Government
Business
Council

EXPERT DIALOGUE

Parting The Clouds

A Conversation on Observability

splunk>

INTRODUCTION

Cybersecurity incidents are on the rise globally, becoming more sophisticated and threatening as they grow. Government and industry IT experts alike have realized that observability — having a clear vision and understanding of what is happening throughout the network supply chain — is crucial to protecting the network. What are government leaders looking at now? How far are they in their observability journey?

To explore those questions, Government Business Council conducted a qualitative research study capturing key insights from security experts across the federal government and DOD.

THE EXPERTS

RICHARD ARCHAMBAULT
Chief Security Officer
Arlington County

JAMIE HOLCOMBE
Chief Information Officer
United States Patent & Trademark Office

THE INTERVIEWS

WHAT DOES OBSERVABILITY MEAN TO YOU WITHIN THE CONTEXT OF YOUR ORGANIZATION?

RICHARD ARCHAMBAULT

There's an overlap between visibility and risk management. For me, there's two things. One is my third party, risk management upfront supply chain. Where are my software and services coming from, and what are they doing? Secondly, can I see what's happening in my own environment to the people accountable? Do I have visibility down to my endpoint devices' work station? We are doing well on one and learning on the other. We're doing well with a lot of the new automation tool set systems. Our ability to see what's going on deep into our network is getting better every year, and it's getting better even without tremendous additional headcount. The interoperability of those tool sets, the automation that some of our vendors are producing to help elevate the most pressing alerts, and do that triage with automation is fantastic. The staff that I do have can then focus on the important things first, because the tools are telling them this is worrisome and this other stuff is noise. That's getting better every year.

JAMIE HOLCOMBE

We're moving to the hybrid cloud and with a lot of microservices, the complexity that are involved with all our products has grown exponentially. We've connected a lot of extensive research into products and methods to provide insight into our customers' experience. We've implemented a suite of products, not just one, that provide our product teams with a holistic view about how their critical apps are actually performing. The products are a wide range of both tactical and strategic. On the tactical side, you have the ability to go out and understand sessions and packets. As you go up the stack on the OSI layers, you can see various levels of monitoring and alerts that we provide. Of course, security is right in there along with performance.

WHAT DO YOU SEE AS TOP CHALLENGES YOUR AGENCY IS FACING RIGHT NOW?

RICHARD ARCHAMBAULT

It changes every year. The tool sets change every year. There's new logic, new automation. So there's a constant training that has to be done for our staff to keep them up to date on how to use those tools to then see what's at risk and then respond to that risk. I do have to keep people constantly up to date on new tools.

Up the stream into my vendors is a challenge. Having visibility into what a vendor security posture is, what a vendor's level of risk or concern about that risk is, is an ongoing topic of conversation. From a governmental perspective, I approach it as a contractual issue to start. As I renegotiate every vendor contract, I'm putting in things like breach notification clauses, requiring that they do some sort of proactive or some sort of a SOC two level audit or internal audit where they get a clean bill of health from an independent third party. But that's really tough. A lot of vendors don't want to sign up for any level of accountability and they don't even want to sign up for breach notification. The challenge becomes: without the contractual triggers, how do I manage that? Then it's really a case by case basis. It's the concerns that we see with the SolarWinds issue, where SolarWinds pushes infected code to their customers. How do I get my vendors to be honest when that risk has presented itself in their environment, and tell me what indicators of compromise they have found so that I can look for them in my environment, and then work with me? If a vendor doesn't cooperate, I will start looking for other solutions. That is really a developing area. Every one of our vendors is unique in what they're willing to accept from a notification perspective, which then means we have a different risk management calculation with just about every vendor. As we, the security profession, learn to trust each other enough to understand what we disclose to one another is highly confidential, we can build that trust. Without that trust, that's going to inhibit the ability to really share that supply chain data and supply chain risk.

JAMIE HOLCOMBE

Cybersecurity is our number one priority right now. We have to have an eye toward remediating our vulnerabilities. We have to have an insider threat program, and we have to have the ability to train employees in security hygiene. They need to recognize social engineering attempts, phishing attempts, and all the different things around security awareness.

WHAT STEPS IS YOUR AGENCY TAKING, OR PLANNING TO TAKE, TOWARDS ACHIEVING OBSERVABILITY?

JAMIE HOLCOMBE

We're moving from observability to resiliency. Just because you can observe everything doesn't mean that you have resiliency. Resiliency is not only for a continuity of operations during disaster and recovery, but also the ability for the people to adapt to whatever changes happen. The fact of the matter is sometimes your stuff doesn't work.

