Project Completed by:

EDUCAUSE
Next-Generation Cloud Security for Higher Education
Tuesday, March 09, 2021
1:00PM - 2:00PM Eastern
>> Good afternoon everyone and again, thank you for attending. I am Hunter Ely strategist for Palo Alto Networks. I want to thank EDUCAUSE for allowing us to speak as well as our panelists for taking time out of their schedules to plan and participate.

>> Good morning I am Mary Welsh, CIO. KU is a fairly large institution, 19,000 undergraduate and 7500 graduate students. We really worry about security all the time. I know that we are focused on network security, which leads to endpoint security and data center security. Which we have a lot of challenges in regard and challenges with security. And we are folding in teaching, learning and working remotely with the pandemic which adds new dimensions to the security challenges. And I think we can also agree that we share the same constraints in regard to finding and resources so there is a lot to balance. But one of the nicest things about being in higher education, is we collaborate, we only share information, we share the lessons learned, we partner and we reached out to colleagues quite a bit and never had anyone decline help, give information or give guidance. Is one of the nicest things about higher education. Sometimes, we are a little competitive when it comes to athletics. But in IT, we are always collaborative. In addition to that, we also have these organizations EDUCAUSE and Internet2 that really understand higher education. And provides structure and guidance for us. So, all you have a lot of challenges we have a lot of shared resources. And having that really helps us develop strategy. I can say, I don't have enough resources and maybe you don't have enough resources. But working together, we can find a path forward. And together, we can develop strategies to deal with all of the challenges that we faced. So, in 2019, I'm going to shift a little bit to what we are doing right now. In 2019, we partnered with Palo Alto and had a project to a store a Porter intrusion protection system and it went very well. This led to an opportunity to engage with the service evaluation. And again, working within higher education, we had the opportunity to work with a wonderful group of technical, higher education experts. It was a real partnership. We leveraged the input and the knowledge of the group to develop this solution. I do want to take a moment to look at it a little holistically. I want to acknowledge working with Internet2, Nick and I spent a good amount of time together. But really made a difference for us, is Internet2 really understands. Having the research and guidance, we also know how to really protect the institutions. And build solutions, but also the structure and contracts that go with them. During this engagement we also built the contract that will be supplied with this. I want to take a
moment to show them a general counsel was actually very, very happy. I don't say that every day but they were very happy that we built a contract that genuinely protects the institution and will protect all institutions. For example, this sort of three or four main battles we grapple with and for example, one is governing laws. In this contract, the governing law is based on the location of the main campus. It really has the insight that for every institution, there put in a really good position. And I'm sorry, Hunter, I forgot to tell you to advance the slide. That was my fault. So, there are a few other things I can put in chat that Nick was able to put in place for us. And it puts the institution in a really good position. And we can come back to details later during the conversation. But then, I would like to shift a little bit to working with Palo Alto. And really, I'm excited about this, I want to say solution but maybe it is multiple solutions. And I will let Hunter speak to it more in detail. But you know, we are all grappling with security, every single day, there's another threat that we have to work through. But in this case, what I really like about this solution is, it is looking down into smaller step. It really provides security. I think Hunter mentioned a maturity model. But it is a nice, thoughtful and carefully laid out plan to start with smaller steps because that is usually what we have to take. And then, moving into a more mature level. I am getting a note that my Internet is unstable. I hope I'm coming through clearly. Thank you. Okay. So, again, looking at these bundles, there are smaller steps, steps that we can take immediately, building to 360 degrees view of security. And in higher education, we generally cannot take the large bites all at once. With funding even if we have funding the resources to fulfill that is really challenging. What I genuinely like about this, is that is very carefully laid out model that we can work our way through over time. You know, the famous triangle time, money and resources. We get restrained so we pull on the leg of time. And this puts us in a really good position to build out our security maturity model. So, I want to stop for a few minutes. I certainly said a lot. If there are any questions we can take them. But at this point, I would like to turn it over to Nick and let him talk about the Internet2 piece of it.

