, triage and alerting for our XDR platform. Our previous MSSP was unable to deliver it. **-Director of Cybersecurity at Mercer International**

CROWDSTRIKE	Please explain your 'Posture Improvement' ranking and the ways in which your vendor has had an impact.
10	The Falcon Complete product allows us to view our security posture from multiple angles. These views, along with CrowdStrike's ability to remediate, has allowed us to drastically improve the security of our environment. **-CIO at Independent Living Systems**
10	Well before I arrived at our company, our security posture was lacking and immature. Detection was only possible post-event on a manual case by case basis. Having CrowdStrike in addition to the included Microsoft Defender toolset, allows us to get much more proactive notifications and many times, remediation has already occurred by the time they send their alerts. **-CIO at Outreach Health Services**
10	It just works and it's hands off and everything is being managed and I feel like we are in good hands. They detect and clean and we get reports asap when things happen. **-CTO at Alliance Ground International**
10	Over the years, CrowdStrike has repeatedly detected and stopped attacks without needing to engage our team. **-CISO at Constellis**
9	Minimal implementation issues, minimal administrative overhead, high efficacy as it relates to the detection of malicious behavior. **-CISO at Owens & Minor**
9	In terms of capacity to scale, breadth of offering, reactivity, expertise, partnerships and automation. **-CIO at Région Ile de France**
9	(1) They educated us on security aspects we didn't think about. We thought we were looking at our security holistically because we weren't. Red Canary filled in the gaps to solidify our attack surfaces. (2) Red Canary ingests data from our endpoints and suing this data has allowed them to report on attack trends which helps us move quicker to eliminate our weaknesses. (3) Red Canary's service just works. **-Director of IT at Pikes Peak Regional Building Department**
9	They didn't have a real security footprint before CrowdStrike, it was a drastic improvement. **-CTO at Commercial Tool Group**
9	CrowdStrike has caught and fixed issues 4-5 times in situations where my organization had not even been made aware of. The saying is that if it gets to your MDR, you're in trouble since that is the last "catch". Luckily, CrowdStrike has been there as that last catch. It also made me move our "detection" further back in the process and Falcon Complete is now ensuring that items are caught before they get to the endpoint. **-CIO at Marian University**
8	Their expertise in their product set has helped close the gaps where our internal resources were lacking knowledge and experience. Their guidance on using the tools and configuring them has helped our organization keep attacks and threats away. **-Deputy CIO at Oppenheimer & Co. Inc.**
8	We had no EDR or managed threat and response before. We really weren't a 24/7 shop and often could only respond to attacks after they happened. CrowdStrike completely changed how we manage and deal with threats and attacks in a good way. **-CTO at Florida State University**
7	Have brought global expertise to the team and uplifted maturity. Improved processes and procedures. Expedited incident response and speed to contain. **-CIO at Gallagher Bassett**

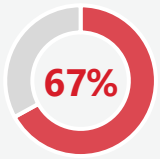
Microsoft Defender	Please explain your 'Posture Improvement' ranking and the ways in which your vendor has had an impact.
9	Prior to the purchase we were not using this type of solution, nor did we have the 24x7x365 coverage. So it was a game changer for us and our posture. **-CIO at Spitzer Autoworld**
8	We had insufficient and manual monitoring prior. We also had a lot of penetration with bad links, takeover attempts, etc.. They are keeping us honest in terms of the way we think about security. **-CTO at Immunotec**
7	Better visibility. Good escalation and isolation processes. Quicker detection and response. Subject matter expertise. **-CISO at GlobalSign**
7	The product has allowed us to review all of our policies for our systems and platforms. As we are mostly a Microsoft shop it provided us with an easy implementation relative to other solutions. We follow Essential 8 and it has allowed us to implement almost all of the measures aligning to this framework. **-CIO at Dementia Australia**
4	We are still working with this new platform and combine that with the fact we already have Sophos engaged via their MDR offering we are not 100% seeing the value of the MS offering just yet. I am very confident based on the soak time we have had with Sophos and we are still building that with MS as a newer vendor and seeing where Sophos might miss something and MS can truly add additional value for the cost. **-CIO at Peloton Consulting Group**

SentinelOne	Please explain your 'Posture Improvement' ranking and the ways in which your vendor has had an impact.
9	We now have excellent visibility of our environment and we have also been able to demonstrate to our cyber insurance brokers that we are taking this area seriously and have a capable partner to help us stay secure. **-CIO at Trafalgar Entertainment Group**
8	We have a lot more data and much better tooling, now. However, sometimes it is overly militant and inflexible - e.g. blocking some games on staff personal devices that use anti-cheat engines. **-IT Manager at BMT Tax Depreciation**
8	We didn't have the capacity to reach 24/7 protection without a solid partner. SentinelOne Vigilance made sure we were at all times (even during weekends and holidays) covered against attacks. **-CISO at Den Helder**

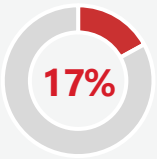
How difficult would it be to replicate the efficiency of your MDR / MSSP Provider with an in-house team?



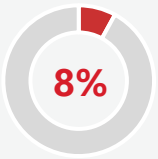
How does the cost of your vendor compare to doing detection and response in-house?



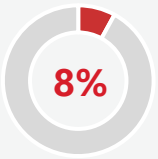
Significantly Less Expensive



Somewhat Less Expensive



About the Same



Somewhat More Expensive

Significantly More Expensive

What role do you foresee Red Canary playing in your organization's long-term security strategy?
I'm at a multi-company VC entity. We have adopted Red Canary at a second venture due to results at first. No additional staff or detection purchases are required. Huge cost savings, drastically undercuts competition. I have 25+ years of incident response experience, so can cover it all with the right tools. This is the right tool for our SMB. **-CISO at Second Wave Delivery Systems**
We hope to partner with them long-term, but everything depends on how the MDR market evolves. **-CISO at Virtual Vaults**
We will continue with them for the foreseeable future. It will be years before our security team grows enough that we could consider on-call shifts and bringing monitoring in-house, and if we did we'd also have to add other software to enable log collection and monitoring. **-Head of Information Security and Privacy at Ovative Group**
As a regular partner with continuous improvements and securing our infrastructure long-term. **-Tech Lead at First Citizens Bank**
Being a trusted partner for MDR/XDR and threat intelligence going forward long term. **-Vice President, Technology Security, Risk & Compliance at FTI Consulting**
Likely to renew in coming year, but may switch to MS Defender from SentinelOne. That is as long as my current pricing stay stable and does not increase significantly. **-IT Director at Dynamic Brands**
We are monitoring the additional functionality (cloud security, data security, identity protection, etc) that Red Canary releases. Today, we are accomplishing these outcomes as effectively internally for a lower cost, but we expect that we will eventually throw several different sources at Red Canary. **-CISO at Sittadel**
I see Red Canary being a long term partner, they have proven theirselves in our environment. We offset the need for dedicated in-house SOC services by utilizing their services. This not only provides better service, but reduces cost significantly. **-Information Security Manager at Nashville Electric Service**
Some sort of EDR solution will always be in play in our environment. There is no reason to change away from Red Canary as they have provided exceptional service. **-CIO at Columbia County School District**
They play a role of a tier-1 security analyst and a security operations advisor to us. **-Director of Information Security at Denver Water**
I am looking into adding additional services such as M365 Account Protection and IAM protection. **-CISO at Wash**
Would be interested in expanding our capabilities as Red Canary grows over time. **-Vice President of IT & Security at Allucent**
They will continue to provide detection and response capabilities around the endpoint, and may extend into other domains (identity, cloud, etc.). **-Security Engineer at Wide Open West**
They enable us to have protection without requiring us to build a dispatch center to monitor our endpoints. **-CIO at Rushmore Electric Power Coop**
Red Canary, or another MDR, will continue to monitor our endpoints and workstations to provide the 24/7 service that is required in today's cybersecurity landscape. **-CIO at Southern Arkansas University**

Insights | Long-Term Outlook [Red Canary]

What role do you foresee Red Canary playing in your organization's long-term security strategy?
Red Canary has been an integral part of our security posture for the last 2 years since we implemented it. Last year I would have said that I could never see us replacing it but after the CrowdStrike outage and Red Canary requiring at least Microsoft E3 I am thinking about replacing it. During that change I lost the integrations with Defender, Entra and Graph. **-Director of IT at Rollie Williams**
We continually evaluate security as it is ever changing. Their ability to stay current with industry innovation and providing good service for price will be the ultimate measure of them staying as a long-term partner. **-CTO at Sun Auto**
We foresee Red Canary being integrated into more aspects of our system and potentially a SEIM offering which would give us comprehensive cloud and network coverage. **-Vice President of IT Operations at Kilbourne Group**
I expect to keep Red Canary in my portfolio for some time. Red Canary is a pure play MDR vendor with almost no proactive offerings, and it can limit their options moving forward. **-Director of Cybersecurity at Mercer International**
In the near-term I see Red Canary as a partner and an extremely important part of our security strategy. We will probably continue to analyze our long-term strategy of in-house vs. MDR, but the current ability to hire and retain in-house talent makes for a difficult business case as the higher MDR costs are offset by the risk reduction in threat mitigation. As with all of security, it will also depend on changes in the security market and the threat landscape. **-Global Director, Cybersecurity Services & Engineering at Bridgestone**
We see Red Canary as a long-term partner, although we will review that annually. **-Director of Product & Solutions at BCC Collaboration Company**
Continued utilization, but we will continue to re-evaluate as the tolerance for additional agents on workstations change or other factors force us to migrate away from Defender. **-Head of Cybersecurity at PGA TOUR**
We started with a 3-year agreement and I expect if they continue to provide good products and service we will continue to partner with them. Our long-term strategy is to work with the best partners available and to not in-house security. Our business is healthcare, not technology. **-Head of Technology and Security at VuePoint Diagnostics**
We will continue to use them as they are a trusted partner. We will still evaluate other vendors on an every other year basis. That is due diligence we need to continue with all our IT vendors. -**Director of IT at Pikes Peak Regional Building Department**
I feel we continue to use them and also integrate more logs into their platform thus providing us with better coverage as we continue to make changes and evolve our security infrastructure. We have no plans to develop our own SOC as we simply cannot afford even a crude implementation of one today. **-CIO at Revere Electric Supply Co.**

Insights | Long-Term Outlook [CrowdStrike]