> **"Resiliency is not only for a continuity of operations during disaster and recovery, but also the ability for the people to adapt to whatever changes happen."**
>
> \> JAMIE HOLCOMBE
> **Chief Information officer**
> **USPTO**

You have to have various plans and contingencies for everything that goes forward. There's really no such thing as full observability. You can have appropriate observability or the ability to measure what you've thought about. We're considering things like chaos engineering, the ability to think of things that we haven't thought about before. Between observability, chaos, and so-called predictability, we're trying to create a more understandable system so that we can respond to things that we haven't anticipated.

ARE THERE ANY EVENTS THAT COME TO MIND IN WHICH YOU THINK YOUR ORGANIZATION WOULD HAVE BENEFITED FROM INCREASED OBSERVABILITY, OR WAS VALIDATED IN ITS CURRENT POSTURE?

RICHARD ARCHAMBAULT

We had already started talking about supply chain risk a couple years ago. When SolarWinds got hacked, that seemed to be the shot heard around the world — everybody heard about it, and realized that they could be installing malware from somebody they trust. Should we really trust them? What does that look like going forward? That's really adjusted a lot of our metrics around how we buy things, how we install them, and how we manage that risk.

JAMIE HOLCOMBE

I arrived at the PTO in 2019. There are two events that happened before my arrival which are key to the resiliency efforts that were ongoing now. One was in 2015 during the Christmas time, the power went out and the entire data center was shut down. In 2018, they had a major application outage where they corrupted some data during a backup recovery. Those two outages together combined to form a organizational and cultural awareness that IT can't be just thought of as the back office, as someplace you can't consider. If you don't change your oil in your car, your engine will seize up. If you don't take care of your IT systems, eventually they will go wrong for you. And what you have been depending on will not be there for your work.

No matter even if you do have contingency plans, even if you do have infrastructure that's ready and able, people need to have the competence to bring those things up. In other words, practice what you preach. If you say you can do this in a plan, do you know how you have to execute those plans at least on an annual basis? People don't understand how many things change in one year. It's a totally different environment. You have to adapt and you have to make sure those contingency plans are good today as they were yesterday and the day before.

WHAT, IF ANY, ARE YOUR AGENCY'S LONG-TERM GOALS IN REGARDS TO OBSERVABILITY?

RICHARD ARCHAMBAULT

I think there will always be something better. We can see how computing power has moved around a lot over the years, and the same is true for security services. We've gone through a couple of boom and bust cycles where we tried to buy the best product and figure out how to integrate it later. Right now, a lot of companies are moving towards one key vendor that brings it all together. Now, we're going towards simplification, by reducing the number of solutions and the number of vendors. But in 10 years, we may be springboarding back the other direction. It just depends on what the right response is for the threat environment we find ourselves in, in five years and 10 years and so on.

JAMIE HOLCOMBE

It's both an organizational cultural change, and product differentiation. Out of the observability realm, as an example, we are a multi hybrid cloud. Each one has its various unique capabilities, its pros and cons. The big thing is trying to get the culture to match the product. Whatever products you're buying, make sure you have the culture to execute that. There is no one answer, there's only the optimal answer at the time. We'll change to whatever is best in the long term. What's best? Best is measured in better, cheaper and faster. If you can materially show me that your product is better, cheaper or faster than what we're using, I'm all ears. Some small businesses can't do this, but we're the United States Patent and Trademark Office. We're big enough that the competition needs to be there so that we can hold our vendors and our product manufacturers accountable.

WHAT IS THE FUTURE LOOKING LIKE FOR YOU RIGHT NOW?

RICHARD ARCHAMBAULT

I'm mostly concerned about end user devices. It's still common in most organizations for you to have administrative access to your laptop and if you have that, then someone can use that to install malware and use it as a jumping off point to discover other problems on our network. The buzzword is zero trust, but the reality of zero trust is just putting everybody in boxes where they can only do what they're supposed to do and preventing them from doing other things. That's my biggest concern — how do we get to a better zero trust environment where all my users just have exactly the

> **It's still common in most organizations for you to have administrative access to your laptop and if you have that, then someone can use that to install malware and use it as a jumping off point to discover other problems on the network."**
>
> > RICHARD ARCHAMBAULT
> **Chief Security Officer**
> **Arlington County**

permission they need to do exactly the job that they have, and don't have the ability to springboard off into other systems that they shouldn't have access to?