>> NICK LEWIS: Thanks, Mary! Just like Hunter gave a little bit about his background prior to Internet2 I was information security officer and I worked throughout higher education for 20+ years. So I have a deep love for higher education as well. A little bit about Internet2 in case you've never heard about us. Internet2 exist to facilitate collaborative effort in US higher education institutions to design and provide selected mission-critical services required to advance all aspects of their academic and service missions. We work by engaging mutual interest collaborations, across diverse communities to advanced scholarship and accelerate discovery. Next slide. A little bit about Internet2 by the numbers. We have got 200+ US higher education members. We have got 60 plus industry partners, with 43 regional network partners, 60 plus government agencies and a large number of, a large number of other institutions across the higher education community. Next slide please. A little bit about my specific area of Internet the net plus division where a trusted ecosystem of tailored top-quality cloud solutions where we have 381 institutions subscribing to at least one NET+ service, 102 institutions subscribe to three or more NET+ services. And 117 institutions have contributed to lease one NET+ service evaluation. Like Mary described University of Kansas doing. Then we have 20 NET+ cloud services in the portfolio. With four new services in developing, including the one we're talking
about today for Palo Alto networks. Next slide please. Getting down a little bit more into details, around the NET+ cloud services. We are partnership to provide portfolio solutions for research and education community. Cost-effective, easy to access, simple to administer and tailored to the unique, shared needs of higher education. Some of the key aspects of NET+ services are, is developed for the community led service evaluation process. We would go through a rigorous process to evaluate the service working with the service evaluation campuses. And then as Mary mentioned, all of this work is backed by a group negotiated agreement. Working with Palo Alto networks in this case, and the other service NET+ providers and other programs. Then we have, once we have that initial service evaluation completed, there is a service advisory board that is supported by a program manager. Like myself, and my colleagues. To support the community engagement and provide oversight to the program. Next slide please. A little bit about more on the NET+ services and what we are about. We are looking at defining a new generation of value-added services. Trying to focus on what campuses need three years out were more so that we can be prepared for the early -- in the rest of the community to identify cloud services quickly and easily and cost effective as possible. We want to leverage the existing resources that are already in place. We have got significant investment in the community with Internet2, we want to utilize that and we want the campus to be able to access cloud services. It helps drive down cost of provisioning and consuming services for your campus. As we have been talking about, these programs lead to deep strategic partnerships with service providers like Palo Alto networks and there been a very strong partner going through the pandemic and working with, continuing to work with us for the past year through all of the various things that have curveballs that everyone in the community has had to work through. As part of keeping the institutions running. As part of the service evaluation and service provider try to leverage a community scale for better pricing and terms across the community. And then lastly, for the NET+ services we look at solutions that meet the performance, usability and security requirements for campuses. Next slide. As part of the service evaluation process, we are trying to make it as, speed up the access to the cloud for campuses, so you can get all of the benefits as rapidly as possible. And as easily as possible across the community. Across your internal campus community and as part of this we try to reduce the time that an individual campus needs to take to adopt a new cloud service. By having pre-negotiated terms and conditions that were developed by your peer institutions. And then having the service providers being required to completely standard compliance documentation that you expect. So they have it ready for you when you ask, you do not need to wait for that were work with them to develop it. It is just done because your peers have worked through those engagements with them. Then we help reduce the cost to speed up Access by working discounts based on the size of the Internet2 membership and the broader higher education community. And us acting as a community can help drive down the cost. And part of driving up costs for the campus, we help minimize legal engagements for campuses by pre-negotiating all of the terms for your campus. So that it should meet the majority of your needs out of the gate! Then we help reduce risk through the contract, legal negotiations, where the important terms for higher education are reflected in that agreement. And then, pricing being backed by the Internet2 -- agreement. All of this is to support the community. We have a number of areas where Internet2 works developing and supporting cloud activities. Of course, would all like to be able to do
presentations like this in person or engage in person and we know that it will be a while until we
can do some of those things. But in the past we have done things like, we partnered with between
industry and higher education to support a domain area research using cloud technology like the
one that was done, large data for University of Kansas. And then another example is more
specific service provider focused. We have done specific events for individual services at their