CROWDSTRIKE	What role do you foresee your vendor playing in your organization's long-term security strategy?
	They are part of the plan to be a long term partner. There are no plans to scale back or terminate the service. **-CIO at Independent Living Systems**
	Most likely will keep it as a solution for EDR, and might expand to their cloud solution as well. **-CISO at Owens & Minor**
	We don't foresee our company moving away from CrowdStrike for our long-term security posture and strategy. They are a trusted partner of ours that have been integral in keeping our environment stable and safe. **-Deputy CIO at Oppenheimer & Co. Inc.**
	Long-term partners - we view them as an extension of our team and have a close relationship with different members of their team. **-CIO at Région Ile de France**
	We have expanded our relationship with them to include their SEIM offering in addition to the Falcon Complete offering. I would expect if they become a market leader in other security aspects through internal development or acquisition, they could expand their footprint. **-CIO at Outreach Health Services**
	It's a long-term partnership. We do not want to hire for this since this industry is hard to keep a team engaged within our organization and turnover will be high and costs will be much higher than what we are paying CrowdStrike. **-CTO at Alliance Ground International**
	We plan to stay with CrowdStrike and expand our investment in them with their other offerings like Identity and Falcon for IT. **-CISO at Constellis**
	We will expand our usage of their products and modules over time. I see them taking a larger role in our security stack. **-CTO at Florida State University**
	I would have to hire a team if we didn't have CrowdStrike. So it would be vastly more expensive to hire someone. **-CTO at Commercial Tool Group**
	I will never be able to afford a security team with a CISO and multiple cybersecurity analysts. As quickly as you get them trained, they head for more money. My team is only 18 to cover all of IT so trying to get an additional team of 3-5 people just isn't in the budget. **-CIO at Marian University**
	They or a similar partner will be an ongoing critical part of our security strategy. They will operate as part of our security team and services to be delivered. **-CIO at Gallagher Bassett**

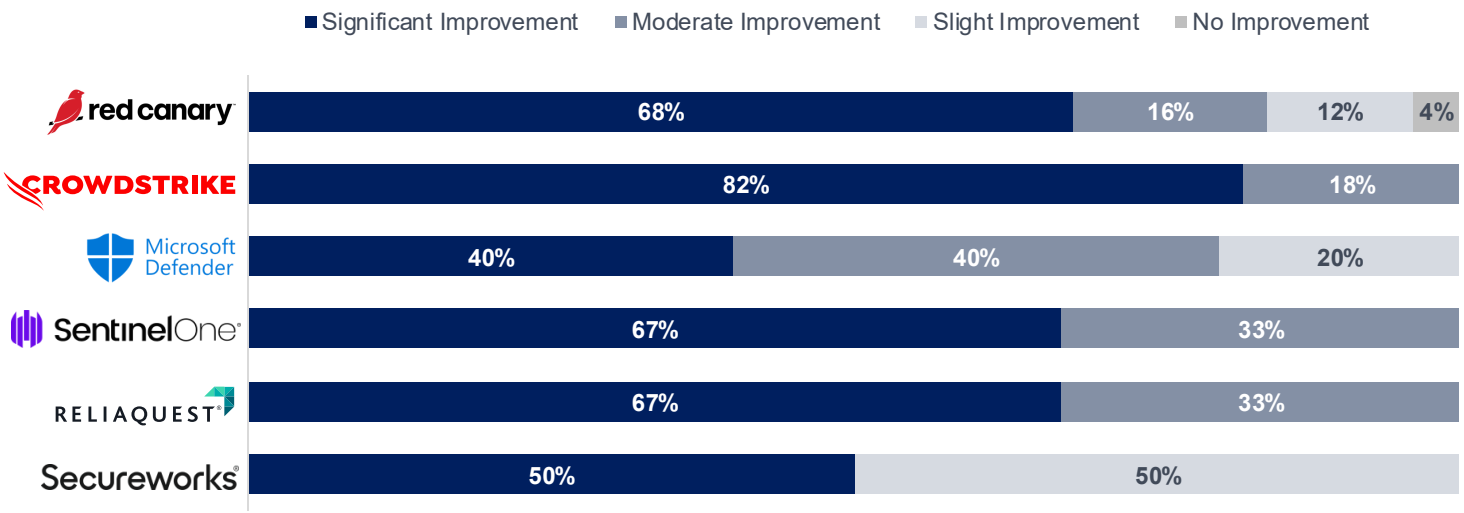
Insights | Long-Term Outlook [Microsoft Defender, SentinelOne]

Microsoft Defender	What role do you foresee your vendor playing in your organization's long-term security strategy?
	It's likely here to stay, assuming no crazy price increases, and/or no major breaches. **-CIO at Spitzer Autoworld**
	Critical role given its integration capabilities with our mainly Windows-based environment. **-CISO at GlobalSign**
	Jury is still out as we are very fond of the Sophos MDR offering and have been using it for years now. Time will tell! **-CIO at Peloton Consulting Group**
	They will be a key part of the organization, but it will be something that we will continually review. **-CIO at Dementia Australia**
	We will stay with them, even though they are more expensive. Security can no longer be an afterthought, and I have been layering in more and more tools every fiscal year. It is our reality now. **-CTO at Immunotec**

SentinelOne	What role do you foresee your vendor playing in your organization's long-term security strategy?
	We partner with the team well and they are helping us to shape our ecosystem and to engineer our areas of concern or potential flaws. **-CIO at Trafalgar Entertainment Group**
	We intend to stick with them for a long time, and have no plans to bring it in-house. **-IT Manager at BMT Tax Depreciation**
	The same role as the current situation. A cybersecurity partner helping to maintain our security posture 24/7. **-CISO at Den Helder**

68% of Red Canary customers suggested that they have seen a significant improvement in their organization's ability to accurately detect threats. Customers suggested that Red Canary (1) often detects sophisticated threats missed by native tools (2) significantly reduces false positives and noise (3) provides effective 24/7 coverage with rapid response times (4) offers value-add services beyond basic EDR through behavioral and contextual analysis.

What type of improvement has your vendor had on your organization's ability to accurately detect threats?



red canary	Can you briefly describe a situation where your vendor identified a threat that might have been missed without it.
	They had alerting for email rules being created called "." and alerting for email rules moving emails from named individuals to the RSS folder. That was not caught by our other MDR. **-CISO at Second Wave Delivery Systems**
	We have tested Red Canary extensively with all kinds of malware samples when we just engaged them. **-CISO at Virtual Vaults**
	They've caught multiple alerts from connected systems that we've not monitored closely. Thankfully, we've had no impactful th reats in our environment (knock wood). **-Head of Information Security and Privacy at Ovative Group**
	They are up to date with the market enhancements needed and that helps. **-Tech Lead at First Citizens Bank**
	I can't think of one that might have been missed. There were several that our NGFWs stopped and alerted us to which Carbon Bl ack and Red Canary allowed to go through, but using Red Canary we were able to determine the payload was never delivered. **-Vice President, Technology Security, Risk & Compliance at FTI Consulting**
	Quickly identified PUP installed on machine that was left logged in by domain admin which was being used by a child of an emp loyee. **-IT Director at Dynamic Brands**
	While Red Canary did not add any discernible detection coverage under our endpoint SKU alone, they have accelerated the speed of our detection. **-CISO at Sittadel**
	During a scheduled third-party security red team, Red Canary detected a side loaded DLL which initiated a C2 Channel over an enc rypted HTTP session to a .azurewebsites.com domain. This was completely missed by Defender and our internal team. This was detected within ~2 hours by Red Canary. **-Information Security Manager at Nashville Electric Service**
	As an organization with a significant number of mobile users, Red Canary is able to remotely "shut down" ransomware and other processes remotely. This has occurred on at least two occasions. **-CIO at Columbia County School District**
	They were able to identify an attempt of privilege escalation on a local server during an penetration testing that we would h ave missed. **-Director of Information Security at Denver Water**
	We had a suspicious login at 2am PST when the majority of my team was asleep. Red Canary was able to disable the account that was compromised and stop any spread before we woke up. **-CISO at Wash**
	Detecting unusual human behaviors and activity. **-Vice President of IT & Security at Allucent**
	We have had numerous attacks that have evaded traditional AV that Red Canary has been able to identify. From eternal blue to crypto miners to web exploits**. -Security Engineer at Wide Open West**
	They are the experts and are looking at items that cortex might not have caught or traffic that isnt detected. Cortex will rank it as Low, Medium, or Hight but Red Canary has their own level of risk. **-CIO at Rushmore Electric Power Coop**
	Red Canary provides the alerting and visibility needed to learn when certain apps are run. For instance, we wanted to get not ified when anyone installed or runs Wireshark or Nmap on a domain computer. Red Canary helped us set up rules to trigger an incident when it happens, and it has happened. We are a school with a cybersecurity program, and more often than not there is a student doing things from a place they shouldn't, so we inform the student and instructor to only use those tools within the designated labs. **-CIO at Southern Arkansas University**

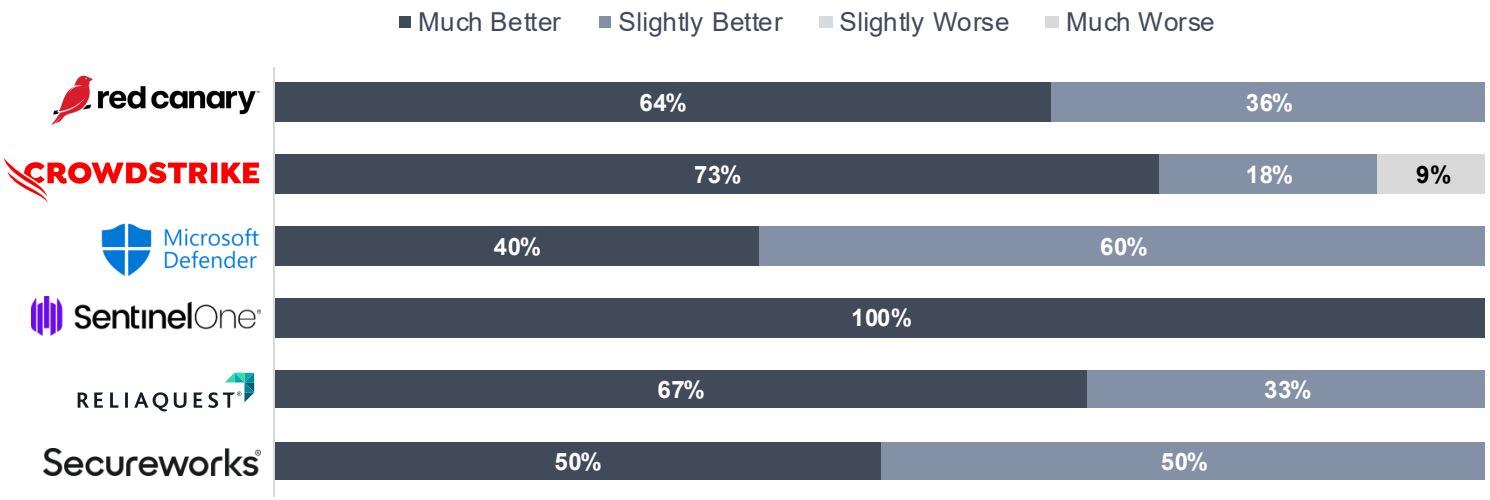
red canary	Can you briefly describe a situation where your vendor identified a threat that might have been missed without it.
	We have thankfully had low threats based on our profile configuration, however, there have been stale accounts that have indicated compromise which were immediately shut down due to automation rules. **-Vice President of IT Operations at Kilbourne Group**
	Not providing an example. I will say they have reduced false positives significantly and automation has correlated to immediate containment based on the rules we set. **-CTO at Sun Auto**
	One of our users opened an email from someone she thought she knew and "logged into Office 365" to view some artwork. It was a phishing email and she was compromised immediately via the install of eM Client. Red Canary detected it via the Cisco Umbrella logs and I was able to stop any further breaches. Without it we would not have discovered it until something bad happened. **-Director of IT at Rollie Williams**
	Red Canary heavily depends on our existing EDR tool for detection and therefore detection rate did not change significantly. Although reaction time and 24/7 coverage were significantly improved. **-Director of Cybersecurity at Mercer International**
	We have seen where Red Canary has been able to detect threats from ransomware groups that utilize "living of the land" techniques. These techniques utilize seemingly normal processes, extensions, etc. that you would expect with an operating system for malicious purposes and went undetected by EDR alone. **-Global Director, Cybersecurity Services & Engineering at Bridgestone**
	This was certainly the case with Darktrace. To date, we have not known of a threat that Red Canary has missed. **-Director of Product & Solutions at BCC Collaboration Company**
	The main situation is that false positives are reduced so that true positives are actually able to be actioned quickly. The time to live on threats is significantly reduced because there's not a need to constantly filter through all the noise and we can focus on the signal. **-Head of Cybersecurity at PGA TOUR**
	We had no monitoring or correlation of signals previously. Threats identified have been limited to riskware and possible account compromise. **-Head of Technology and Security at VuePoint Diagnostics**
	We had 'spun up' a virtual machine in MS Azure cloud for serving GIS data. It is public facing so we needed to have constant monitoring on it which Red Canary provided. They monitored surface attacks coming from multiple countries trying to find vulnerabilities. Using their data and recommendations, we were able to tighten up that surface which decreased the amount of attacks. -**Director of IT at Pikes Peak Regional Building Department**
	There have been a reasonable number of instances where we were notified of potentially malicious activity where we were not alerted via our standard alerts. In all cases Red Canary also follows up and takes action based upon rules we have set. If we did not have Red Canary in place we would be reliant on internal research and action which would take significantly longer to act upon. **-CIO at Revere Electric Supply Co.**

