[music]

Paul Thies: When it comes to cyber-based threats, few things are as critical to safety and success as the element of time. With the proliferation of bad actors, malicious activity, and the exponential growth of technology, it is imperative that, to survive, you need to be able to identify and respond to a cyber threat very, very quickly. Sometimes it's not enough to go it alone, you need strategic alliances to develop innovative solutions to stay a step ahead of the dangers around you.

Take, for example, the recent technological alliance between HPE, Jacobs, and several other entities. Together, they created an Extreme Search solution that shrunk the response time of a Splunk dashboard from 10 hours to just under 12 minutes. This integrated alliance delivered the kind of solution that is exactly what many federal customers are looking for as they strive to fulfill the Executive Order 14028, Improving the Nation's Cybersecurity.

Hello, I'm your host, Paul Thies. On this episode of *If/When*, we explored the topic of technological alliances. Joining me for this discussion are Shep Bostin, enterprise architect for Hewlett Packard Enterprise, and Doug Wolfe, vice president, and general manager for Jacobs. Well, Shep and Doug, thank you both so much for joining me today. We're going to be talking about technology alliances.

In part of that, we're going to be discussing Extreme Search and the work that HPE and Jacobs have been doing together to really enhance product offering and also leverage partnership together to better serve clients. To get us started, I'd like to start with you, Shep, if I may, and admittedly, I don't know a lot about Extreme Search and some of the technology behind it. I wanted to ask, Shep, if you might just start us off, explain what is Extreme Search, and can you explain it in a layman's terms, and what it does?

Shep Bostin: Sure, Paul. That's a great question. I've actually had to answer that question for our own internal folks, as well as for customers who might benefit from this Extreme Search offering. It really focuses on something that, on the surface, seems like one of the more mundane functions of IT, which is capturing and storing log files from applications, and network traffic, and firewalls, and so forth.

It turns out that analyzing log files really is a key to detecting and responding to potential security threats. The purpose of Extreme Search is to make it possible to search all of an organization's current log files in a tiny fraction of the time that it would take using any of the other previously existing potential solutions to that problem. The faster you can analyze that log data, the faster you can respond to any threats that you detect.

Since most folks, at least, have seen news headlines around some of the big security breaches of recent years, that's really what this is all about, the knowledge is power when it comes to understanding that you are under attack, and that's really what Extreme Search is designed to enable.

Paul: Now, this is really fascinating and I've got to assume that part of what has engendered this technology alliance that we're discussing today is that it's really enabling these organizations like HPE and Jacobs and others to come together and

share their expertise so that together we're stronger kind of thing, as opposed to trying to go it alone particularly when you're trying to combat bad actors who mean you harm.

Now, Doug, can you describe for us this technology partnership for our listeners? Who are the players and what role did each play?

Doug Wolfe: Sure. When I think about Extreme Search, I think about two technologies and probably one technique. The first is in hardware technology and that's brought to us by Samsung, and building together this smart solid-state drive that they have put together. It's a 4-terabyte drive and then they've paired up with Xilinx and AMD to put an accelerator, high-speed compute device, or an FPGA right there next to the memory.

You're bringing compute to the memory, and that's very impressive in the Extreme Search case. If you look at where HP is done now, we're able to take 24 of these drives and install those into a single 2U server, and so you're able to, at a single time, launch 24 of these acceleration devices and be able to search across all of those drives. It ends up being about 96 terabytes on a single server. That's a phenomenal amount of data to search and we get extremely fast, 25-minute or less search times across all of that data.

The other really interesting thing here is that it scales horizontally. If you have 200 terabytes, you can add another server. You can add in more servers and it still takes about the 25 minutes to search even up to petabytes of data. On the software side, the key here is that we're able to process that data without going through the traditional database processes, so the ETL and indexing, you can think of putting data into an Oracle or some Postgres or open source type database.

By being able to bypass that, it gives us a tremendous amount of speed and it allows us to access that data immediately as it arrives. Lewis Rhodes Labs has been working with us on putting the software on the FPGA, and the SmartSSD, and then BlackLynx, now Jacobs, is building the software that processes the incoming data as well as provides the interface to the tools and allows you to integrate that into your IT environment.

When I talked about a technique, we built an API into Splunk, which is a common system incident, an event management tool that we can now run Extreme Search from that Splunk interface. We can do all of the queries through Splunk and we bring the results back to Splunk, so it's a very seamless transition, and we're able to partner with other SIEM-type providers, Splunk being the biggest one with being able to integrate that seamlessly.

It ends up being an HPE server, 24 solid-state drive brought to you by Samsung. We've got Lewis Rhodes Labs software as well as Jacob software on that particular server. That's the partnership suite.