meetings where we gather all of the higher attendees to share information about the service
provider and provide the engagement. And of course, like this webinar today, we have a myriad
of virtual and great engagements like getting started with NET+ training series were higher
education communities able to learn about how to adopt GCP then talk about learning
management systems for transitioning to online learning and preparing for fall of 2020. And then
introduction to the research and education community for AWS for researchers to increase the
speed that they can adapt AWS and cloud services across their community to improve, increase
speed of adoption of cloud services. We have a number of other community projects and
activities. Like the Internet2 and EDUCAUSE higher education cloud. Then the architecture
wiki. We also have REN-ISAC we have cloud security across the community and assessing
services where NET+ has adopted the core aspect of the NET+ program. Next slide please. There
are a large number of other ways to engage with the NET+ program and community through the
program. You can just, like all of the 300+ other institutions, can engage through signing up
through a program. And then, you come through the contract and stay for the community. So you
can engage with your peers on, how do you use this feature functionality? I am trying to solve
this problem, so that you can ask your peers what is going on with the service on their campus or
how they best deployed it. And then, taking up if you're deeply engaged, you can join or
interested in more deeply engaged in, you can get involved in a service advisory board open to
NET+ subscribers and help provide oversight and engagement for the overall community across
that particular program. We have a number of working groups, we have a storage working group
where they're talking about how to manage cloud storage across multiple different cloud
services. And if you're so inclined, like Mary and University of Kansas and other campuses
involved in the service evaluation, you can get involved and volunteer time as part of a service
evaluation. I have heard from campuses that they appreciate being able to hear how their peers
are assessing cloud services across other campuses. And some campuses learn to use it as
professional development for learning how other campuses have done the assessment so they can
translate that back to their home institution. And then as I mentioned before we got a large
number of virtual events where like this one, you can attend and engage and ask questions. Next
slide please. Other ways to engage, you've got basic Internet2 membership and InCommon
participation. We know that comprehensive service evaluation going through Palo Alto networks
may not scale to meet all of the cloud services that the campus might need to address. So being
able to have that flexible model may help your campus address all of the other cloud services on
your community. Then there is of course, a large number of other options with colleagues at
EDUCAUSE and REN-ISAC will record it very closely with information security aspects
because we want to most effectively use the community resources and help people get to solve
problems that they are trying to work on now and that they see coming in the future. Next slide
please. Now we get specifically to the NET+ Palo Alto engagement. We started out with service
evaluation last March. With our standard 90 day plan to work through the engagement and we had the same thing happened to us that did everyone else. Where the pandemic hit and had to change course so working with University of Nebraska, who sponsoring Drexel, Duquesne, rice, Kansas, Kentucky and Villanova. We started the work and then, where we were including the Prisma Access cloud and SaaS as part of specific products that will be included in the bundles that Hunter will talk a little bit more about later. As part of the service evaluation. Then we had the pandemic, next slide please. What we started hearing from campuses at the beginning of the pandemic was, teachers need to be able to be prepared to educate remotely. We'll have capacity to support remote access to 20 percent of our workforce. We do not have the network capacity to support over 50 percent of our users working remotely. When we heard this, we thought, there's a real problem here! We need to do something now. We need to help our peers, we need to help the community with something right now. And so that is where we took sort of a turn off of our plan. Next slide please. And we took a turn off of the plan, based upon the pandemic and what we are hearing from the community where we did what we call pre-evaluation agreement where Palo Alto worked with us on doing a pre-evaluation agreement just for Prisma Access because we knew compasses had and immediate need to get back to campuses for a number of different reasons. So as part of that we did pre-evaluation agreement and once we completed that, we started engaging with re-engaging on service evaluation going through the steps and getting close to the end of that process. Next slide please. As part of the process, the service evaluation process we went and did a security review where we reviewed the HECVAT and give them feedback. Discussed InCommon integration and how identity may or may not be used in different services included in the evaluation. Then we discussed network integration, as mentioned before we want to use what is already in place. And we discovered that with Palo Alto networks they were hosted on AWS/GCP so we can already use what's in place to provide high-level network performance to campuses. And then as Mary mentioned, we started working through the customer agreement where we include higher education terms and protections for campuses. Next slide please. I think that handed over to Hunter!