CROWDSTRIKE	Can you briefly describe a situation where your vendor identified a threat that might have been missed without it.
	While not an actual threat, CrowdStrike has identified and stopped our systems engineers attempting to work around security p rotocols to perform activities. **-CIO at Independent Living Systems**
	Inbound email malware attack. Microsoft's O365 missed the threat on the way in but CrowdStrike detected/blocked when the exec utable was activated. **-CISO at Owens & Minor**
	CrowdStrike was able to detect a potential threat from an external connection and once the tool identified the issue, our int ernal network/incident response team reviewed with the CrowdStrike team to collaborate on the right mediation and resolution. **-Deputy CIO at Oppenheimer & Co. Inc.**
	It was during a week with a DDoS attack that went under the radar of our automated detection and they saw in real time the at tempts. **-CIO at Région Ile de France**
	There have been numerous detections it has alerted and remediated that our other provider (defender) did not even alert. One key one is wave browser and how it tries to auto download and install through rouge Google-ads. CrowdStrike will detect and prevent any software execution and quarantine the file automatically. **-CIO at Outreach Health Services**
	They detect everything that needs to be detected on the devices. We only wish email had a similar solution. **-CTO at Alliance Ground International**
	CrowdStrike has detected lateral movement of accounts across our environment and isolated the account and killed communicatio n from those devices. **-CISO at Constellis**
	We had a ransomware attack happening at 1 AM. It hit a decentralized unit (not managed by us or CrowdStrike). The attack star ted to propagate, and we had CrowdStrike call us to tell us that one of our domain servers was acting off and they shut it down. We got our on-call folks on it, detected the attack from another area and disconnected them. We would never have seen this until morning without CrowdStrike and by then it would have been to o late. **-CTO at Florida State University**
	My guys internally are pretty good but they just can't be here 24/7 and we watch our systems like a hawk. Not that we can't b e breached of course. **-CTO at Commercial Tool Group**
	We've had three events where an endpoint was about to be infected and CrowdStrike saved the day. We're a BYOD environment and prior to having CrowdStrike, we had endpoint issues 2-3x/month. Now very rarely do issues even get to the endpoint and if they do, CrowdStrike tackles and cl eans them well in advance of my team even knowing about it. **-CIO at Marian University**

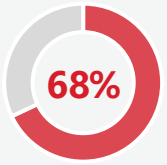
Microsoft Defender	Can you briefly describe a situation where your vendor identified a threat that might have been missed without it.
	There have been several situations already where a threat occurred in the off-hours and we would not have known or done anything about it until the next day (likely too late). **-CIO at Spitzer Autoworld**
	Phishing clicks. Attempts of infected machines to spread. Microsoft 365 mailbox hijacks and isolation thereof. Attacks on our federated authentication service. **-CISO at GlobalSign**
	We are still trying to access this level of benefit as we have yet to see Microsoft catch something Sophos didn't. I like the concept of having two different sets of professionals monitoring our endpoints and infra but will need more time to determine if the Microsoft offering will show the necessary value long-term. **-CIO at Peloton Consulting Group**
	Items that looked like they were patched but needed policy changes that would have otherwise not been detected. **-CIO at Dementia Australia**
	We had a senior member of staff click a bad link that caused all sorts of problems with impersonation, attempts to penetrate finance, and other issues. We now get reports of penetration attempts and deflection, and it allows us to train people more succinctly, as well as have a better comfort level that we are protected. **-CTO at Immunotec**

SentinelOne	Can you briefly describe a situation where your vendor identified a threat that might have been missed without it.
	We have been able to work with the team to review specific threats coming in from key geographical areas that are not actual threats so we can centralize our attention to more likely sources of threats. Previously we had a more blanketed approach. **-CIO at Trafalgar Entertainment Group**
	It has picked up staff installing cracked software / key generators with malicious payloads, that we would otherwise not have known about. **-IT Manager at BMT Tax Depreciation**
	SentinelOne does not rely only on signature-based detection and therefore found a behavioral anomaly with their AI system. An unusual powershell command was executed, spawning child processes with encrypted payload. Antivirus was not able to detect, but Vigilance did. **-CISO at Den Helder**

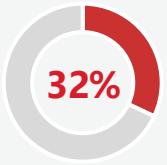
How does your vendor's accuracy/false positive rate compare to alternatives you've used or evaluated?



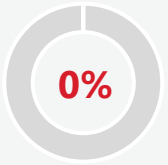
How much do you value your MDR / MSSP having a sophisticated threat intelligence & research arm?



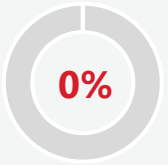
Critical
Key Decision Factor



Important
Not Critical



Somewhat Important
Nice to Have



Not Important
Other Factors Matter

Insights | Likelihood of Recommending

The majority of customers voiced positive feedback on Red Canary's core MDR offering citing detection accuracy and low false -positive rates as a basis for recommending the platform to other organizations (9.0). The combination of automated detection and human expertise receives consistent praise, with many customers noting significant improvements over previous security solutions. While there was some negative feedback from smaller organizations on service quality inconsistencies and pricing, mid-market organizations with moderate security maturity tend to have the easiest time extracting value from the platform.

How likely are you to recommend your vendor to another business looking for a MDR / MSSP provider?

red canary	Please elaborate on your 'Likelihood of Recommending' ranking.
10	Red Canary is widely applicable. It's so easy to use regardless of how seasoned your team is. They make it extremely easy to apply processes to incident response, even if your organization has none. **-CISO at Sittadel**
10	I've had a very positive experience and feel we are getting great value for the money. It was easy to onboard, they are inexpensive for what I get, and we've had good results overall. Their CEO sent a "How do we improve" email and responded when feedback was given. I like that we get to take advantage of the threats their customer base has. Their combination of automation and humans really helps me avoid getting BS alerts. Last of all, I really like that I have in-depth visibility into the work they do to analyze events and comment. **-CISO at Second Wave Delivery Systems**
10	We had a very good working relationship. The support is great. The product is working well. They do excellent research. We believe in the direction they are going. **-CISO at Virtual Vaults**
10	We've been very happy with them, customer service continues to excellent and engaged, they continue to improve and expand their threat monitoring and detection capabilities. **-Head of Information Security and Privacy at Ovative Group**
10	Low false positives, dedicated personal to your account, quick to implement and large list of data connectors and integrations. Contribute to security community with numerous free tools, quick to implement new detection rules based off of new threats in the environment. **-Information Security Manager at Nashville Electric Service**
10	Red Canary has been an invaluable tool in our security posture. Their ability to react and catch positive events while containing false positives has been a significant benefit for our district. **-CIO at Columbia County School District**
10	They offer best-in-class endpoint detection and response and are very easy to work with. The detections published are easy to read and respond to. They also offer basic automated responses tailored to the EDR tool. **-Security Engineer at Wide Open West**
10	For other organizations in our industry or size, a partner like Red Canary is a great fit. I have recommended them to other organizations as well as technology partners. **-Head of Technology and Security at VuePoint Diagnostics**
10	Red Canary has been around and they have figured out what works and what doesn't. We trust them which goes a long way in security. They might be a little more expensive than other providers but for us, they are a known commodity. We also like the team they assigned us and our scheduled meetings with them to discuss their analysis. **-Director of IT at Pikes Peak Regional Building Department**
10	It is a solution that is reasonable to implement and the pricing is fair. We have had great success with the events is has notified us of in the last year. I have already recommended this solution to others considering similar platforms. **-CIO at Revere Electric Supply Co.**
9	Because it is great. I gave it a 9 which is the highest possible rating as you need to evaluate your needs to choose a vendor. **-Tech Lead at First Citizens Bank**
9	I like their tech and content. They are cost competitive to other options and have proved to be a good partner. **-IT Director at Dynamic Brands**
9	Because they have a really good threat intelligence research team to enhance their detection capabilities compared to their competitors. **-Director of Information Security at Denver Water**
9	It's a fantastic product and it can scale to large corporations needs. I would highly recommend it to anyone with a robust IT budget. **-Director of IT at Rollie Williams**

red canary	Please elaborate on your 'Likelihood of Recommending' ranking.
9	We are happy with Red Canary having had no known threat go undetected since we onboarded them at our organization. **-Director of Product & Solutions at BCC Collaboration Company**
9	Recommending Red Canary is environment and provider specific. For our size of business and the software stack we run, it is a good fit. For larger or more complex firms, it may not be a good choice. **-Vice President of IT Operations at Kilbourne Group**
9	In addition to the advanced threat detection and automated response capabilities that allows for almost immediate improvement in security posture, the Red Canary team has been great to work with and very responsive. Their threat analysts provide recommendations to help improve our security posture across domains (Cloud, Endpoint, Network). They also continue to expand their ability to ingest data from new sources to furt her expand coverage for threat detection and have taken our input to improve their own processes and technology. **-Global Director, Cybersecurity Services & Engineering at Bridgestone**
8	Red Canary's expertise in this area is really good. They present the data in a way that even the most untrained eye can pick up what is going on. **-Vice President, Technology Security, Risk & Compliance at FTI Consulting**
8	The quality of the service has been lackluster lately and I am looking at alternative options for 2025. The initial onboarding team and the current support team are not of the same caliber. **-CISO at Wash**
8	Price competitive, great interoperability with my Microsoft environment, easy implementation and high -quality service. Having worked with another MDR provider I Red Canary is a night and day difference service. I'm no longer worried about missing threats. **-Vice President of IT & Security at Allucent**
8	Sales team needs to be more involved and follow up with customers making sure they are getting the best of their product. Several things were disabled from the beginning that we caught. **-CIO at Rushmore Electric Power Coop**
8	They are much improved over our prior provider but some gaps still exist. Threat intelligence and dark web monitoring cannot be offered and we are still more involved in remediation that we had hoped - not 24/7 hands off monitoring. **-CTO at Sun Auto**
8	Red Canary is good at delivering their core offering, but their narrow scope of services can be limiting factor for many use cases. **-Director of Cybersecurity at Mercer International**
8	If your environment has the ability to integrate the logs of the supported applications into Red Canary then there is a lot o f value to utilizing Red Canary. If the various applications you manage aren't able to be integrated, manually parsing and trying to build playbooks on Red Canary can be challenging**. -Head of Cybersecurity at PGA TOUR**
6	Pricing is very, very high, but then again, they were first to market and have a great reputation. But if I can find another MDR/SOC for 1/3rd of the price, I will jump ship. There are a lot of options out there these days. It is a good product, but very expensive even for state / lo cal government customers. **-CIO at Southern Arkansas University**

