Q&A with Netflix DVD’s Jimmy Sanders

Featuring Jimmy Sanders, VP of information security at Netflix DVD

Tell us about your process for choosing VMware Carbon Black

Before we had VMware Carbon Black, we were using traditional antivirus (AV). I reviewed various products, developed an evaluation matrix and did a proof of concept with five to six endpoint detection and response (EDR) solutions. Out of everyone we looked at, VMware Carbon Black offered the best value for the DVD division. As a standard, every year, we ensure that we are using the most innovative security products and test for the best of the best. For the past five years, VMware Carbon Black has stood out to be a great solution for DVD.

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

We originally chose VMware Carbon Black for its EDR capabilities but have since realized the security value that detection and prevention together can provide us, allowing us to create time-saving automated responses. We also leverage VMware Carbon Black solutions for their effective threat hunting capabilities. Collecting endpoint data 24x7 gives us the chance to conduct advanced attacker profiling and intelligence enrichment, making our team much more efficient.

Our biggest value point that we’ve seen since using VMware Carbon Black is endpoint protection automation and open APIs. VMware Carbon Black is a non-signature-based solution, which means we do not have to worry about zero-day signatures anymore. The technology focuses more on “how is the malware performing?” and not “what is the signature of the malware?”

What are you planning to present at Connect this year?

My presentation is called, “Endpoint Nirvana: Two-Way Telemetry to Achieve Internal and External Endpoint Security Parity.” I plan to use the VMware Carbon Black platform solutions—VMware Carbon Black Cloud Endpoint™ Standard and VMware Carbon Black™ Cloud Enterprise EDR™—to demonstrate that when you see something happen within your internal environment, you can apply those same logistics in an automated fashion to your endpoint solution no matter where you’re located.
What’s exciting about Carbon Black Cloud Enterprise EDR is that it gives you the ability to do an automatic updated threat list. You can use external information to feed into Carbon Black Cloud Enterprise EDR, and use the APIs in End-point Standard to automatically change your policies.

“We leverage VMware Carbon Black solutions for their effective threat hunting capabilities... giving us the chance to conduct advanced attacker profiling and intelligence enrichment.”

JIMMY SANDERS
VP OF INFORMATION SECURITY, NETFLIX DVD

I plan to show examples where if a user gets a high-level alert, you can put the machine in a medium or high lockdown mode automatically until you can do further research, and you can use Carbon Black Cloud Enterprise EDR to do that research. Ultimately, you can do all of this through APIs and automation. In this presentation, I want to show fellow security leaders how to leverage VMware Carbon Black within their overall security stack to pivot and take action.

What would be your advice to other CISOs? First, if you haven’t already started automating your stack, you’re already behind the curve. Don’t wait, start to automate the things that you do on a daily basis that can be very repetitive for your team. Second, the reason why I use tools like VMware Carbon Black is because they have open APIs that can integrate with each other. This integration can give you a holistic security solution instead of a single-point security solution.

Discover more companies who have found success with VMware Carbon Black. Visit: carbonblack.com/why-cb/customer-success.