>> HUNTER ELY: Thanks a lot, Nick. And thank you, Mary, for that start out. So, I want to spend time of the process. Before that, I always have to learn how to use the slides. And then I will go to the next slide. I was put this up as my first slide anytime I do a presentation. And they do this for a couple reasons. One, it reminds me of a couple of things. He reminds me that I am here as a Palo Alto networks employee and certainly, selling products and services key to our existence and my mortgage getting paid. I'm here because I have a deep appreciation and love of education. Nick and I share our backgrounds in that we spent a lot of time in higher education. And we're looking for other ways to support that. As my Northstar I always remind myself that we are in support of the mission of the University. Whether it's research, workforce preparation, all of these things are important in keeping that stuff secure. It is absolutely crucial. Moving forward, let's talk about what we did over the last, it has been a year. We spent several months at the beginning, then took some breaks because of the pandemic and had to slow things down. But we had several meetings where we talked about what can Palo Alto networks to support the community that is outside of the firewall? You know, if I were to guess, say most of the
attendees here know that we are a firewall company first and that is how we were founded. But everything I'm going to talk about is all of the other things we do. Not all of the other things but majority of the other things we do. Because it's clear that we are known as a firewall company but not known as a visibility and security company. Which I think is again, critical to the success of higher education and security of all various things to deal with. The pandemic brought a few things to the front. The top was this massive shift in consistent secure remote access. Simple remote access. This is a direct, falling on of the pandemic. Everyone had to work from home or work remotely. We had to find a way to bring those resources back. That was what we did in the pre-evaluation. Agreement with Internet2. The need was acute and timely and they agreed to help us with that. It has been in a place for a while. And we will continue discovering other things that were going on in the higher Ed world. And make sure that we are speaking to the security needs. The move to the cloud has been accelerated. The pandemic has highlighted some of that. Certainly, traditional cybersecurity tools cannot meet the needs of next generation infrastructure. We are finding that tools -- nearly every school of talk to in the last couple of years, has been a multi-cloud school. Whether they meant to or not, the central IT group, and while researchers are using GCP for their research project and how are you marrying all of that data and security data amongst the tools? We will not tell researchers they cannot use GCP. So you have to find a way to enable them to work more securely. Then there is growing need for visibility across an ever-expanding network set including cloud on premise and in many cases, home networks now. Shadow IT is harder than ever to detect and you know, your users are often well-intentioned but they are trying to solve some of their personal IT problems from their house, and shadow IT comes a risk. We also talk about higher Ed is the inventor of bring your own devices. I believe that is still to be true. And we need to find ways to bring visibility to those devices so they do not bring risk to your networks. We need to have contextual alerting between servers networks and applications and all of those pieces and parts that make up your networks. This is something we repeatedly heard about in the service evaluation process as part of a bigger visibility problem that exists. Then of course, the great motivator that will deal with is compliance to applicable regulations and laws. You know, we have federal research something everyone has to do with when it comes to student data and a myriad of other things including things like normal justice information systems for those that have police departments and systems like that. Then this inadequate staffing to meet security needs. This is the beginning of time, prior -- problem with higher Ed. I don't think anyone is overwhelmed with security personnel with nothing to do. We need to become more efficient and automation is a way to help meet some of those needs. Lastly, this is a sort of a sticking point for me personally. There's just too many security products out there that do a very specific task, perhaps very well. But they do not share the data between the applications or any others so how do we get a holistic view of your environment if we are not sharing threat data amongst the applications? Clearly, the best model is failing. We took all of those challenges and distill them down into what we are calling four bundles or solution sets. These are four areas that we saw that we can make a real difference and to Mary's point, help bring up the maturity model of the University. As well as allow them to build these in a way that makes sense for them at that time. Based upon budgetary considerations and all of their other needs. And then you can mix and match these in a way that meets all of
your needs over time. The first one of course, secure remote access for all use cases everywhere. For us it means cloud delivered security. Every product called (Term?) which will solve that for you. Very simply. And it plugs in all of the other services. Many cloud native security that is normalized and managed across all platforms. When I think cloud native I'm thinking the big picture. I am thinking about not just infrastructure, or platform as a service but the applications that we all use. There it is box.com, shout out to them for another net plus service. Or office 365 or G suite, these are things that need to be managed and secured in a similar manner to all the other cloud services you have. And then of course, bring the threat data all back to the central point for normalization and management. We need to rethink what traditional antivirus means and what is now called, we call it XDR. -- Weird to think about what the next generation detection response technology looks like and how to apply it across all of these cases. Lastly, in the most mature organizations, we really see a move to automation as a way to solve the nagging everyday problems. You know, I know that no one of this cause ever had to deal with spam or phishing but this is an area where you see those emails coming in you could do something with them in automated fashion so you're not burning person time trying to deal with these low hanging fruit situations. Automation engines that can connect all of these pieces together so that you can automate a threat, put a ticket together and all that threat data you can either act on that or put it to the bigger context of what's