CROWDSTRIKE	Please elaborate on your 'Likelihood of Recommending' ranking.
10	CrowdStrike is the Cadillac of EDR/MDR solutions. They are extremely responsive, and the platform tools are intuitive and very functional. **-CIO at Independent Living Systems**
10	Unless you have a fully staffed 24/7 internal SOC (i.e. much larger security budget), you need a partner like CrowdStrike to provide that 24/7 protection and can not only protect but remediate and even disconnect a device from the network if necessary. **-CIO at Outreach Health Services**
10	They deliver on what we need. Has the full package and is hands off. We also secured a very good deal for a long-term commitment. We are not looking to change anytime soon. **-CTO at Alliance Ground International**
10	CrowdStrike is a complete solution that takes work away from internal teams and allows us to focus on other areas. Other solutions tend to give you work; meaning that they alert you but do very little to prevent or stop an attack without internal intervention. **-CISO at Constellis**
9	For overall value and effectiveness, it is hard to beat. Despite the challenges of earlier this year, with the breach, their ability to detect and stop threats remains top notch. **-CISO at Owens & Minor**
9	They've saved our butts several times. They are easy to work with and they have engaged staff that are helpful. Only thing I don't like about them is price but maybe you get what you pay for. **-CTO at Florida State University**
9	CrowdStrike is doing an amazing job for us right now and I would recommend them to anyone. CrowdStrike needs to continue with R&D to ensure they stay on top! **-CIO at Marian University**
8	If an organization is already using CrowdStrike tools for endpoint & threat detection, there would be no better choice for a managed detection service as they know their solutions and potential threats the best. **-Deputy CIO at Oppenheimer & Co. Inc.**
8	For large enterprises that have a very strong offering. **-CIO at Région Ile de France**
7	Pricing is too high. They are arrogant, which caused their global outage. They need to understand that the customers are key, not themselves. **-CTO at Commercial Tool Group**
7	Great service, responsiveness and work as a trusted partner. They are key to our operations and have improved our service offering and capability in the security team. **-CIO at Gallagher Bassett**

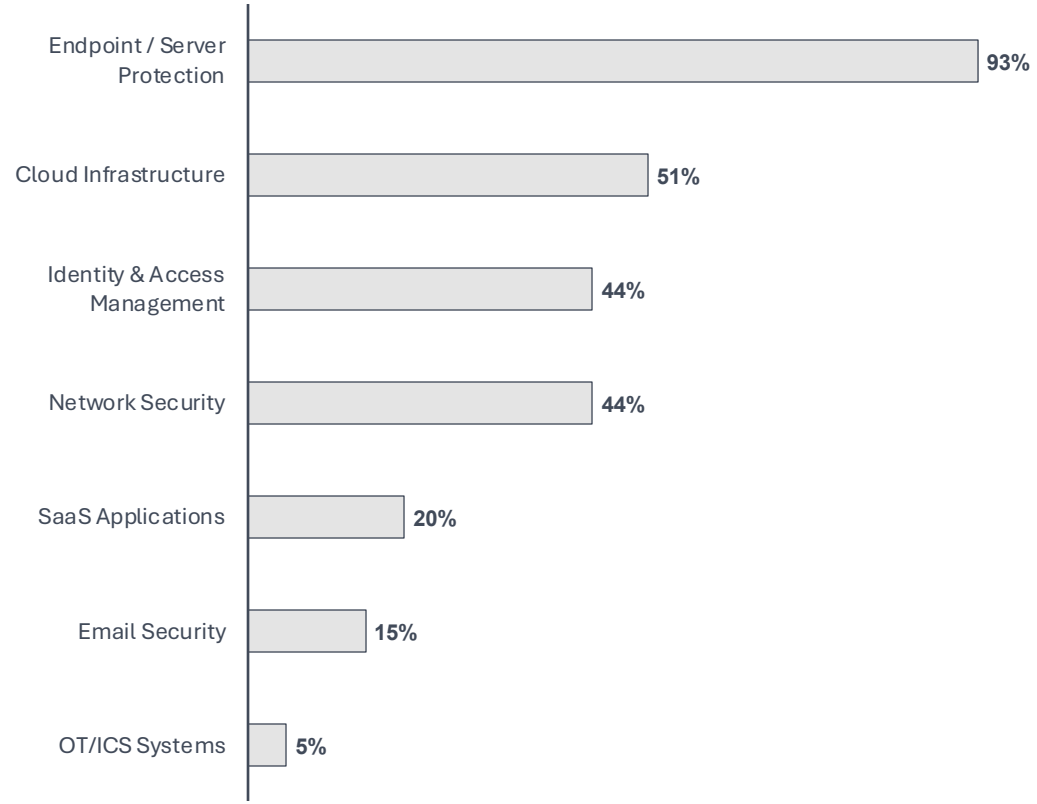
Microsoft Defender	Please elaborate on your 'Likelihood of Recommending' ranking.
9	The solution is priced right, has many robust features, is extremely accurate and overall we are familiar with the Microsoft ecosystem. **-CIO at Spitzer Autoworld**
8	Satisfied with the features, pricing, quality and service delivery. Compatibility and integration within complex global busin ess environments. **-CISO at GlobalSign**
7	They provide the service that we need. I would recommend them but at the same time I would encourage any organisation to complete their own due diligence before they choose a product. One product does not suit all. **-CIO at Dementia Australia**
7	Well, it really depends on the coverage they want and how much they are willing to spend. It is also better to have tools fro m Microsoft as they work better together. **-CTO at Immunotec**
6	Still comparing the Microsoft offering alongside the current time-tested Sophos MDR offering. Jury is still out on whether or not the Microsoft offering can show value and stay in our stack outside the one year demo period we have contracted. **-CIO at Peloton Consulting Group**

SentinelOne	Please elaborate on your 'Likelihood of Recommending' ranking.
9	They have been a great partner and have helped transform an area that was of great concern to the board. They have a good lev el of interaction with our business so more socially engineered threats are also being spotted. **-CIO at Trafalgar Entertainment Group**
9	SentinelOne Vigilance provides a solid basis to protect organization's assets. The service is partly automated, which relieves the securi ty team. **-CISO at Den Helder**
8	Very thorough, ots of telemetry - but sometimes can be difficult to manage the tools in advanced / anamolous situations (e.g. if ELAM is corrupted). **-IT Manager at BMT Tax Depreciation**

Insights | Coverage Trends By Detection Surface

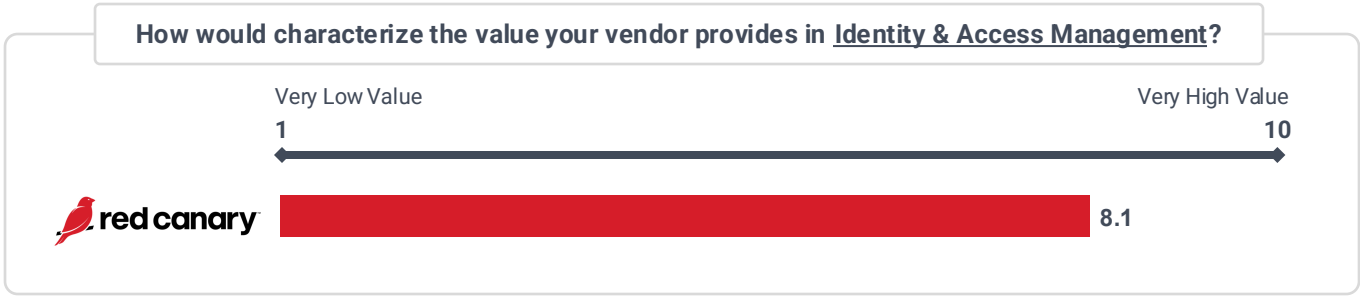
Most Covered Detection Surfaces	01	02	03
	Endpoint / Server Protection	Cloud Infrastructure	Identity & Access Management

Which detection surfaces is your vendor covering with their detection & response services?



red canary — Customer Responses Only

Detection Surface(s) Covered	
Endpoint / Server Protection	100%
Cloud Infrastructure	60%
Identity & Access Management	52%
Network Security	36%
SaaS Applications	20%
Email Security	12%
OT/ICS Systems	0%