JAMIE HOLCOMBE

Our new nominated director, Kathi Vidal, said in her Senate confirmation hearing that she is interested in ensuring we have international intellectual property coordination, collaboration and transparency. That's essential. We operate within the worldwide structure. There's a lot of things to consider in that and how we can interrelate and monitor, through observability and resilience, that data exchange at an international pace. We have to have common data elements. That's why there is an effort underway at the World IP Organization to ensure that these data elements are shared and understood, so that we can exchange information once it's published, whether it's the award or rejection. And why it was rejected is very important for other people to understand and know not to bark up the wrong tree.

WHAT IS MOST USEFUL IN A PARTNERSHIP TO YOU?

RICHARD ARCHAMBAULT

I'm looking at how quickly a vendor discloses and how quickly they patch. Generally speaking, as an industry, they'll send out a patch for a security thing we found a few months ago and want you to install it as quickly as possible. That was really how things worked for years. This year, I've had vendors approach me and say that they have had a significant thing prevent this job that they cannot fix yet. Here are three things you can do to protect yourself until we can get you the patch. So that has shrunk dramatically for at least this one vendor — their time from noticing the security issue to telling us about it dramatically decreased. I want to see that continue to decrease. As soon as you know about it, tell me. Then, after that let's get it patched as quickly as possible, but there are always things we can do in that gap period between understanding the issue and patching the issue. We need to have the benefit of that time to protect ourselves.

JAMIE HOLCOMBE

Especially when I'm talking with products and manufacturers, it's understanding their core differentiation between their competitors and applying with laser focus what they believe to be the solution or answer set so that our staff can then implement and solve for better, cheaper and faster. You can apply one tool for one purpose, another tool for another purpose, and we could have both tools. And we don't want to throw away tools. A craftsman is known by the tools that he uses, and we like to have sharp tools in our bag to be able to do it. If someone can show us how to be sharper, that's what we need.

SPLUNK'S PERSPECTIVE

> Stephen Savas, AVP Observability, Splunk Public Sector

The primary challenge that government agencies face is high levels of complexity from challenging deployment scenarios like multiple clouds, complex dependencies between services, managing legacy systems and simplifying to modern APM and unpredictable system behavior. In addition, there are too many legacy tools and fragmented workflows resulting in siloed sources of data. This includes existing tools that can't keep up with the speed and scale of modern application environments. Finally, there's a lack of information sharing across agencies, which is often amplified due to cultural (internal) barriers. This is a real issue across government that must be improved and is a significant headwind to the Government achieving its stated goals.

To deliver services and meet the missions required, U.S. Government agencies depend on the largest, most complex IT infrastructures in the entire world. Their requirements change regularly, and the underlying technologies change even more rapidly. Today's migration to the cloud is a great example of this. The most important step agencies must take is to establish a common data platform that can accommodate scale and ever-changing requirements and technologies. Government systems are mission-critical and the need to manage and optimize those systems is not new. What is new is the explosion in complexity and the interwoven nature of their systems. Data has always been the underlying foundation for monitoring and as the world moves to observability, data will only increase in importance.

SPLUNK’S PERSPECTIVE

> Stephen Savas, AVP Observability, Splunk Public Sector

Splunk provides the industry’s most comprehensive observability solution which drives value in the following ways:

Only Splunk’s real-time streaming analytics and NoSample™ data collection ingests and analyzes all alerts, events, logs, metrics, and traces and only Splunk’s customized visualizations help find more issues accurately in seconds. This means 100% visibility into application performance with unsampled monitoring of every customer interaction from front end to back end.

Splunk’s integrated portfolio includes all the observability capabilities you need to support and visualize your entire stack to optimize capacity and spend. One single troubleshooting workflow means enhanced cross-team collaboration for better operational efficiency. Our industry-leading observability solution helps you accelerate your digital transformation and strengthen your market positioning by leveraging your existing investment with Splunk.

Only Splunk’s real-time streaming analytics and NoSample™ data collection ingests and analyzes all alerts, events, logs, metrics, and traces and only Splunk’s customized visualizations help find more issues accurately in seconds. This means 100% visibility into application performance with unsampled monitoring of every customer interaction from front end to back end.

ABOUT GBC

As Government Executive Media Group's research division, Government Business Council (GBC) is dedicated to advancing the business of government through analysis, insight, and analytical independence. An extension of Government Executive's 50 years of exemplary editorial standards and commitment to the highest ethical values, GBC studies influential decision makers from across government to produce intelligence-based research and analysis.

Learn more at www.govexec.com/insights.

ABOUT SPLUNK

Innovation takes many forms: transformative business changes and incremental optimizations. Both types of innovation are predicated on having secure and resilient systems. With Splunk, customers efficiently ensure security and resilience, freeing up resources to identify opportunities in their data and deliver innovations, even in the face of unpredictability.

Learn more at www.splunk.com.