Paul: Wow. Now, Shep, can you talk a little bit about how the partnership worked, the practical matters that had to be attended to? I'm sure that everybody has their own sensitivities and their own special capabilities that they bring to a partnership

like this. Practically speaking, how do you engender that, that collaboration and that openness for a program like this to be successful?

Shep: Well, I think, you captured the word right there which is collaboration. It really was a collaborative effort as Doug described the technical components of the solution. We had Samsung with a hardware piece, AMD had purchased Xilinx, which produced the accelerator that's embedded on those Samsung drives. HPE is producing the servers, which happen to use not only those accelerated SmartSSDs but also AMD CPUs, which have a very high core count and lots of RAM in these Extreme Search servers to help with the performance.

Then, as Doug mentioned, Lewis Rhodes Labs produced an important piece of underlying software technology that helped glue all these technical resources together to produce very fast results. Then Doug's group now at Jacob's put the final glue together to plug this into Splunk, which is by far the leading as he explained SIEM tool in the marketplace used by a lot of different organizations. I think to make this all work, everyone understood what role they were playing in all of this. It certainly helped that HPE has a very solid partnership already with AMD. We sell lots and lots of AMD servers and accelerator technology. It helped that the organization that Doug with BlackLynx that joined Jacobs. Jacobs is a longtime partner to HPE as well as customer of HPE.

They've purchased technology from us, Jacobs has as a company, but also we've worked together in fulfilling the needs of a variety of customers out there. We have a history of collaboration as well. I think it helps to build a relationship among a group of partners who've already done some successful things together. Then I think, from a practical standpoint, as we start to go to market with this and introduce it to customers, we're now in that phase where we have the first few customers who are actually using this.

We're starting within the federal sales organization to go after more customers who can benefit from this product. I think there, again, it's a collaborative effort between all of the parties involved to explain the technology, to show customers why it works as well as it does, and to educate the salesforce, particularly with HPE, because we have a large sales force, educating our sales team has been a focus of mine.

It's not explicitly "part of my job", but it's more I had the opportunity to get involved with Doug and with the AMD Xilinx folks. I've been helping internally to write blog posts and create internal collateral materials so that we can start to build up the customer base for this offer.

Paul: I've got to imagine that customers generally like to see these kinds of alliances, like to see the best of a number of players brought to bear to tackle a problem and really work together to address their needs. Now, Doug, BlackLynx joined the Jacobs family in late 2021. It's pretty new still to Jacobs. Talk to us a little bit about what led BlackLynx/Jacobs to get involved in this program? Can you share a little bit about the role that-- I understand there's an executive order that played in creating this opportunity?

Doug: Absolutely. I can tell you firsthand that having lived on the customer side, it is certainly helpful when people help bring solutions and help solve problems that are

out there, as well as provide a way to transition, because frequently you'll see great technology, but not having an easy way to get it integrated into the system is particularly important. One of the things that we were focused on at BlackLynx was being able to process many different digital streams, not just event logs that censor streams, or other digital types of data, to do that as rapidly as possible.

We were focused on the intelligence community and the DoD market. The executive order came along, and they've had a recognition that across the federal ecosystem, there's a huge amount of vulnerabilities. We see that in the papers all the time. It's a sprawling enterprise. There's all kinds of different networks and systems and computers and you name it, connected together. The good news is that we capture a lot of logs about how all the systems work together.

We have not, to date, had an ability to capture those logs and then efficiently process data to tell us what's working, what's not working, what's normal, what's abnormal. The fact that the White House and then OMB came out with these executive orders and directors for agencies of the government to implement this kind of analytic and to have these logs online and searchable for the past year or so really aligned with the technology that we had been building and that we came together with on the Extreme Search.

It's not the only use case for Extreme Search, but it is a near-term immediate one and it works exceptionally well for that case. The other thing is that not just the federal government, but contractors that do business with the government industry, everyone has an interest in solving this problem. We think it's a much bigger than just government type of product that we're providing here.

Eventually, we'll get in working with Jacobs into more of the operational technology and even the infrastructure technology, where you're measuring other things through a factory or through a pipeline or water treatment, et cetera, and we can process that data as well. This is the opening use case. We think there's a lot of exciting things to come even after just processing only event logs.

Paul: That's fascinating. I'll step out on a limb. I've got to imagine that, with the proliferation of internet of thing devices and smart sensors in infrastructure and smart environments and, like you said, wastewater plants and things like that, digital twinning and all of that, there's so much data out there that anything that can be done to make that processing run smoother, faster, identify potential security blips and things, it can only be a good thing, right?

Doug: Absolutely.

Shep: Shep, let me ask you to expound a little bit on the idea of an alliance like this and the benefits that it brings to clients when they see improved performance, I'm assuming yes, but then also things like reduced cost or any other benefits that clients both in the government sector, but then also as Doug was alluding to more and more in the private sector, what kind of benefits do you foresee clients will be able to enjoy from something like this?