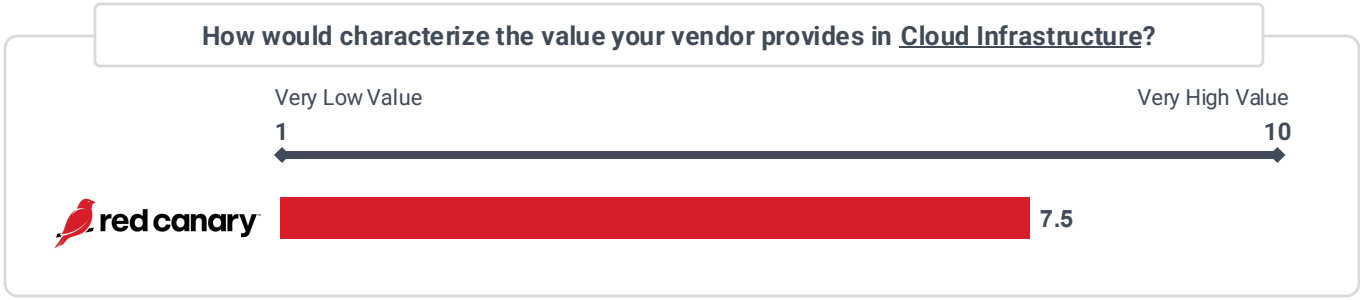


Why aren't you using Red Canary to protect your identity detection surfaces? Do you see a scenario where you leverage Red Canary for these purposes in the future?
We have Okta for said purpose and have a long-term contract with them. **-Tech Lead at First Citizens Bank**
We use Microsoft Active Directory on our own AD Servers, Red Canary does not offer identity detection for this. **-Vice President, Technology Security, Risk & Compliance at FTI Consulting**
We're handling this responsibility internally with our Microsoft Security team. We don't see an immediate opportunity to move this to Red Canary, but it has our interest. Moving identity logs to Red Canary will almost certainly be done in tandem with cloud. **-CISO at Sittadel**
Utilizing multiple products across detection surfaces provides a much better solution. Putting the proverbial "all your eggs in one basket" limits detection. **-CIO at Columbia County School District**
We have a solid set of conditional access policies that are built into our E5 tenant with Microsoft Entra ID. **-CISO at Wash**
This is simply a matter of budget and cost. Should more money be available in the future, we may leverage them. **-Security Engineer at Wide Open West**
Yes, that would require looking at Active Directory (AD) logs and there would need to be more software involved. **-CIO at Rushmore Electric Power Coop**
Cost. We simply cannot afford additional modules after the expense of endpoints. **-CIO at Southern Arkansas University**
Not all of our users have E3 licenses that are required to enable this feature. I do see us moving to all E3 licenses to enable this feature. We had this feature for the first year of the deployment until the upgrade to the Graph integration nullified this feature. **-Director of IT at Rollie Williams**
Already part of Microsoft's Active Directory offering, so we did not see value in replacing. **-CTO at Sun Auto**
Haven't had time to configure this yet, but will be doing so shortly. **-Director of Product & Solutions at BCC Collaboration Company**
We chose Microsoft for this as it is very easy to do using Office. So convenience was a factor in this decision. Plus, the offering from Microsoft works for us. At this time, I don't see a scenario that would make us switch to Red Canary. **-Director of IT at Pikes Peak Regional Building Department**

	**Why aren't you using your vendor to protect your identity detection surfaces? Do you see a scenario where you leverage your vendor for these purposes in the future?**
We are currently using other tools of IAM/PAM. We would be open to leveraging CrowdStrike in the future.	**-Deputy CIO at Oppenheimer & Co. Inc.**
Because we have 4 other vendors on these fields. They cover IAM, PAM and IGA.	**-CIO at Région Ile de France**
We are using both CrowdStrike and Intermedia to do identity detection.	**-CTO at Commercial Tool Group**
We had other tools in place for IAM. There might be a time we move CS Complete to Identity but not now.	**-CIO at Marian University**
We manage this in-house. There are no plans to outsource this to a partner/3rd party.	**-CIO at Gallagher Bassett**

	**Why aren't you using your vendor to protect your identity detection surfaces? Do you see a scenario where you leverage your vendor for these purposes in the future?**
At the moment we are happy with our setup and how we manage it. We didnt have the funding to include all parts.	**-CIO at Dementia Australia**
We use the built in protections with Azure AD, which requires MFA through the Outlook Mobile app. I don't see a need in the future to switch.	**-CTO at Immunotec**

	**Why aren't you using your vendor to protect your identity detection surfaces? Do you see a scenario where you leverage your vendor for these purposes in the future?**
We will look to include this in the future. We are currently seeing out an existing contract.	**-CIO at Trafalgar Entertainment Group**



Why aren't you using Red Canary to protect your cloud detection surfaces? Do you see a scenario where you leverage Red Canary for these purposes in the future?
We use Microsoft Defender for Cloud for that. This has been recommended to us by several parties as being the best solution. **-CISO at Virtual Vaults**
We have not rolled this out for Red Canary and AWS as of yet. **-Vice President, Technology Security, Risk & Compliance at FTI Consulting**
We just built out our Microsoft operations before Red Canary added those skus in. **-CISO at Sittadel**
Our environment utilizes a separate cloud detection product. Would we migrate to Red Canary for Cloud Detection? At this time no. **-CIO at Columbia County School District**
We are using Red Canary to protect our Windows servers that are using Microsoft Defender. **-CISO at Wash**
We currently have a different product filling that role. I do see them potentially offering that in the future. **-Security Engineer at Wide Open West**
We do not have any cloud infrastructure. **-CIO at Southern Arkansas University**
Not all of our users have E3 licenses that are required to reenable this feature. We had this for the first year until the Graph integration upgrade disabled it. **-Director of IT at Rollie Williams**
Using Native Azure tools and did not see value in replacing them. **-CTO at Sun Auto**
We do not host our own cloud applications - this is all handled via identity to our SAAS platforms. **-Vice President of IT Operations at Kilbourne Group**

CROWDSTRIKE	Why aren't you using your vendor to protect your cloud detection surfaces? Do you see a scenario where you leverage your vendor for these purposes in the future?
	We are currently using our cloud provider's best of breed cloud detection services. We would be open to investigating using CrowdStrike in the future. **-Deputy CIO at Oppenheimer & Co. Inc.**
	Currently we are leveraging Defender for Cloud and Azure protection services. I do not think CrowdStrike has a product offering that can "currently" outperform Microsoft native tools. That could change in the future. **-CIO at Outreach Health Services**
	Not much to protect at this time. There could be a scenario in the future to help protect our cloud systems but right now we rely on the SaaS providers. **-CTO at Alliance Ground International**
	Right now it's a measured roll out plan. We will probably roll out more features such as cloud as we get budgets aligned. There is no technical reason we aren't using it. **-CTO at Florida State University**
	We don't use the cloud today but it's possible we leverage CrowdStrike's services when we do transition to the cloud. **-CTO at Commercial Tool Group**
	We manage this in-house. There are no plans to outsource this to a partner/3rd party. **-CIO at Gallagher Bassett**

Microsoft Defender	Why aren't you using your vendor to protect your cloud detection surfaces? Do you see a scenario where you leverage your vendor for these purposes in the future?
	Part of the MS ecosystem and solid reviews/results so it made sense. We also needed additional protection. **-CIO at Spitzer Autoworld**
	We do not have a large footprint in Azure. We have a large footprint in Oracle OCI and use their security services. **-CIO at Peloton Consulting Group**

Insights | Vendor Benefits

Red Canary delivers substantial value through effective security team augmentation, particularly benefiting organizations with limited internal security resources. Customers consistently highlight the combination of reduced workload and enhanced security capabilities, with many noting the ability to reallocate internal resources to strategic initiatives rather than alert investigation. The service provides multiple layers of value beyond basic MDR functionality, including security education, strategic guidance, and access to security expertise.

red canary	What benefits have you experienced from leveraging the specialized skills and expertise of Red Canary?
	Even though they are a generic service to some extent, they do provide high-touch service. With Red Canary, I'm able to get the benefits of a larger MSSP but with less human error. It has been very positive. We are small, limited staff. This onboarding was easy and gives me metrics to show how well we are protected. **-CISO at Second Wave Delivery Systems**
	Asking them all kind of questions related to security products, tooling and best practices. **-CISO at Virtual Vaults**
	Better monitoring, complete triage and analysis, more internal resource availability. **-Head of Information Security and Privacy at Ovative Group**
	It has helped reduce security headaches and threat detection with long term security planning made easy. **-Tech Lead at First Citizens Bank**
	Their analyses are very responsive and easy to work with. **-Vice President, Technology Security, Risk & Compliance at FTI Consulting**
	We have had zero significant incidents and require very little time to investigate incidents. **-IT Director at Dynamic Brands**
	We particularly appreciate the work of Jeff Felling, who publishes the Monthly Intelligence Insights. These are continual proof-of-value reports and keep our team abreast of prevalent threats. **-CISO at Sittadel**
	Our on-site security staff has been able to focus on more strategic products, versus investigating alerts all day long which are non-critical. **-Information Security Manager at Nashville Electric Service**
	Having limited personnel to focus on security should be a concern for any IT environment. Red Canary augments internal security knowledge and management and provides insights often overlooks by the limited personnel on hand. **-CIO at Columbia County School District**
	The benefit is their threat intelligence data can provide deeper and richer identification of more sophisticated attacks. **-Director of Information Security at Denver Water**
	The major benefit has been the fact that I do not have to hire in-house staff. **-CISO at Wash**
	They have been able to educate us on best practices and a good focus on automating play books. **-Vice President of IT & Security at Allucent**
	Extended detection and response as well as technical expertise in incidents. **-Security Engineer at Wide Open West**
	Learned more about their research and how they get their information. **-CIO at Rushmore Electric Power Coop**
	Time savings digging into potential incidents and classifying them. Stress savings due to having a knowledgeable cybersecurity person to explain it all. **-CIO at Southern Arkansas University**

red canary	What benefits have you experienced from leveraging the specialized skills and expertise of Red Canary?
	The biggest benefit is our improved security posture and peace of mind. We benefit from the research scientists that Red Canary employs to improve the detection and remediation process. I have access to the best security minds in the business via my Red Canary portal. They are very helpful and always willing to assist with playbooks and general security questions. **-Director of IT at Rollie Williams**
	They are a big help in automation of our responses to a detected threat. **-CTO at Sun Auto**
	Enhanced configuration of our Microsoft Security tenant. **-Vice President of IT Operations at Kilbourne Group**
	24/7 coverage, improved time to respond, better elimination of false positives. **-Director of Cybersecurity at Mercer International**
	The access to connect with analysts directly has been very beneficial. When we have confirmed threat detections we can get a direct breakdown from an analyst as well as recommended actions for our internal teams to take. **-Global Director, Cybersecurity Services & Engineering at Bridgestone**
	They have been able to not only offer configuration advice but also general threat knowledge. **-Director of Product & Solutions at BCC Collaboration Company**
	Reduction in false positives and faster remediation times. **-Head of Cybersecurity at PGA TOUR**
	We have tightened some of our controls at the recommendations of Red Canary. **-Head of Technology and Security at VuePoint Diagnostics**
	They have become the security experts I don't have in house. For me, that means one less area to manage and worry about. Another benefit is the education they give us on what areas to focus on and recommendations to fix. **-Director of IT at Pikes Peak Regional Building Department**
	The key for me is identifying a concern, but providing the action to prevent further issues or make recommendations depending on the severity of the issue has been critical for us. Using them has also provide additional tools and educational opportunities to build our security experience which helps as the environment continues to be challenging. **-CIO at Revere Electric Supply Co.**

CROWDSTRIKE	What benefits have you experienced from leveraging the specialized skills and expertise of your vendor?
	They are the foremost experts in the field and will work with us to improve the environment. We've identified opportunities t o eliminate other utilities that have overlapping services. **-CIO at Independent Living Systems**
	Great analysts/experts. They have provided great guidance to my more junior level in-house analysts. **-CISO at Owens & Minor**
	Our network, cyber & incident response teams have learned a tremendous amount from our CrowdStrike team on identifying and me diating threats quickly and have become very knowledgeable on the CrowdStrike tools we have deployed through this collaboration. **-Deputy CIO at Oppenheimer & Co. Inc.**
	Capacity as well as the training they provide to our teams. **-CIO at Région Ile de France**
	Just the overall awareness of attacks on our endpoints but also the expertise they provide as they monitor larger threat acto rs and how they are evolving their attack strategies. They conduct multiple webinars and knowledge base articles based on these larger actors. **-CIO at Outreach Health Services**
	Excellent experience and we used them to help us understand items and to complete table tops exercises. **-CTO at Alliance Ground International**
	If there is an attack that requests internal intervention, CrowdStrike provides all the information they have on the case upfront and provide remediation recommendations as part of that communication. They are also on standby to assist further if needed. **-CISO at Constellis**
	We have two major incidents averted in the last year and many minor ones. We feel our protection level is higher now. **-CTO at Florida State University**
	Frankly we don't use them. They are there for an insurance policy. Maybe we could utilize them for more but today I don't have the time. **-CTO at Commercial Tool Group**
	They work side-by-side with my team and are an extension of my team, not just another vendor. **-CIO at Marian University**
	Toolset, maturity, processes and capability. **-CIO at Gallagher Bassett**

