# **Robert Smith**

TO: John Jones, Chief Technology Officer

Alpha Omega Partners

FROM: Robert Smith, IT Team Lead

Alpha Omega Partners

SUBJECT: **Endpoint Detection and Response Solution Options**

**Introduction**

Alpha Omega Partners acquired Beta Beta Solutions in the last week. The acquisition will increase our portfolio of clients and will dramatically expand our sensitive data intake. One of the conditions of the acquisition is the adoption of more focused and comprehensive cybersecurity solutions. Endpoint detection and response (EDR) solutions Without an upgrade to an endpoint detection and response (EDR) solution, we will lose critical clients brought into our portfolio by the acquisition. We will not be able to adequately protect our data assets and will not be able to render detailed insights of threats in our monthly security reports.

**Key Findings**

Our security operations team has reviewed the client requirements and found three EDR solutions that will meet minimal system security requirements. Our most important security criteria are as follows:

* Integration and deployment times need to be minimal to allow for a smooth, post-acquisition transition.
* Competent support from the service provider.
* Regular updates to minimize prolonged downtime.

**EDR Options**

1. **Singularity (SentinelOne)** – The EDR solution from SentinelOne offers great pricing flexibility for a comprehensive set of tools that works well with the Windows OS.

* Users rate all capabilities within .2 points of a perfect score of 5.
* Technical support provides FAQs and How To tutorials.
* 100% cloud-based; runs without internet connectivity on the network.
* User friendly, web-based management console.
* Incident response, including monitoring, analysis, and maintenance, is handled by SentinelOne without any collaborative requirements passed on to the subscriber.

Criticisms center on a few considerations:

* The platform requires updates every few months, contributing to downtime.
* Customer support is hit or miss depending on the responding agent.

1. **Falcon (Crowdstrike)** – The EDR solution from Crowdstrike is another cloud-based platform.

* Includes event recording to provide threat visibility.
* Incident Workbench helps organizations analyze an event.
* Pricing is based on packages with optional add-on features.
* Incident response handling is collaborative and relies on interaction with the subscribing organization.

Criticisms focus on user friendliness:

* Cluttered layout for a web-based management console.
* Multiple menus for operating the platform adds to confusion.

1. **Carbon Black (VMWare)** – The EDR solution from VMWare is a basic but well-praised platform.

* 100% cloud-based.
* Easy to navigate, web-based console.
* Works with Windows, Mac, and Linux OS.
* Investigative features allow for incident response by the subscriber’s own SOC team.

Criticisms:

* Higher pricing per endpoint.
* Pricing is only available through contacting VMWare’s partners.
* Upgrade from the Standard package is necessary for 24-hour phone support.

**Conclusion**

There are many EDR solution options on the market. We reviewed three of the highest rated options, intuiting that many reviews with a higher score would effectively flag quality. We only reviewed solutions that had industry expert reviews. Many of the solutions are cloud-based and offer resilience even when the local network is down. All are compatible with Windows, our only OS. We lack a core SOC team, so solutions with collaborative incident response are not the easiest option though doable. Our team needs a user interface that is easy to operate and monitor and must have customer service at the ready on short notice in the event of an attack. As we report on security matters to our clients, we may need the option to choose additional services that expand the EDR solution’s capabilities.

**Recommendation**

We recommend Singularity by SentinelOne because we need a fast, comprehensive solution that is as hands-free as possible. We recognize that the cybersecurity team at Alpha Omega Partners will expand in the coming years in step with our client growth. This will afford opportunities to self-manage and collaborate on threat mitigation and incident response. At that time, we may revisit our EDR solution service contract and consider a new option instead of renewing. For now, our immediate objectives guided our recommendation:

* **Deployment** – We need a service that guards all endpoints and has a deployment timeline that minimizes disruption of business.
* **Incident response** – Our team is not fully prepared to handle the implications of an attack at current scale. Contracting with a service that provides all incident response steps is critical.
* **Additional services** – Both Singularity and Falcon include expandable options for their monthly service packages. Each additional service adds to the monthly subscription cost but are easy to implement.

While Falcon could be a viable alternative in the future, its interface needs to be redesigned for ease of use. We do not recommend Carbon Black in its current iteration; the solution significantly slows computer performance across the network. Additionally, VMWare only allows sales through partners; not being able to negotiate directly with the owner of the program could signal other difficulties in working with the company.

As the in-house team at Alpha Omega Partners expands, we can consider different options as we acquire new skillsets.

Sources

Cynet. Endpoint Protection and EDR. Cynet, 2021, <https://www.cynet.com/endpoint-protection-and-edr/the-ultimate-rfp-template/>

Gartner. Falcon vs Singularity Platform. Gartner, 2022, <https://www.gartner.com/reviews/market/endpoint-detection-and-response-solutions/compare/product/falcon-vs-singularity-platform>

LDI Connect. Crowdstrike Falcon Vs. SentinelOne Singularity XDR: 3 Differences. LDI Connect, 2022, <https://myldi.com/blog/crowdstrike-falcon-vs-sentinelone-singularity-xdr/>

Crowdstrike. Falcon Insight: Endpoint Detection and Response (EDR). Crowdstrike, 2022, <https://www.crowdstrike.com/products/endpoint-security/falcon-insight-edr/>

The Blueprint. Carbon Black Review. The Motley Fool, 2022, <https://www.fool.com/the-blueprint/carbon-black-review/>