Replacing SecureWorks AETD with Red Canary

Not all managed Carbon Black Response solutions are equal. Learn why a customer made the switch from SecureWorks Advanced Endpoint Detection and Response (AETD) to Red Canary Managed Endpoint Detection and Response (MEDR).

CHALLENGE

A SecureWorks customer was unhappy with the quality of the service and needed a partner that could reliably and accurately detect threats.

SOLUTION

Red Canary layered on top of Carbon Black Response giving the firm the detection, response, and support it desired.

BENEFITS

- Broad detection of threats ranging from malware to advanced attacker techniques
- Timely detection, easy-to-understand reporting, and tooling to empower immediate response
- Triage and investigation of each threat resulting in zero false positives to the firm
- Ability to seamlessly integrate alongside other managed solutions

SNAPSHOT

A private investment firm with highly mobile users rolled out SecureWorks AETD to enhance visibility and threat detection across laptops. However, the firm's Director of Technology quickly discovered that the solution did not live up to his expectations. Threats often lingered in the network for days or weeks at a time, leaving endpoints vulnerable. The firm needed a partner that deeply understood endpoint data and would quickly and accurately detect threats.

A TRUE MANAGED ENDPOINT DETECTION & RESPONSE SOLUTION

The Director was convinced that Carbon Black Response was the best Endpoint Detection and Response (EDR) sensor due to its depth of visibility into endpoint activity and robust forensics capabilities. He knew that Red Canary had a strong partnership with Carbon Black and expertise managing the endpoint data it collected.

After deploying Red Canary's MEDR solution, the firm saw an immediate improvement in detection efficiency and response time. Whereas it previously took days or weeks to detect a threat, Red Canary enabled the team to control the situation within minutes to hours, regardless of the endpoint's global location.

"Red Canary has the ability to master the data and detect threats as they happen. We have been able to use their detections to immediately stop threats. We haven't seen the same level of EDR expertise with any other vendor."

— Director of Technology

red canary

MANAGED CARBON BLACK RESPONSE: COMPARING RED CANARY AND SECUREWORKS

	SecureWorks AETD	Red Canary MEDR	Red Canary Value
Carbon Black Server Management	Hosted and managed on premise by the customer	Fully hosted and managed by Red Canary	No need to procure and manage a Carbon Black server
Threat Detection Coverage	Detection uses a subset of SecureWorks Threat Intel Feed to identify threats with known bad indicators	Detection relies primarily on behavioral analysis and anomaly detection	Identifies attackers' patterns and behaviors
Triage & Analysis of Potential Threats	Events are forwarded to the customer, resulting in all triage being handled by customer	Red Canary SOC performs full investigations of every potential threat	No false positives
Alerts / Detection Information	Alerts include indicators and host information and can be very difficult to interpret	Detections include behavior observations, user/endpoint information, and a detailed timeline of how the threat progressed	Quickly understand the threat before making a response decision
Threat Remediation	Customers take detections, investigate the validity, and respond using normal workflow/tools	Customers can remotely isolate endpoints and surgically respond to individual processes, files, and registry modifications. Red Canary is built on an open API and integrates with other security and response tools	Easily integrate detections into a pre-existing workflow and use response tooling to control the threat without IT support
Technical Support	Limited support and frequent difficulties getting an expert to answer questions	Dedicated technical experts with experience in security engineering, analysis, and incident response	Receive dedicated assistance with implementation, trouble-shooting, response, and overall security improvements
Miscellaneous	SecureWorks manages dozens of products and offers many different services, a benefit for organizations that want to work with one vendor	Red Canary is a custom-built Managed EDR solution	Rely on focused expertise that is 100% dedicated to partnering with customers to make their security better
Price	$60/endpoint	$100/endpoint	

red canary

IN THEIR OWN WORDS

A YEAR WITH SECUREWORKS AETD WITH LITTLE TO SHOW FOR IT

"We used SecureWorks' IDS sensors to detect malware and intrusion attempts. I needed visibility across my endpoints and SecureWorks' Managed Carbon Black offering sounded promising. I was excited to get access to advanced endpoint detection without having to build up my team to manage it internally.

Instead we saw that this specific offering from SecureWorks was not effective. We would get notifications days or weeks after an incident. That time frame just wasn't relevant for us. It became obvious that they didn't know how to work with endpoint data. At the end of my contract I started looking for a different managed provider."

EVALUATING RED CANARY MANAGED ENDPOINT DETECTION AND RESPONSE

"I still wanted Carbon Black Response on my endpoints. I just needed to find the right company to manage it. That is when I engaged with Red Canary. A lot of what we discussed when I evaluated them really showed me they were the right choice. For example, they have the same lineage as Carbon Black Response and were Carbon Black's first technology and managed service partner. After an in-depth Proof of Concept, they were able to check all of the boxes I included in my evaluation."

KEY EVALUATION CRITERIA

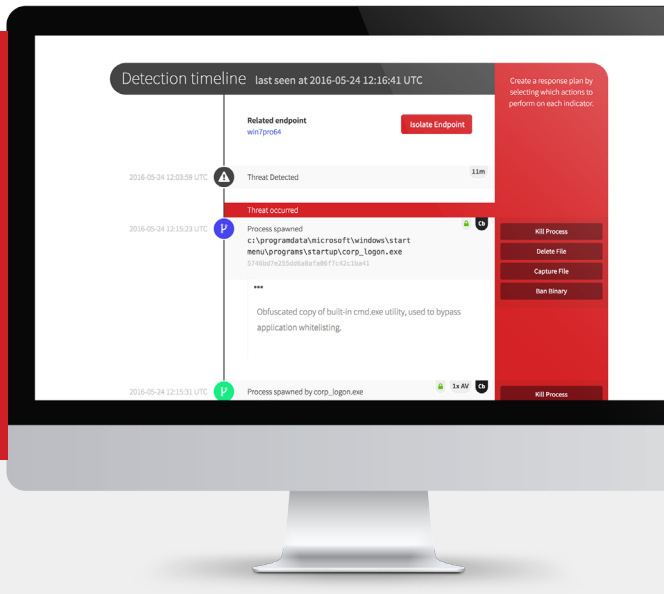
- Proven expertise managing Carbon Black Response
- Advanced threat detection (behaviors and signatures)
- Minimal to no false positives
- Timely detection (within hours)
- Limited involvement required from internal team and existing MSSP
- Ability to integrate detections and endpoint telemetry with other tools and existing MSSP

LIFE WITH RED CANARY

"Red Canary has helped us defend against many different types of threats and give us a level of visibility into endpoint activity that we previously never had. They are a small part of our overall security program, but I can confidently say I am much less concerned about my endpoints getting compromised. Red Canary will continue to be a foundational part of my security program and I am glad I found a partner with true expertise in endpoint security."

About Red Canary

Red Canary helps customers secure their endpoints and stop attacks before they result in breaches. The Managed Endpoint Detection and Response solution quickly and accurately identifies threats on customers' endpoints ranging from compromised credentials to lateral movement to crimeware. Every threat is investigated by a Red Canary Analyst to remove false positives and provide the context required for remediation.



red canary

See how Red Canary can help you secure your endpoints.

855.977.0686 | info@redcanary.com | www.redcanary.com