Shep: The solution certainly fills a vital need for our customers. As Doug touched on, first and foremost, for those of us who work at least part of the time in the federal

government space, there are those recent mandates by way of the Executive Order and the OMB directive that all of those agencies must comply with. It's dramatically increasing the amount of log data that they retain. Some of these very large entities within the federal government, they were retaining maybe 90 to 120, maybe as much as 180 days of log data.

It's a lot of information and it's not so much that the space to store it all is all that expensive these days, disk space has come down. It's more of it takes so long to analyze the information that there was just no point in keeping more than that because it could take days, even weeks, to run certain kinds of reports and queries against the data. It's really crazy how long it takes to go through all of that information and get a useful answer.

This jibes with what you both were talking about a moment ago with IoT and OT which obviously impacts not just the government, but all kinds of organizations. HPE has tons of very large customers in, say, manufacturing, oil and gas, healthcare, and so forth. Where part of why the customer hasn't done the kinds of analysis that's necessary to say, "If not prevent a solar winds attack, perhaps detect that attack much sooner so that you can shut down those exposures" is quite frankly-- it just wasn't possible to efficiently and rapidly analyze data from a wide range of streams, as Doug described.

You just couldn't get the answers fast enough to be useful. One of the big benefits that Extreme Search delivers is certainly improved performance, as you put it, is almost too weak of a term, really. It's a dramatic order of magnitude or more performance enhancement to use a technology like Extreme Search with the hardware and software components that are optimized for this task.

That's a huge, huge thing. By reducing the time that it takes to find out that you're under a potential threat by responding to that faster, the risk mitigation, the savings of potential losses. I forget what the estimate is. It's something like $1 million a day for servers to be down in many of these organizations. If you get attacked and you can't respond to and shut down that attack, you can incur tremendous costs associated with remediating any kind of a breach. Of course, worst of all, if you think about some of the federal spaces, as Doug and I have talked about, in intelligence community and defense, as well as in some places like healthcare and oil and gas, the costs of breaches can translate into lost lives. You literally can have people's lives on the line because you're under attack and you're unable to detect, respond to, and shut down those kinds of breaches quickly and effectively. I think those are just among some of the benefits.

As I put it way back at the beginning, it's hard when you first say to someone, "Oh, it's a great way of analyzing log files." If they're not well informed, they go, "Oh, well, that sounds really boring." This is some of the most important and interesting work that people can do to protect their organizations and ultimately to protect the people whom they serve.

Paul: Yes, and security is probably not taken as seriously as it should be across organizations, data security, and it's like the exponential costs are probably incalculable. When you attack a system and there's so many systems that are interdependent and, like you said, it's not just wild hyperbole that say that people's

lives could be endangered. You think about like emergency response systems and stuff that could be impacted by a bad action and things like that, or time is everything.

The longer it takes to respond to things or even impacts the things more mundane, like supply chain items and things, it's just that the impacts are far-reaching and people just have no idea, I think. Shep, let me ask you, this is the devil's advocate type of question, but how does something like this technical alliance coming together as parties, delivering an improvement, how does it deliver an improvement over what might be currently available in terms of solutions in the marketplace?

Shep: Well, really there's what I've described to our own sales team as this kind of three-legged stool of the things that Extreme Search does that are really unique within the market today. First and foremost, as we've touched on, is the performance of the solution. It's faster by a lot, by an order of magnitude or more than any solution that's out there. Hand in glove with that, believe it or not, the analytics that are available today for logs don't span multiple sites within an organization.

These days, the typical way that people analyze log and network information is on a site-by-site basis. It's up to each site to review its own exposures. You cannot, as a senior IT manager across a large multi-site organization, whether we're talking about a government agency that has many locations or bases, or whether we're talking about a healthcare enterprise that's got multiple hospitals, there's not been a multi-site analytical solution.

Extreme search is, in addition to being really fast, is multi-site. You can sit at a single workstation through a familiar Splunk interface and ask some analytical questions about your entire enterprise. It will go out to the Extreme Search servers that are installed in each of those locations, and then it will aggregate the resulting information from all of those locations and present it as a consolidated view.

That is simply not existing in the marketplace today. It's a huge benefit when you look at some of these government agencies that are all-- There's really no government agency, even the smallest ones that exist only in one place, it's the federal government, it's everywhere. This is a solution that really provides something unique with the multisite capability, and then of course the performance metric, and as Doug mentioned, the architecture is such with the smartSSDs and the software that's been created for Extreme Search, that you can get an answer in 25 minutes or less at any scale because these Extreme Search servers are out there in your various locations.

You scale them up to meet the size of the enterprise, and so they're able to deliver that result rapidly. Then I would say the final leg of that three-legged stool, which tends to be the most surprising to our salespeople, is it's actually less expensive to implement and operate Extreme Search across an organization. In fact, the larger the organization is the more that that cost differential becomes apparent versus the conventional approaches that folks take today, which is just shocking.