going on and move on from there. So, these four solutions as I will go into detail over the next few slides. Just to give you an idea of the thought processes. The challenges here were around remote workers and students. The idea they need flexible policies for access of different systems, based on different users. And perhaps, even the assets that they are using to get to those various remote services. And scalability and manageability of the system as dealing with you know, the traditional VPN case of a few hundred users to potentially hundreds, thousands, tens of thousands of faculty, staff and students. For us, using a cloud delivered a scalable model is really the way to go. And that was with Prisma access. It is the remote access component where we are adding cortex data Lake for the Lodge management or collection point for the logs. We include panorama as a way to manage this across your infrastructure. And of course, global protect and support. Global protect is, is the same client as Prisma Access but attached to the firewall. If you have on premise needs as well as remote access needs, we've got you covered in this remote access bundle. Again, this bundle was built out of these conversations with service evaluation. And by putting it together in this way, you accept success with all the pieces and parts you need day one. Second challenges around cloud native security. This is again, everything from containers, infrastructure, platform and SaaS applications. Some things include budgetary considerations around operational expenses for capitol expenses. The flexibility it gives you and the speed to deliver that the cloud can bring, but there's a lot of tools we traditionally used that are lagging far behind. An increasingly multi-cloud infrastructures are complicating these efforts. If you are in Oracle, using that you are often forced into the Oracle cloud. So there's one cloud. How do you manage across multiple clouds? This gives you greater visibility and contextual holiday which again, use contextuality because it is critical to success. And this gives greater flexibility to meet needs. Now you can say you can use GCP but in this way. It allows them to have the flux ability for the tools they want and allows you flexibility still provide at level security. Components here Prisma
cloud, we have Prisma SaaS, traditionally -- a cloud service for SaaS applications, lived cortex data Lake you will see a theme here with that in a minute. And subscriptions to support that. That includes zero day subscription, DNS and URL subscriptions as well. Third challenges around next generation endpoint detection and response. Bring your own devices continues to be a challenge and managing your ever-expanding BYO infrastructure. BYO uses are critical to reducing risk pretty gives you security across all devices. And again contextual visibility shared across infrastructure. We have two versions of XDR. It's traditionally more like a traditional antivirus client that it is a little bit less intrusive on your endpoints. This is great for workstations and your daily use assets. Then we have XDR Pro which is redesigned for data center servers, things of that nature. High-value endpoints you want greater logging on and more protection opportunities. Again, cortex data Lake to Todd is altogether. And again, all of the various subscriptions to support that. The subscriptions are the same technically, as the subscriptions for the firewalls and that they provide the same benefits, just applied to the cloud services instead of your firewall. Lastly, we have security ops automation bundle. This is really you know, Mary and I were talking about this a few days ago. She sees this as sort of the you know, the maturity model really sort of reaching its peak because once you have all these other pieces in place, you can use automation and start tying them together. The example used earlier was phishing. If an email comes in you can reach into the cloud service to the email deletion from the rest of the mailbox, pull it into cortex so that it can make sure there is nothing, no payloads in there if it is just a simple phishing email you can put that into the ticketing system, and bring the threat data to cortex for later analysis or follow-up if you need. But it can all be done to these multiple systems tying them together through automation, for us it is called XSOAR and we use data Lake to store the data. These alerts and playbooks are two areas where I'm really excited to partner with Internet2. I see a bright future with the community where we can start building playbooks and potentially sharing them with each other and really start bringing up the game of the community which is ultimately, what we want to do with the, with all of these bundles. To reinstate the bond also put them in this picture and we will, we will go on the next steps and questions. I really like this picture because it shows them altogether. But again as Mary pointed out, this is sort of a path for you. You can start with remote access, move into cloud security, then endpoint detection response and ultimately automating all these things. If you're pieces of some of the solutions you can certainly go in any order but there is sort of a nice story to tell here of maturity model over time so going left to right. We've been working on this for one year. The pandemic slowed us down quite a bit and put service evaluation members in some tight spot and we really appreciate the continued help with the community. We are almost there. We have to finish the service evaluation. What does that mean? The boring legal stuff is going on, some of the business stuff is going on but those are all you know inside baseball sort of things we need to get done. That stuff will be done very shortly. You know community engagement and co-market planning, today is an example. There is an opportunity for us to really talk about our partnerships but really highlight University of Kansas has been doing and how Internet2 has been assisting us. We anticipate full availability in the next several weeks certainly, Spring 2021. And most importantly, please contact us if you are interested in being involved or if you just want more information on the program. With that I will put this thank you slide up. I will beg you not to not
bother Mary on Internet2 stuff. So she does get too mad at me. You can reach out to her on anything community related. But you can reach out to Nick or I on any questions you have on the program going forward. As well as reach out to local Palo Alto networks rep. With that I will stop sharing and I believe we will move into questions. Mary, a question for you. This is from Sean O'Brien. No idea who that might be. [LAUGHTER] Obviously, pandemic has required major changes in the approach to security with faculty, staff and students working remotely. But services that Palo Alto office has this created demand for at your university?