Microsoft Defender	What benefits have you experienced from leveraging the specialized skills and expertise of your vendor?
	Extremely accurate results. Around the clock coverage that we did not have prior. **-CIO at Spitzer Autoworld**
	Expanded coverage of security detection and visibility on assets and events. Improved response and reduction of false positiv es. **-CISO at GlobalSign**
	We are liking some of security reports and overall communications from MS for being part of the program. Since we mostly have windows-based endpoints, we are seeing a little stronger of a knowledge base from Microsoft on their own operating system than from Sophos. **-CIO at Peloton Consulting Group**
	They have larger teams and more extensive knowledge than we could have in-house. We are able to tap into their knowledge and shape our strategies in a way that would be more challenging in-house. **-CIO at Dementia Australia**
	I don't have to hire overpriced full-time consultants. **-CTO at Immunotec**

SentinelOne	What benefits have you experienced from leveraging the specialized skills and expertise of your vendor?
	Better security engagement across the wider business. **-CIO at Trafalgar Entertainment Group**
	They provide detailed advice and information about the risks on our environment. **-IT Manager at BMT Tax Depreciation**
	SentinelOne has a huge staff with extensive knowledge that would be possible to hire for a mid-size organization. By leveraging the specialised skills and expertise we could grow our security posture. **-CISO at Den Helder**

Insights | Feature Requests

Red Canary customer feedback reveals several key areas for potential product enhancements, including: (1) broader integration support across network security tools, cloud services (particularly AWS and Azure), and identity management systems (2) enhanced log management capabilities (3) an expansion beyond pure MDR into broader security advisory services, including proactive security posture reviews and threat intelligence sharing (4) reporting improvements and dashboard customization capabilities.

What else would you like to see from Red Canary? Whether it be additional expertise, additional features/modules, etc.
KnowBe4 phish alert analysis vs. just log retention. **-CISO at Second Wave Delivery Systems**
To further expand their identity monitoring. **-CISO at Virtual Vaults**
Add SAAS monitoring for sensitive apps, integrate network logging into collection/analysis. **-Head of Information Security and Privacy at Ovative Group**
I would like to see more ways to intake data to provide additional intelligence and insight into the whole picture. **-Vice President, Technology Security, Risk & Compliance at FTI Consulting**
I would like to see more correlation on identity for cloud (M365) vs on-prem (AD) and explore replacing S1 with Defender. **-IT Director at Dynamic Brands**
Red Canary provides so much expertise in the way of reports, webinars, and events, but none of it can be applied to our team's CPE/CEU requirements. This is a small point of frustration, because it really is one of the largest contributors to several team members' training. **-CISO at Sittadel**
I would like to see more integration with network security ingestions (firewall logs as an example). I would also like to see a tool to store security log data that we are sending to them so we can query later. This would prevent the need for us to pay for a SIEM in most cases. **-Information Security Manager at Nashville Electric Service**
"If something works, don't change it". Red Canary provides our environment with what we need. Every IT environment is different and unique, so it's difficult to say what other features we would like from this vendor. **-CIO at Columbia County School District**
Their incident response services can be a game changer in helping my team to get more ready during an incident. **-Director of Information Security at Denver Water**
A better portal. There needs to be additional data feeds that other providers provide (ReliaQuest) **-CISO at Wash**
A broader discussion about general security threats and where they believe we may have blind spots even if they don't provide a technical solution. I want a general security partner. **-Vice President of IT & Security at Allucent**
Nothing comes to mind, but we are not currently leveraging Red Canary's full catalog, so it is hard to think past that. **-Security Engineer at Wide Open West**
More integration with other network security such as SPAN monitoring. **-CIO at Rushmore Electric Power Coop**
Significantly reduced pricing for public sector customers. **-CIO at Southern Arkansas University**

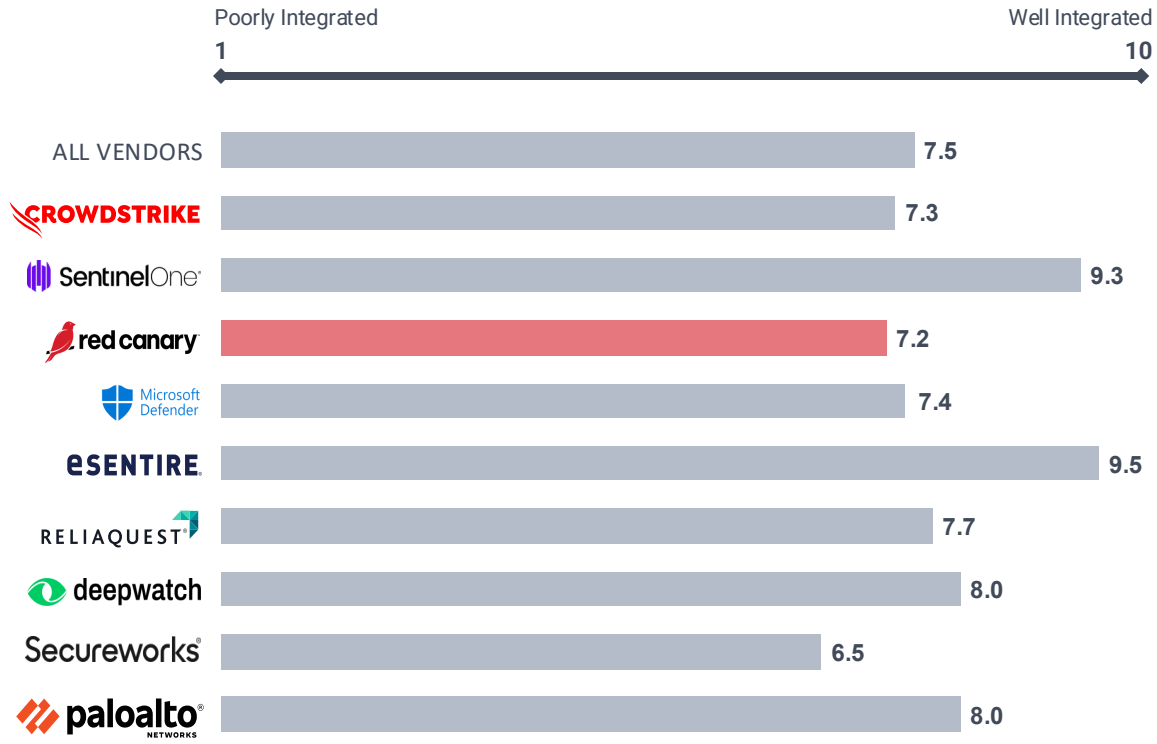
What else would you like to see from Red Canary? Whether it be additional expertise, additional features/modules, etc.
While we are almost a $200M company we are not very large and Red Canary caters to larger companies. It would be nice to have more focus on the 200 endpoint space. I would also like to see more integration options. **-Director of IT at Rollie Williams**
Tell us how we can use their tools across other areas to reduce costs and/or provide second level of protection. **-CTO at Sun Auto**
Deeper configuration and automation assistance with the Microsoft security suite. **-Vice President of IT Operations at Kilbourne Group**
Proactive services, such as security posture review, vulnerability management, simulated attacks can significantly improve Re d Canary's portfolio. **-Director of Cybersecurity at Mercer International**
I would like to see continued improvement in the cloud detection capabilities (AWS and Azure). I'd also like to see integrati on with network solutions, which is limited today. I'm would also like better reporting from their threat intelligence both specific to what they see within our environment, but also across their customer base. **-Global Director, Cybersecurity Services & Engineering at Bridgestone**
I would like to see more knowledge sharing on a more regular basis to encourage customers of their superiority. **-Director of Product & Solutions at BCC Collaboration Company**
Better integrations with some applications, some of this is challenging just because of what's possible to pull out of the ap plications, but many still don't have built in detection rules 2+ years later. **-Head of Cybersecurity at PGA TOUR**
More customizable parsers and integrations with 3rd-party systems. The syslog ingestion is limited as they can only retain and search the logs, not act on them**. -Head of Technology and Security at VuePoint Diagnostics**
As with most vendors, improvements to the dashboard. It is good and has come a long way, but I would like it to be more configurable for my needs. Other than that, they provide a good sound service that meets our needs. -**Director of IT at Pikes Peak Regional Building Department**
I would like to see them enable us to better integrate additional logs and thus provide more coverage for our environment. Th ey seem to struggle with post sales follow up which is not uncommon. I need to continue to review and bridge gaps we discover in our environment. I am hoping tha t Red Canary can be a partner to assist us in those efforts. **-CIO at Revere Electric Supply Co.**

CROWDSTRIKE	What else would you like to see from your vendor? Whether it be additional expertise, additional features/modules, etc.
	I think that if there was a honeypot offering that could include the ability to sandbox items it would be helpful. **-CIO at Independent Living Systems**
	Incorporate AI in the future. Ideally, the majority of everything CrowdStrike does should be run by a top-notch AI model. **-CISO at Owens & Minor**
	We are extremely pleased with CrowdStrike. If they do offer IAM/PAM and cloud solutions that integrate seamlessly with the to ols we use, that would be something we'd be interested in investigating. **-Deputy CIO at Oppenheimer & Co. Inc.**
	More Gen AI features in terms of knowledge management, automation and detection of weak signals. **-CIO at Région Ile de France**
	Email security and secure web gateway could be two strong areas where they could leverage their overall security model (eithe r through net new development or acquiring an industry leader in that space). **-CIO at Outreach Health Services**
	I would like to have them look into a complete solution for email which I don't think they have such a tool at this time. **-CTO at Alliance Ground International**
	I would like to see Falcon for IT expand in there management of IT related functions that have an impact on security. Their p atching module is a great start but there can be more in terms of configuration management similar to an MDM. **-CISO at Constellis**
	Not sure here. If we were attacked we would use them to remediate. We get briefings from them on the threat landscape. We've been to their annual conference twice which is very valuable. **-CTO at Florida State University**
	I used to get fruitful and actionable reports from OpenSystems with my previous company. I don't see this from CrowdStrike, I'm sure it exists, but I have to chase it down rather than it coming to me more naturally. They should be contacting me with actual threat vectors daily. They should b e as they have access to the system suggesting update/upgrades. **-CTO at Commercial Tool Group**
	I would like to see them have quarterly releases that expand their solutions and SEIM. I really need to ensure we're getting the best out of our yearly costs! **-CIO at Marian University**

Microsoft Defender	What else would you like to see from your vendor? Whether it be additional expertise, additional features/modules, etc.
	More expertise in third-party cloud components e.g. Salesforce, Atlassian. Improved integration with their own Github.com product when it comes to SAST. **-CISO at GlobalSign**
	I would like to see better coverage and analysis on non-windows platforms. **-CIO at Peloton Consulting Group**
	Future roadmaps is an important one for me. The threat landscape is constantly evolving and it will be important for any tech company to keep up with the improvements in threat tech. **-CIO at Dementia Australia**

SentinelOne	What else would you like to see from your vendor? Whether it be additional expertise, additional features/modules, etc.
	Deeper integration into our app stack. **-CIO at Trafalgar Entertainment Group**
	Perhaps more pro-active guidance on things we could be doing better. **-IT Manager at BMT Tax Depreciation**
	The only thing I could think is a bit more one on one advice how to improve our security posture by changing procedures or the way we work. **-CISO at Den Helder**

How well integrated is your vendor with your other security tools in terms of ensuring complete threat coverage?



