SANS

Analyst Program

WhatWorks

WhatWorks in Migrating to the Cloud while Maintaining Security and Network Performance (with a remote workforce)

ExtraHop

Introduction

The need for businesses to rapidly move to near 100% work at home has increased the importance of detailed and accurate visibility into user activity in remote connections to both on-premises data centers and public cloud-based services. One effective and efficient way of achieving this visibility is for network operations and security operations to use common tools that support the views and insight into both performance issues and security-relevant changes and anomalies.

During this SANS WhatWorks webcast, SANS Director of Emerging Security Trends John Pescatore interviews Juan Canales, Senior Manager of Enterprise Security and Architecture at Hill Physicians Medical Group (HPMG), to gain Mr. Canales' insight on what he went through in the business justification and deployment of ExtraHops Reveal(x) to increase visibility into network traffic during HPMGs transition to cloud-based computing. This visibility has already proved invaluable in maintaining reliability and security of remote communications as HPMG runs completely remote operations during the current health crisis.

About the User

Juan Canales joined HPMG in March of May 2012. Prior to being Senior Manager of Enterprise Security and Architecture he was HPMG Enterprise Architect where he designed HPMG's datacenters and IT Cloud Strategy. He is a leading security professional with more than 20 years of experience in computer, network and information security. He has worked in high-tech, manufacturing, financial and health care verticals. Mr. Canales has served as NetApp's and VMware CxO Advisory Board Member.

About the Interviewer

John Pescatore joined SANS as Director of Emerging Security Trends in January 2013 after more than 13 years as lead security analyst for Gartner, running consulting groups at Trusted Information Systems and Entrust, 11 years with GTE, and service with both the National Security Agency, where he designed secure voice systems, and the U.S. Secret Service, where he developed secure communications and surveillance systems and "the occasional ballistic armor installation." John has testified before Congress about cybersecurity, was named one of the 15 most-influential people in security in 2008 and is an NSA-certified cryptologic engineer.

Question
I'd like to welcome Jan Canales to SANS What Works. Juan, tell me a little bit about your background and the role you play at HMPG.

Answer
I'm the Senior Manager of Enterprise Security and Architecture at Hill Physicians Medical Group (HPMG). I've been here for about eight years and I'm in charge of security for all our applications and systems. I report to the Senior Director of Enterprise Security, Infrastructure and Operations who reports to the CIO. I've been in IT for about 20 years, with 10 years working specifically on security in high-tech manufacturing, financial, and now healthcare.

Question
What does HPMG do and how large are the operations?

Answer
HPMG is northern California's largest independent health care practice association, consisting of local hospitals and commercial health plans. We are primarily a payer of claims for health plans and independent providers, with about 400,000 members overall.

The range of security and privacy requirements is quite wide because all these providers have patients, and all these providers have their own systems. The HPMG back office is my responsibility along with our Electronic Health Record (EHR) system and some other care systems that our doctors use to provide care.

Question
What was the business driver that started you down the path of looking at products like ExtraHop's?

Answer
When I first joined Hill Physicians Medical Group about 8 years ago, I joined as the enterprise architect, focused on infrastructure. My first task was to develop an IT strategy and roadmap that included privacy and security. HPMG was struggling with older technology that had very low availability and performance was terrible. We wanted to move to cloud computing, but our business users and our IT users were telling me that one of the main pain points they had was performance. Back then, from a performance perspective it was a hard sell to go from physical to virtual. So, my main challenge was to assure we could both monitor the infrastructure and secure it, without impacting performance and shooting ourselves in the foot.

"I started looking at solutions that could provide visibility into the environment with little to no overhead. I found a couple of solutions, ExtraHop being one of them."

Question
How did you proceed on the cloud migration?

Answer
While management wanted to move to 100% cloud computing, we wanted to take a measured and sequential approach. The first step of the roadmap was to go from

traditional infrastructure to a private cloud. We needed to learn the impact on operations and performance of going virtual and the impact on business before using any public cloud services. Once we were comfortable there, we would look for other business line applications that could move to public Software as a Service (SaaS). Then we would start moving more of our infrastructure to SaaS and public Infrastructure as a Service (IaaS).

Question

So, where in that process did you start figuring out how to make sure you had the necessary security and performance visibility?

Answer

I've used ExtraHop for about eight years now. At the start of the cloud migration, we used ExtraHop primarily for the performance monitoring capabilities. As the migration proceeded and expanded, we were among the first to start using ExtraHop as a security tool as well, even before ExtraHop introduced its focus on security. We were able to adopt and deploy their security enhancements almost immediately as they released them because security was a core use case for us from the start.