>> MARY WALSH: Well, I think the biggest challenge as we retreated from campus, is, we really did not have visibility into what students, faculty and staff, how can I say this? Devices they were using, how they were accessing the network but of course there was had to come back to our network to access the LMS, enterprise systems, data, that was the concern that really prompted a lot of these conversations. As I said, we engage with Palo Alto 2019, for a border IPS. Which made us sleep a lot better at night. Then it was the next step and that opened the conversation with Hunter about the service evaluation. So, reading left to right in the bundles that Hunter shared in that last slide, we were really focused on the remote access. How we were going to manage that. This is still in the very -- stages but that is the next worry. What devices folks are using, how they're accessing you know, it was really interesting at the beginning of the pandemic. We all seem to be going down the same path. We didn't really coordinate but we had to expand the VPN, we had to provide hotspots for students, faculty and staff who didn't have access to Internet. We supplied as many laptops as much technology as we could. But at the same time, we didn't really have the control and visibility we have on campus. So, those were open to the conversation and that's what we are looking for right now.

>> HUNTER ELY: Thank you, Mary.

>> MARY WALSH: Did I answer your question, Sean?

>> HUNTER ELY: Yes, he says.

>> NICK LEWIS: Just expand, sorry, Hunter. What I just heard from Mary, like she mentioned, the community sort of seemed to be working on the same issues as well and that is what we saw across all of my other services. Trying to figure out how to resolve these challenges and how to reuse the existing things that we are ready have in place to support our challenges and then identify only the highest priority things that might be necessary to support the new challenges because of how constrained campuses are from the, putting it mildly, severe budget challenges that were driven by the pandemic. And so, campuses were not looking at new things but trying to figure out how to resolve these problems and coincidentally, it took many of the same exact approaches.

>> HUNTER ELY: I think a good follow-up is, you know, just a question to the attendees. And you can feel free to chime in in the chat. How have the events in the last year caused you to
rethink your security strategy? How are you looking at risk? I often look and say these things are all based on risk calculation because at the end of the day, we are all risk managers. But over the last year, how have you changed or rethought your security approach to deal with new risks? And so, while you are putting stuff in the chat, perhaps, we can open up to any other questions while we wait. Secure desktops as though they are laptops. They will walk out the door, yet!

>> NICK LEWIS: Everything is more mobile than you anticipated! People too. Speaker is going to safety variation of the shadow IT problem. People trying to solve a problem the desktop needs to come home with them. Solve that problem. A lack of documentation of current systems. That's interesting. One of the things that we heard early on was that hardware-based remote access solutions, traditional VPN, if you will were very difficult to scale and it was part of the reason we were allowed to Duke evaluation with Prisma Access because we could scale and that was an acute problem we saw early in the pandemic. This idea that folks are going from 200 to 5000 VPN connections. So yeah, completely understand that one.