Does your vendor take response or remediation actions for you?

	All Vendors	red canary
NO	84%	76%
YES	16%	24%

What advantages have you noticed from having independent security tools working together to enhance security?
I like being able to integrate many tools into one monitored platform to choose the EDR and identity tools that fit our company size, budget and needs. **-IT Director at Dynamic Brands**
Because we are a cybersecurity company and the reputation damage we would receive from an unmitigated cybersecurity incident would be crippling for our growth. For that reason, we appreciate the way independent security tools escalate to our internal cybersecurity operations. We own the decisions required to determine the scope of an incident, and leadership is confident that we are never asleep at the wheel, because there is no expectation that tool harmony or services will take care of it on our behalf. This is a more expensive and less efficient operation that keeps our incident response processes sharp, practiced, and complete. **-CISO at Sittadel**
The ability for all authentication logs (Okta, Entra) and Endpoint logs to be aggregated together in one place for threat identification. This isn to possible without an independent system or SIEM. **-Information Security Manager at Nashville Electric Service**
Automation between systems is very important. Having a SANS trained staff member in understanding integration techniques and who can write code to assist in these integrations is critical. **-CIO at Columbia County School District**
It provides better visibility across the enterprise during an incident and a faster enrichment process than if they are not working tougher. **-Director of Information Security at Denver Water**
The main advantage is the ability to use the best of breed instead of a one solution / single dashboard. **-CISO at Wash**
I don't have to do anything in particular to integrate them. Feels like plug and play. **-Vice President of IT & Security at Allucent**
It gives a holistic view and response to threats. It also makes incident response easier. **-Security Engineer at Wide Open West**
Prevents a widespread problem with other endpoints by isolating the device immediately. **-CIO at Rushmore Electric Power Coop**
Correlation between events on different systems. Red Canary does not really integrate with our stack except EDR. Or maybe we just aren't paying for those features. **-CIO at Southern Arkansas University**
It seems no one product has the answer for every aspect of the enterprise so I think having independent security tools working together is a requirement in this day and age of modern IT security. The advantages are having multiple products working together that covers the entire attack surface. Where one tool may be great at a handful of things that same tool may not be great at others. I view the tool stack and a layer approach to having a digital protection cover. **-Director of IT at Rollie Williams**
Don't like having all my security eggs in one basket. Want it to be multiple layers like an onion but not too complex for us to understand, manage or create a poor user experience. **-CTO at Sun Auto**

What advantages have you noticed from having independent security tools working together to enhance security?
Increased visibility of threat analysis, requires a comprehensive configuration that stays aligned in order to operate which creates a strong configuration loop. **-Vice President of IT Operations at Kilbourne Group**
It helps us since we are 100% remote and use 2 cloud infrastructures. I like that there is no agent and it is pretty lightweight overall, but, they will still pick up the phone and call me if needed. I like taking advantage of their Threat Intelligence and alerts from their customer base and TI to increase my posture overall. **-CISO at Second Wave Delivery Systems**
Not much so far. We have a simple security stack. We haven't seen the need to integrate all those in a single glass of pane yet. **-CISO at Virtual Vaults**
Better coverage and redundancy in case one system misses something another vendor catches. **-Head of Information Security and Privacy at Ovative Group**
This has helped us reduce the overall burden on internal teams which can focus on application development. **-Tech Lead at First Citizens Bank**
Getting the best of breed coverage and technology instead of having one large vendor that does a lot of things average. **-Vice President, Technology Security, Risk & Compliance at FTI Consulting**
We have a very diverse computing landscape and it is necessary for us to have many independent security tools based on compatibility. This ensures a broader spectrum of coverage, but also requires the need for some integration point to ensure threats don't go undetected in a standalone portal. If the integration works well it is very beneficial in ensuring the same baseline detection capability across the landscape. **-Global Director, Cybersecurity Services & Engineering at Bridgestone**
This brings a holistic response to threats. All of the tools and engineers working together to protect us. **-Director of Product & Solutions at BCC Collaboration Company**
It allows for customization of the environment to get the right solution based on the need. Most suites do a lot of things ok, but not necessarily great. This can really be seen in the mail protection space where tools like Proofpoint have acquired many solid products but not fully integrated them so management is challenging. **-Head of Cybersecurity at PGA TOUR**
We can select products or tools that best fit our environment and technology stack. **-Head of Technology and Security at VuePoint Diagnostics**
A wider more solid platform that covers our attack surfaces. More isn't necessarily better but being able to integrate specific tools that are best in class allows us to have stronger security. **-Director of IT at Pikes Peak Regional Building Department**
My thoughts are this is a plus as each provider cannot be everything to everyone, so having a smaller number of partners on overwatch seems to be a smart strategy so far. It seems to have worked well for us. The journey continues. **-CIO at Revere Electric Supply Co.**

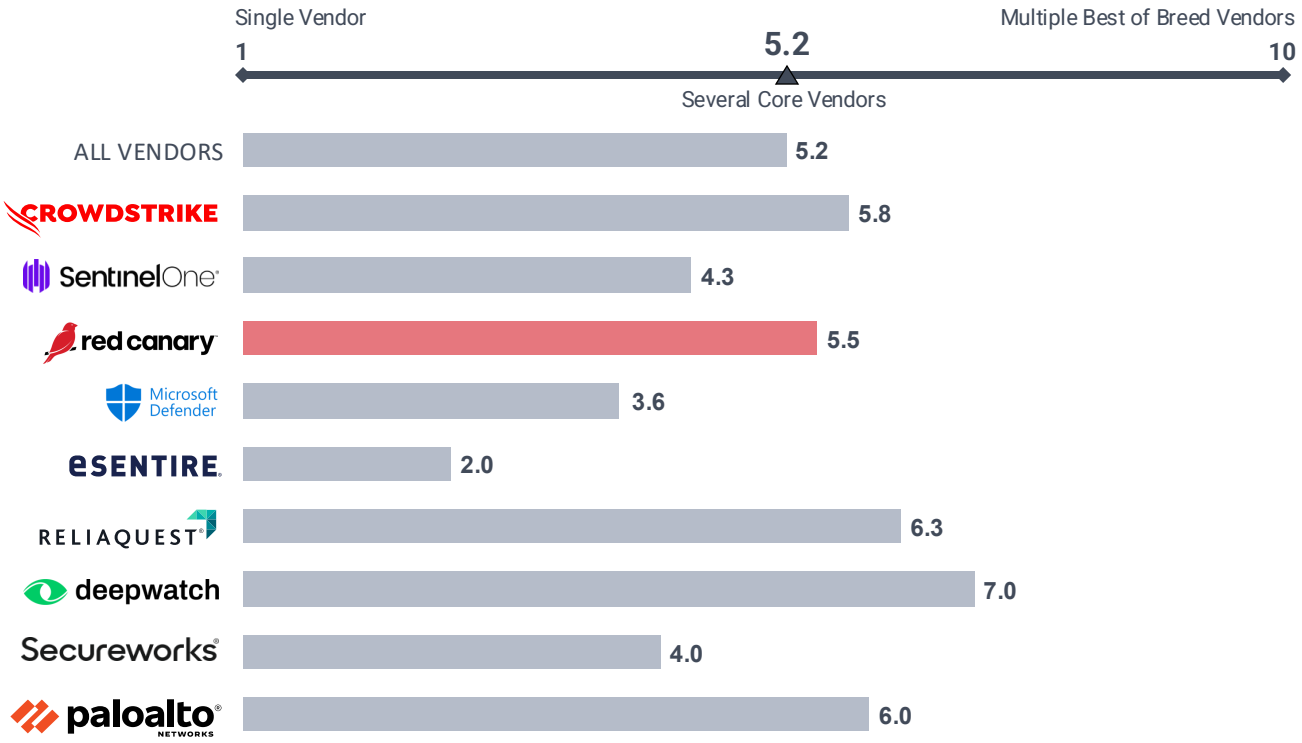
CROWDSTRIKE	What advantages have you noticed from having independent security tools working together to enhance security?
	We leverage the CrowdStrike SIEM to correlate events across a majority of our platforms. This gives us a global view of the environment. **-CIO at Independent Living Systems**
	I can't say there are any major advantages, just no major drawbacks. **-CISO at Owens & Minor**
	We feel that using best of breed tools has provided us better coverage and support, but we do struggle with their integration and just using Splunk as the repository to comb through and connect potential related incidents. **-Deputy CIO at Oppenheimer & Co. Inc.**
	Capacity to scale to different workloads and types of Information systems. **-CIO at Région Ile de France**
	There are still some vendors/areas that are the market leader in their respective spaces. Web security and email secure gateway are two examples. While it would be nice to have them all in one toolset, currently you still need to have them separate for best in class. **-CIO at Outreach Health Services**
	There are areas we need to use other tools and at this time we are not fully integrated but like that we get different tools for different things and helps keep everyone on their toes. **-CTO at Alliance Ground International**
	As much as possible, there is a single place to go to start an investigation. **-CISO at Constellis**
	Not sure we have. There is a constant integration issue. We have Proofpoint and it can somewhat work with CrowdStrike but it doesn't give you much. We see no integration with Rapid 7, etc. I'm not sure there is more value in independent tools other than price. **-CTO at Florida State University**
	Back in the day we used to say the knot in the barn door is what we had to find and secure. Today that's the only part of the door that's actually secured. Today it's more like the whole farm really. You need to have an electric fence, cattle guards, drones, cameras, dogs, cats and a shotgun. There is no one security company that can keep all attack vectors safe, you need to have a grouping of tools as if the hackers compromise you "only" protectio n, you are dead in the water or in my analogy, you just lost a bunch of farm life. **-CTO at Commercial Tool Group**
	It provides a complete security picture and increases our security posture. Having your tools work together is critical! **-CIO at Marian University**
	They work as an extension of our team and seamlessly integrate into our team. Provide 24/7 monitoring and response, with global coverage. **-CIO at Gallagher Bassett**

