

Case Study

Cybereason Endpoint Detection & Response



Nick LaPointe

Information Security Administrator at a insurance company with 1,001-5,000 employees

- ✓ Review by a Real User
- ✓ Verified by IT Central Station

What is our primary use case?

We use Cybereason for endpoint detection, response, and protection.

What is most valuable?

All of the features are valuable. I like the managed detection response feature a little bit more than most. We have a small team and it allows us to confidently go on breaks and after-hours leaving the Cybereason team to manage it.

Cybereason absolutely enables us to mitigate and isolate on the fly. Our managed detection response telemetry has dropped dramatically since we began using it. It's very top-of-mind. We were running some tabletop exercises and none of the detections were getting triggered by the managed security services provider. So we

needed to find a solution that would trigger high-fidelity alerts. That was Cybereason and it dramatically changed our landscape from the detection and response perspective.

We evaluated Cybereason based on our junior analysts. We had hands-on keyboard time with them and they provided feedback on use cases that we've given them. Cybereason came out on top as being the easiest to use out of the three solutions that we considered.

The main difference between them was the overall ability to detect the evolving threat in the kill chain was a lot easier to view and alert on for Cybereason. Whereas the others failed to trigger an event anywhere in the kill chain. It had to have a few of the dominoes fall in the kill chain prior to having the event triggered. So it was clear that Cybereason detects threats anywhere within the MITRE ATT&CK framework,



whereas the other ones had to follow a series of events.

Cybereason provides an operation-centric approach to security that enables us to instantly visualize an entire malicious operation from the root cause to every affected endpoint and in real-time. Their overall view within the threat landscape is very easy to understand and visualize. It helps the junior analysts respond and contain to it in a timely manner.

This approach also helped us to move beyond chasing multiple alerts. It came to a point where now we're in an almost set it and forget it stage where it just alerts us and we can direct our attention elsewhere, which is helping the business grow and reach its mission goals.

We have a level up on the attack adversaries with Cybereason due to its nature of detecting malicious user and process behavior analytics. It does a phenomenal job in detecting anomalous behavior on the network and alerting us immediately with the whole story behind it. So it definitely enables us to adapt to attacks and act more swiftly than the attackers can adjust their tactics.

It also leverages indicators of behavior as a means of detecting attacks. Its AI hunting engine does a exceptional job in weeding out the noise and giving us high-fidelity alerts based on indicators of compromise. Which also helps us to detect attacks earlier using this approach. It automates everything.

The time it takes to detect attacks has been reduced through this approach. At least half if

not 60% of our time is not spent on threat hunting anymore. It allowed us to be more business-focused and delivering products and solutions to market quicker for our clients.

Cybereason reduced our detection by 85%. Telemetry and reports are upwards of 90% reduced time.

What needs improvement?

Ad hoc higher-level reporting to senior management could be implemented. That's definitely an area of improvement that they need to focus on.

Their endpoint protection piece for device management and storage device protection could use maturation.

For how long have I used the solution?

I started using Cybereason EDR shortly over a year now. It was March of 2020.

What do I think about the stability of the solution?

The performance was better than the endpoint detection response of our previous solution. We've actually had comments from end-users once we deployed Cybereason, and we noticed the outgoing solution that their computers have increased in speed.



What do I think about the scalability of the solution?

Scalability is endless, especially in a SaaS deployment. We scaled from zero to 2,900 in three weeks, and we saw no degradation in threat hunting query performance within the platform or any ill effects on the platform itself.

It does require maintenance for deploying upgraded sensors and for tweaking policies as new features come out. I don't think that would be maintenance. Upgrading endpoint sensors on mission critical device I recommend a maintenance window just to follow industry best practices, however all other devices can be completed during normal business hours.

How are customer service and technical support?

Their technical support is very competent. They know the product inside and out and they try to understand the business's needs before any solution is provided.

Which solution did I use previously and why did I switch?

Symantec was our previous provider. It was through tabletop exercises that we found that it just wasn't triggering alerts that it should have been, so it led us to review other products.

How was the initial setup?

The setup was completely fast-paced and extremely straightforward.

We were under a somewhat constrained timeline for rollout. It usually takes us six to eight weeks to roll something of this magnitude out to the organization, but having the pandemic upon us, we actually got it fully deployed in under three weeks. That's how easy it was to roll out and deploy.

The deployment was done all internally. It was a little bit more than just our security team. It was help from our tier-one support analyst as well, but we got it rolled out with a handful of people. Six people were involved in the project in deploying over 2,900 sensors.

We are currently looking at their mobile device management solution or their protection solution to expand usage.

What was our ROI?

We will see a positive ROI, I believe, in the next 12 to 24 months.

What's my experience with pricing, setup cost, and licensing?

It's not the cheapest, but it's the best.

There are no additional costs to standard licensing.



What other advice do I have?

My advice would be: Don't hesitate. Pull the trigger and you won't be disappointed.

It's always watching the house. No matter what you throw at it, it will detect anything you give it. It detects anomalies within the environment.

I would rate it an 9.5 out of 10.

Read 5 reviews of Cybereason Endpoint Detection & Response

[See All Reviews](#)