"We were able to adopt and deploy their security enhancements almost immediately."

Question

What was the process you used to evaluate competing products? Why did you end up choosing ExtraHop?

Answer

We ended up doing bake offs/proof of concepts. Our process is generally to create evaluation criteria that helps us narrow the choices to three candidate solutions. At that level we are mostly looking at how much of the problem is it really going to solve.

We bring in candidate vendors to show us what the solution will look like and how practical it is to deploy and manage in our environment. We look at the Gartner peer reviews and Magic Quadrant. Is this vendor going to be able to execute what they're saying they're going to execute? We ended up choosing three products to evaluate in more detail, focusing on how easy it is to implement, how fast can we execute, and the acquisition and maintenance cost factor, of course.

We ended up looking at AppDynamics, ExtraHop and one other that I can't remember. The major difference between the products that we looked at was that most of the products out there were agent based, and we ran into overhead issues.

When we did the bake-off, some of these tools were really good at what they were doing but as we enabled additional metrics to record, the overhead increased. Lots of vendors claim their endpoint agents only consume 1% of resources, but that is at the minimum configuration. If you enable more logging, more metrics, then that overhead increases. That's what we saw in the bake off. ExtraHop's approach was the clear leader in performance.

"That's what we saw in the bake off. ExtraHop's approach was the clear leader in performance."

Question

Were there any other reasons beyond performance?

Answer

Performance was the major factor but at the end of the meeting with ExtraHop I said, "Take the last 10 minutes to wow me – what can you show me?" They showed me a dependency map which I had never seen in these tools. They showed me a system and its dependencies on the network. It created a dynamic map that I'm able to pull into Visio. As the enterprise architect, I was responsible for documenting the network and it was a challenge for me (or anyone else) to understand the real dependencies.

This really was a "wow" moment for me because it showed me that I could use Reveal(X) to get this information on my own, even if the business or IT user didn't understand the system. This product would let me know all the transactions and all the protocols from everything that was connected to that system and it gave me this map that I could use. That combined with the performance advantages caused ExtraHop to be the clear winner.

"This really was a "wow" moment for me because it showed me that I could use Reveal(X) to get this information on my own, even if the business or IT user didn't understand the system."

Question

We often see network operations using different tools from security operations. How did you get started using Reveal(X) for both performance and for security visibility?

Answer

The first use case that I recall was that we our doctors were having problems reconnecting to a critical EHR application. They were getting connected. But then, they were getting disconnected and then getting white screens which usually meant a performance issue. They called me and we used Reveal(X) to inspect traffic and we found that there was a particular tool that the IT team was using to collect metrics on the EHR system, and it was making hourly calls on the system. It was a Windows Measurement Interface (WMI) call that taxed the environment so much that user connections were timing out and the application would freeze.

While that was a performance use case, it made me realize the ability to detect anytime an application is injecting questionable processes into the operating system is very powerful for detecting active malware. That's when it totally flipped, and we began using Reveal(X) for security visibility.

Question

Once you chose ExtraHop, you had to deploy it. Walk us through how you got started and what's involved to roll it out to get the full visibility?

Answer

The first step was to feed the network traffic into Reveal(X) The first thing I did is create a Remote Switch Port ANalyzer (RSPAN) SPAN port connections from my Cisco UCS primary switch. We are a Cisco FlexPod shop, running NetApp and Cisco products. So, we got started feeding ExtraHop directly from that.

Over time, we saw that span port configurations can impact network performance. So, we moved the traffic feed from the UCS switch to a Gigamon network tap system to avoid the potential performance issues. We wanted to introduce data slowly. We have micro segmentation in our network and we started by first choosing the primary VLAN that we were concerned about. We started to look at data in our environment, understanding what systems were talking to each other. We were mainly looking at the layer seven aspect of the network and then using the native reports from ExtraHop to tell us where potential bottlenecks were. From there we started addressing them as they would come up using those dashboards and those reports.

Using that incremental approach is how we were able to go to market with this. We started to advertise to the other departments some of the reports, share with them Internet data that they didn't even know their systems were generating. They really appreciated the visibility and started fixing their code or fixing their systems according to what that performance or security data showed that was the problem.

Question

As you moved along in your cloud strategy, how did you make sure you maintained the visibility with ExtraHop?