Microsoft Defender	What advantages have you noticed from having independent security tools working together to enhance security?
	Provides some overlap but certainly addresses gaps that a single solution provides. **-CIO at Spitzer Autoworld**
	Quicker response rate, better investigation capabilities, wider coverage and information aggregations. **-CISO at GlobalSign**
	Having the 24/7 coverage and the ability to interact in real-time with a compromised endpoint has been excellent and provides piece of mind, especially given our global footprint. The integration into the M365 platform has been nice as well so we don't have to learn a new portal. **-CIO at Peloton Consulting Group**
	It provides a faster response to a threat and allows for the detection outside of a single product set. If they are in isolation it slows down the ability to counteract and increases the risk of a threat impact. **-CIO at Dementia Australia**
	Multiple points of review and different ways of looking at things. I do like the holistic approach to having tools tightly in tegrated, but a few on the outside are valuable. **-CTO at Immunotec**

SentinelOne	What advantages have you noticed from having independent security tools working together to enhance security?
	We have a greater sense of coverage across our estate and hopefully less gaps from a single vendor. **-CIO at Trafalgar Entertainment Group**
	We have far greater data and it leads to much more informed decisions, as well as insight into our overall security posture whereas before we were blind. **-IT Manager at BMT Tax Depreciation**
	Having independent security tools working together gives a better coverage and a higher chance to correlate a threat. And one vendor for all security would also be a single point of failure. **-CISO at Den Helder**

Our fieldwork suggests that organizations prefer working with several core security vendors (5.2 on a 10-point scale) rather than consolidating with a single vendor or spreading across multiple best-of-breed solutions. There is a clear correlation with team size and resources with larger organizations with dedicated security teams favoring a best-of-breed approach and prioritizing specialized capabilities over operational simplicity, whereas smaller teams strongly prefer vendor consolidation to manage complexity and resource constraints. There is universal recognition that complete reliance on a single vendor creates dangerous security and operational risks. The emerging consensus appears to be a balanced approach using several core vendors (typically 3-5) that excel in their respective domains, providing sufficient security coverage while maintaining manageable operational complexity. This strategy allows organizations to mitigate single-vendor risk while avoiding the operational overhead of managing too many specialized solutions.

What best describes your preference related to the # of security tools, services, and incident response providers you work with?



	Please elaborate on your 'Security Stack Preference' ranking.
10	Due to the nature of what needs to be protected, the solutions need to be able to detect and address nation state threats. If the tooling can provide faster time to detection and remediation, then it's worth the price. While the complexity may increase due to different applications to manage, there never seems to be a silver bullet solution that is able to solve every problem with a full suite of products. **-Head of Cybersecurity at PGA TOUR**
10	This gives us more confidence in the quality of their solutions. We are looking to get the best security there is. We are willing to trade convenience for that. **-CISO at Virtual Vaults**
10	Each surface identified earlier has specific needs and challenges associated with mitigation and response. For any vendor to believe they are best in breed across all of these would be irresponsible in my honest opinion. Selecting best of breed vendors for each surface and maybe a central monitoring vendor would be ideal. **-CIO at Columbia County School District**
8	I prefer to use a tool that is purpose built and not a single solution that is not in the top 3 tools for its purpose. **-CISO at Wash**
8	Too many vendors makes it too complicated to manage contracts, but having more eyes on all levels of your security enhances your security posture significantly. If one doesn't catch it, the others will. **-CIO at Rushmore Electric Power Coop**
7	Never put all your eggs in one basket as it will introduce single point of failure which is the policy we abide by. **-Tech Lead at First Citizens Bank**
7	I prefer to choose a best of breed approach to select tools that fit our company size and budget and needs. **-IT Director at Dynamic Brands**
7	5 = prefer several core vendors to layer the tools and create a multifaceted protection net. No one tool does it all and does it best. In this day and age multiple tools are required for the beast defense. **-Director of IT at Rollie Williams**
6	I prefer multiple best-in-class vendors for sectors of coverage; I don't want to spend the majority of my time managing vendor relationships, but I want my investment going into the most effective vendors I can afford. **-Head of Information Security and Privacy at Ovative Group**
6	I believe it is better to have multiple vendors that excel in their space than one watered down vendor. **-Vice President, Technology Security, Risk & Compliance at FTI Consulting**
6	If you have too many vendors in your stack, you tend to get saturated with trying to learn them all. Their nuances. I prefer less vendors as they are easy to manage. **-Director of IT at Pikes Peak Regional Building Department**
6	I see risk in using a single vendor, plus I am skeptical anyone can be all things to everyone. On the flip side I do not wish to have so many vendors it is a challenge to gain synergy across the infrastructure. Hence my stating I like having a smaller number of vendors to provide better integration across all platforms while limiting the amount of overlap between tools. **-CIO at Revere Electric Supply Co.**
5	I like a balance of looking for the best tooling, while not having tool sprawl. Tool consolidation also helps with budgeting. -**Security Engineer at Wide Open West**
5	Small team. Can't be too complex that we can't manage/understand it or create user disruption. Also cost considerations of best of breed and layering **-CTO at Sun Auto**
5	Our computing landscape would not allow for a single platform provider (although this is a market trend). However, having best of breed in every area is not cost effective and often not necessary for the level of security we are looking for. So our approach is to focus on a few core vendors to cover our environment. **-Global Director, Cybersecurity Services & Engineering at Bridgestone**

Insights | Security Stack Consolidation Preference

	Please elaborate on your 'Security Stack Preference' ranking.
4	No single vendor does a satisfactory job in detecting threats in all parts of the IT landscape. By using "best of breed" approach for detection and prevention capabilities to avoid weak spots in different areas. **-Director of Cybersecurity at Mercer International**
4	We try to consolidate tools where we can for efficiency. I believe the more tools you have, the more that is needed to keep them all working and working together. However, I also do not like to put all of my eggs in one basket. Fore example we could use Entra ID for SSO, however due to the criticality of the services it provides, we have decided to implement Okta as it is a better and more scalable product. **-Information Security Manager at Nashville Electric Service**
4	We would never select a single vendor due to not wanting to have all our eggs in one basket, however, it is important to minimize the number of vendors in use too. **-Director of Product & Solutions at BCC Collaboration Company**
4	While a single vendor is great they do not always serve all of our needs. I prefer a small number of core vendors that focus on their own core strengths. Then having a security platform that lines up well and integrate with those core vendors is the right choice. **-Head of Technology and Security at VuePoint Diagnostics**
3	We are using Radiant Security as well, but only due to the very low cost as we helped them, feedback wise, when they launched. **-CISO at Second Wave Delivery Systems**
3	We prefer to invest heavily in native tools (such as Windows or Microsoft) and tools to cover gaps in the native tools. Because of the way security tools continually expand their features, it is difficult to avoid overlapping features, but we try to fully utilize each tool we work with before acquiring another tool. **-CISO at Sittadel**
3	Consolidation of vendor helps to reduce complexity for us to operate but increased our operational risk due to our heavily reliance on a single vendor. We prefer a few core vendors that can cover each other. **-Director of Information Security at Denver Water**
3	I have a very small team and my ability to manage multiple vendors is very challenging. We don't have the skillsets and required expertise to manage multiple vendors. And the cost would be much higher with a best of breed approach. **-Vice President of IT & Security at Allucent**
3	We would prefer to have a simpler security stack to reduce complexity and cost for our small team. **-Vice President of IT Operations at Kilbourne Group**
1	With a small IT team, simplicity is key. A single pane of glass makes things much easier to manage. I haven't found that silver-bullet vendor yet, but it's a dream to strive for. **-CIO at Southern Arkansas University**

CROWDSTRIKE	Please elaborate on your 'Security Stack Preference' ranking.
9	That was our preferred approach to ensure we have the best tools with the expertise in a limited scope. We are re-thinking that approach due to the lack of integration and difficulty navigating multiple platforms to identify the true problem. **-Deputy CIO at Oppenheimer & Co. Inc.**
8	Until there are vendors that can provide best-in-class coverage / service for multiple security segments, it still makes sense to evaluate them all independently to ensure they can provide superior services. For example, we did move our SIEM solution over to CrowdStrike after evaluating their offering. **-CIO at Outreach Health Services**
8	If your one vendor gets compromised, you are in trouble if they protect your whole stack. **-CTO at Commercial Tool Group**
7	Because it gives us the capacity to have better incident detection and resolution as long as there are APIs between them. **-CIO at Région Ile de France**
5	We do best of breed for a select few solutions that we believe are core to a strong security program like an MDR. We also like to keep a small vendor footprint so that our internal staff are vary effective in managing the solutions that we do have. **-CISO at Constellis**
5	I would like to reduce my technology stack and we're working our way there. However, we need to make sure that the single vendor approach really makes sense. **-CIO at Marian University**
5	We don't want a ton of disparate systems, but we also do not want to be exposed to a singular vendor. **-CISO at Owens & Minor**
4	We prefer a couple of large vendors that cover a lot of space for us in general. We haven't found that at the right price yet in security like we have with database or other areas of it. **-CTO at Florida State University**
2	We don't want too many vendors because in the event of a breach we have to deal with too many vendors pointing the finger at each other. **-CTO at Alliance Ground International**
2	Single point of contact and delivering a wide breadth of services. Easier to manage and for them to take ownership of the end-to-end services. **-CIO at Gallagher Bassett**

Microsoft Defender	Please elaborate on your 'Security Stack Preference' ranking.
6	There is cost benefit of having all your eggs in one basket, but sometimes a vendor's offering may be lacking and you need multiple to get the best of both worlds. It all depends. **-CIO at Spitzer Autoworld**
4	The more vendors the more complex the integration, maintenance and compatibility efforts. Had bad experiences with vendors upgrading and changing their platforms/services and integrations breaking. **-CISO at GlobalSign**
4	I believe that we cannot rely on just one. Look at the CrowdStrike incident recently. A single vendor limits the detection of errors and increases the possibility of downtime. I also believe that a single vendor can have a priority focus that can narrow their field of view. Having several vendors allows for a broader scope. **-CIO at Dementia Australia**
3	Tightly integrated tools means easier management and coordination. It can lead to a savings benefit. **-CTO at Immunotec**
1	I have liked a single vendor approach so far so that everything is easier to train, manage and respond to. With that said, I was really referring to end-point security as we have a different vendors for different areas of the security stack such as Mimecast and Oracle. **-CIO at Peloton Consulting Group**

SentinelOne	Please elaborate on your 'Security Stack Preference' ranking.
6	From experience there are great lessons to be taken from a small number of good partners. It helps to keep everyone focused on the risks and not get complacent. **-CIO at Trafalgar Entertainment Group**
6	As said before, you do not want too much reliability on one vendor, since it is a single point of failure. But too many vendors is an issue as well, since no one wants to read all dashboards and it makes the architecture more complex. **-CISO at Den Helder**
1	I prefer one vendor to help us manage all our tooling because it avoids finger-pointing, having to chase vendors for logs or data, trying to get vendors to work together, etc. Instead one vendor has all the data and is responsible for the entire ticket / environment. **-IT Manager at BMT Tax Depreciation**