The reality is that, today, to try to accomplish these results, enterprises invest in very expensive indexing servers to sit in these various locations and try to ingest, like Doug mentioned the term ETL, where they extract, transform, and load vast amounts

of log data and index that data in order to present results to queries. That is a very costly process, and it's very costly hardware that's necessary, and it's more costly the bigger the organization is.

These solutions for big organizations, these are not what you'd call dirt cheap off-the-shelf best buy kinds of things. These are serious enterprise-class solutions, but when compared to what's out there on the market today, the cost differential for larger organizations can literally be millions of dollars. It's better because it's multisite, it's faster, and shockingly it's even a little cheaper. That's kind of the big three that I've gone to our salespeople with that makes it a very compelling solution for customers.

Paul: That's really fascinating. I really think that, and I've seen it just in a very pedestrian way, I'm not necessarily like a data scientist or anything, but I have seen, like in thought leadership, there's just, in the last several years, at the executive level, there's more and more of an emphasis like in the chief information science officer level to really focus more in investing at the enterprise level on security and on data governance, more so than probably ever before.

It's because it's the world we live in that the threats are ever increasing and they're ever growing in sophistication. It really becomes, I think, incumbent on clients to just get serious about making those kinds of investments. Like Shep you're saying, it's not something you can just pull off the shelf Best Buy.

It's also probably not something that you want to try to stitch together with a bunch of different providers here, there, and everywhere as an organization, but you want to be able to go with a proven winning solution as opposed to trying to like, "Well, we bought a little bit of this from this group over here, but then on this other geography we bought this solution. Now let's try to figure out how we make them talk together."

It sounds like, with this technology alliance, with Extreme Search, that you've got that greater centralization where, as a client, you can see more of what's going on. You can leverage economies of scale, I guess might be a way I would put it. That's more effective. You invest a little bit more now maybe, but the returns are immeasurable in terms of getting serious about data security and about the threats that your organization's faced with.

Shep: Well, and I think the collaboration is key because the first question that a customer has after they're sold on the idea is, how do I do this? They just don't know. That's where the collaboration particularly between Jacobs and HPE is really a big part of this puzzle because the necessity of having experienced people who can go deploy this solution as an integrated solution and not just a bunch of gear and software that it's up to the customer to do, that's really where the rubber meets the road for the customer, and they go, "Okay, I get it, I feel like I can move forward because you guys are two big reputable companies who know what you're doing, you've done it before."

That's been, I think, the win as we start to pursue opportunities together.

Paul: Yes. You've taken the pain out of trying to figure out how different parts will work together. You create a seamless solution that works across the enterprise. Now Doug, let me ask you, Jacobs does so many different things and, like you alluded to,

"We're in the infrastructure business, and we're in aerospace, and we're in cyber and data, we do all kinds of things at Jacobs." How do you see this particular service? How does it enhance the work that Jacobs is already providing? How does it contribute to, as you see, Jacobs value proposition?

Doug: I think Jacobs has had a strategic initiative now to really look at how to get into data and data analytics and understand that particular side of it. We do have a number of folks that are deployed to customers across the government, other locations as well where we're entrusted with running system operation centers. Those folks are seeing the challenges that we've talked about and Shep talked about a few minutes ago, in terms of not being able to understand or know exactly what's going on in the infrastructure.

I feel like the opportunity for the folks that are with the customers that are hands-on, that are really focused on mission and making the mission work to be able to understand and bring products that are highly performant and can make a difference on that mission, I think that there's significant opportunity there. Then I believe, as we are able to reach other customers with the particular technology, that you've got an opportunity to add additional services and to help make sure that the system is working and running and operating and fits within the ecosystem.

As much as we do, and we do a lot, we don't do everything, and there's other important tools and other applications that need to continue running as well. Ensuring that that customer environment is as smooth and seamless as possible is still going to be incredibly important. This just gives us a bigger way to contribute to the overall customer mission both on the product technology side, as well as those hands-on services.

Paul: Excellent. Doug and Shep, I want to thank you both so much for joining me today and talking about this. I know when I saw some of the notes come through, it was just mind-boggling how fast something like Extreme Search, and I'll have to look them up and put them in the show notes here, but you go from hours to seconds practically in terms of how it truncates the time, the speed to deliver information is just mind-boggling.

It's great to see organizations like HPE and Jacobs get together and solve for solutions and really find interesting ways to solve problems that, maybe on their own, it would be harder to do, I would imagine. Anyway, Shep and Doug, I want to just thank you both so much for your time today.

Doug: Thank you, Paul.

Shep: [unintelligible 00:33:02] joining you, Paul. Thank you.

[music]

[00:33:18] [END OF AUDIO]