Carbon Black. CB CUSTOMER SPOTLIGHT

Q&A With ALLETE’s Jeff Rotenberger

Featuring Jeff Rotenberger, Cybersecurity Analyst at ALLETE

INDUSTRY

Energy & Utilities

COMPANY SIZE

~2,000 employees

SECURITY CHALLENGES

+Wasted work hours

+Insufficient security tools

PRODUCT

CB Response

KEY BENEFITS

+Faster time to remediation

+Little to no user impact

Tell us about your process for choosing Carbon Black.

We noticed that we were spending an inordinate amount of time dealing with endpoint-related issues. We didn’t have enough tools in the space, and as a result our PC support team was doing a lot of the endpoint remediation and mitigation. The team did not have the proper training or toolset, and in many cases, if an endpoint was compromised, it often meant that the endpoint was boxed up and shipped back to corporate headquarters to be reimaged. That’s a lot of wasted hours – for staff and for the affected employees. After about two years, we saw a demo of Carbon Black and CB Response was the most viable solution for us.

What is the value you’ve seen since using Carbon Black?

After deploying CB Response, we essentially took PC support out of doing any kind of security functions. As a result, we’ve saved hundreds of hours a month that our team was previously dedicating to security-related endpoint issues. Because of Carbon Black’s unique capabilities in Live Response and the use of the API, we could do it all ourselves, and in most cases, without the user being impacted, which was a tremendous win for us.

> *“After deploying CB Response, we essentially took PC support out of doing any kind of security functions. As a result, we’ve saved hundreds of hours a month.”*
>
> *- Jeff Rotenberger, Cybersecurity Analyst*

How has the industry changed since you first started?

It’s been interesting to watch the security evolution here at ALLETE. When I joined, the cybersecurity team was relatively new and relegated to our little corner. Then, we started to do more things, like with Carbon Black, where we became more involved in both the user and endpoint space. I think there’s been a lot more recognition about the importance of both our role and the impact of cyber awareness training. Our training has evolved to the point where we are now conducting presentations and talking to large groups about cybersecurity, which has been really rewarding.

How did the Carbon Black APIs influence your security practice?

When I attended my first CB Connect conference, our team was really invested in Live Response, but we kept hearing about this API. At CB Connect, I watched a presentation by Red Canary on their Surveyor tool, where they ran a Python script against the API and surveyed every single endpoint that had Carbon Black on it for all their different file sharing programs. I realized that this was a problem in our company at the time, and I understood how powerful this API could be and some of the amazing stuff we could do with it. I returned from the conference with all these different ideas, telling my team, “we’re just scratching the surface here with what we can do with this tool.” Since implementing the APIs, we’ve gone from using them as standalone scripts with security automation orchestration (SAO) to using them in conjunction with Resilient.

What’s one piece of advice you would share about a career in cybersecurity?

Never stop learning. Cybersecurity is a very wide space and there’s room for all kinds of people in it. Just keep reading, keep learning, figure out where you fit in that space and go for it. We’ve got a lot of things to tackle in cybersecurity and we need plenty of awesome people to do it.

About Carbon Black

Carbon Black (NASDAQ: CBLK) is a leading provider of next-generation endpoint security delivered via the cloud. Leveraging its big data and analytics cloud platform – the CB Predictive Security Cloud – Carbon Black consolidates prevention, detection, response, threat hunting and managed services into a single platform with a single agent and single console, making it easier for organizations to consolidate security stacks and achieve better protection. As a cybersecurity innovator, Carbon Black has pioneered multiple endpoint security categories, including application control, endpoint detection and response (EDR), and next-generation antivirus (NGAV) enabling customers to defend against the most advanced threats. More than 4,300 global customers, including 35 of the Fortune 100, trust Carbon Black to keep their organizations safe.

Carbon Black.

1100 Winter Street
Waltham, MA 02451 USA
P 617.393.7400 F 617.393.7499
www.carbonblack.com