>> HUNTER ELY: We have a question from Brett earlier about what products are universities funding necessary to do their due diligence when they use third-party SaaS solutions? You know this is a shout out to the HECVAT, if I'm reading this correctly. The HECVAT, which is a large and cumbersome thing on some days, is a very important document. We spent a lot of time working on that. And at the end of it we felt we really accomplish something because we were going through in a systemic way and answering all the questions in the document. So that you as a member of Internet2, part of this community can say this answers all the questions I have around how we do things like code and how we protect our services in the cloud, I think that the HECVAT was a huge help there. I'm pretty excited about the cloud scorecard. Going forward because I think that is going to give folks a nice quick view into comments with the cloud services are capable of and security they provide. And of course, I think when it comes to due diligence, if a product or service is on NET+ you know that due diligence has been applied to it. Obviously is a personal story real quick. When I was a customer, I needed cloud storage the very first place I looked was Internet2. Because if Internet2 vetted someone it would meet my needs it was almost no question per the price, the contract and terms, all that was great but the fact that it was an evaluated service and ready to go, I could feel comfortable buying it. That was money in the bank for me. That is the few things I would think about when I think about due diligence, particularly in higher Ed. Another question for me. I probably will not have a good answer for. Other any plans to extend the offering to include subscriptions or licenses related to the firewall? For example the (Term?) the answer is, short answer is no. There is a lot of reasons for that. But the subscriptions as they are applied to the firewall, are based upon that hardware. The long answer is I don't know. How this plays out over time, I really don't know. Mark, if you could reach out to me or your Palo Alto rep we can dig into that question. But you know again, it's about the licenses being tied to the firewall and also about potentially, enterprise agreements tied to firewalls include subscriptions. We do not want to confuse that with what we were doing with cloud services through Internet2. You can purchase them at the same time and we can make it work for you, absolutely. But the subscriptions themselves, it's a little gray in that area. I don't
want to paint a bad picture there, it's just a licensing, it's the big issue there. The services
themselves are set.

>> NICK LEWIS: To add a little more color on the complexity. There is Quitman across the
community and we know that the community has a different subscriptions, different resellers,
different support that they need. Resellers for management and implementation, things like that
for campus. We wanted to work with, within the existing scenarios that the campuses already
have. So that we can do this as streamlined as possible for a campus. If you have a reseller that
you like working with, or a partner you like working with the implement in services or doing
health checks, or things like that, we designed it to work within that situation. Where it is not
always the case because of the specific service provider but with Palo Alto, were able to do that
and provide that type of benefit, that flexibility to the community when they engage through the
NET+ Palo Alto program.

>> MARY WALSH: I would like to follow up on that, Nick. That was one of the three main
things our general counsel was focused on. Of course, the governing laws and the logos. We are
kind of particular about our logos and our names. But there was a commitment there, using
plaintext which Hunter did in this presentation. But the third thing was the constraints around
with Palo Alto, agreed to all agents and sub agents will also be constrained by. As you say,
anything, a reseller uses will have this same constraint. And it was really important to us. It was
very thoughtful, but very carefully laid out. And we appreciate it.

>> I one last question I think we can squeeze in under the wire if you're quick. What criteria do
you use in order to select Palo Alto as a partner to help with security remote access?

>> NICK LEWIS: The NET+ program works with community engagement and suggested. So
University of Nebraska and Lincoln sponsored Palo Alto as part of the NET+ service evaluation.
And then, Mary and the rest of her colleagues signed up to do the service evaluation. So that we
can do that vetting for the community. Internet2 does not, we don't take who wins or loses. We
rely on the campuses to do the service evaluation.

>> HUNTER ELY: Thank you. I will hand it back over to Jason now.

>> JASON MARTIN: Awesome, thank you so much! Thank you for joining safe and engaging
session and conversation. Before you sign up today please click on the session evaluation link.
You'll find that in the chat window. Your comments are very important to us. The sessions
recording and presentation slides will be posted to the website later today. Please feel free to
share with colleagues. Finally, please join us for the next industry and campus webinar March 16
at 1:00 PM Eastern dear about campus IT modernization. An identity journey. On behalf of
EDUCAUSE I am Jason Martin. Thank you for joining us today.