Answer

Part of the original plans for migration to the cloud recognized the need for visibility to make sure the vendors were meeting the SLAs that they agreed to. We quickly saw we could use Reveal(X) to do a measurement of before and after the migration. For an on-premise system we would record its performance baseline on for roughly 30 days. Then, we would move that product or those virtual machines, and we would move it the cloud hosting solution and measure the latency, the round type times, where there could potentially be the bottlenecks. That gave us critical visibility so that we could adjust the performance as well as support security visibility.

"We quickly saw we could use Reveal(X) to do a measurement of before and after the migration."

Question

How do you now typically use ExtraHop operationally?

Answer

Today, we run both the performance and the security ExtraHop editions. The performance product is primarily used by the IT infrastructure team. My security team is using Reveal(X) security tool

because it has more security metrics, and more dashboards specific to security. The metrics are specific to security events.

The security team uses Reveal(X) to tell the infrastructure team that they have to patch a system that has a vulnerability, for instance. Often the IT Ops infrastructure team will say, "We don't see that. Can you share this information with us?" We give them access to the Reveal(X) system. We basically integrated the security and IT ops teams using Reveal(X).

We have configured ExtraHop (and all of our security tools) to export Syslog events into Splunk. Both the security and infrastructure teams use Splunk as a log management system. We have our mobile and remote systems feed into Splunk. We get real time alerts and dashboards to constantly monitor what's going on in our infrastructure.

"We get real time alerts and dashboards to constantly monitor what's going on in our infrastructure."

Question

How do you find the experience trying to maintain the visibility with the recent need to support everyone working from home?

Answer

We've always need to fully support remote work but we have never had 100 percent of the company work remotely. That's the change. What we've experienced is that the workload has gone up from 150 people working remotely concurrently to now having 700 concurrent remote workers. It has been pretty straightforward to use the ExtraHop products to help us monitor our environment and secure it.

A few weeks ago, we had an incident where everybody was connected. After lunch we were getting a lot of calls that users could not get re-connected. Using Extrahop, we could quickly determine that there wasn't a DDoS attack going on or any other malicious event. Turns out someone in IT ops made a change in the VDI configuration that mistakenly created a white list where only one person could connect to the network! The ExtraHop tools helped us to quickly baseline the network, understand what was really happening, and quickly get everyone back online.

"The ExtraHop tools helped us to quickly baseline the network, understand what was really happening, and quickly get everyone back online."

Question

What sort of tech support do you use from ExtraHop, if any, and how do you rate their tech support?

Answer

The tech support is great. The ExtraHop product is very robust. I'm rarely making a service call about something that doesn't work -most of my calls have been to see if the product can do something that isn't an obvious feature.

I'm always trying to think outside the box – what else can the product do? For those kinds

of calls, ExtraHop has provided top engineers as part of their support engineering (SE) program. Extrahop has been meeting with us about once a month, and they're always providing me feedback as to what's coming, what's in the new releases, what things have been fixed. They work with my security engineers to actually go through the process of updating the products and walking through with the new features, what those features are.

"ExtraHop has provided top engineers as part of their support engineering (SE) program"

Question

What are some things that you know now that, if you knew then, you might do something differently or you want to pass your wisdom to somebody just getting started looking at or using Reveal(X)?

Answer

I would say the span port versus a physical tap would be the main one because after we moved away from the spanning port to the physical tap, we saw huge performance improvements in our systems. The latency went from 50 milliseconds to, I believe, five milliseconds. It was that drastic.

The second one would be there are some products in ExtraHop (like Explorer) that are available as physical appliances, and some as virtual appliances. We went with some of the virtual appliances but found in our environment that the processing and memory requirements under load would impact overall performance of our virtual environment. We moved to a dedicated physical appliance cluster, a physical cluster with dedicated resources for the security tools. If I were started now, I would purchase physical appliances for running tools like Explorer.

Webcast

WhatWorks in Migrating to the Cloud while Maintaining Security and Network Performance (with a remote workforce)
Speaker: John Pescatore

Listen Here: sans.org/u/12sH

About ExtraHop

ExtraHop delivers cloud-native network detection and response to secure the hybrid enterprise. Our breakthrough approach applies advanced machine learning to all cloud and network traffic to provide complete visibility, real-time threat detection, and intelligent response. With this approach, we give the world's leading enterprises including The Home Depot, Credit Suisse, Liberty Global and Caesars Entertainment the perspective they need to rise above the noise to detect threats, ensure the availability of critical applications, and secure their investment in cloud.

About SANS WhatWorks

WhatWorks is a user-to-user program in which security managers who have implemented effective Internet security technologies tell why they deployed it, how it works, how it improves security, what problems they faced and what lessons they learned.