Project Completed by:

EDUCAUSE
Industry and Campus webinar: Zero Trust Strategy: Enabling the Hybrid Campus Experience
Tuesday, October 6, 2020
1:00PM- 2:00PM Eastern
Welcome to today’s Industry Trust Strategy: Enabling the Hybrid Campus Experience. This is Brian Kelly, Director of the Cybersecurity Program at EDUCAUSE, and I’ll be your moderator for today. EDUCAUSE is pleased to welcome today’s speaker, Steve Faehl. I will introduce him in just a moment, but first let me give a brief orientation on our session’s learning environment. Our virtual room or learning space is subdivided into several windows. Our presenter’s slides are now showing in the presentation window, which is the largest on the screen. The tall window on the left serves as the public chat space for all of us. You can use the chat to make comments, share resources, or to pose questions to our presenters. We will hold Q&A until the end of the presentation, but we encourage you to type your questions into the chat throughout the Webinar. If you have any audio issues, click on the link in the lower left-hand corner. And at any time, you can direct a private message to Technical Help by clicking in the top-right corner of the Chat window. A drop-down menu will appear where you can select Start Chat With and Hosts. The session recording and slides will be archived later today on the EDUCAUSE website. And now, let’s turn to today’s presentation -- Implementing Key Elements of an Effective Zero Trust strategy can ensure a smooth digital experience for higher ed institutions, whether students and faculty are on or off campus. The Zero Trust approach recommended by Microsoft can enable greater control over access to applications and data without introducing unnecessary friction to the education experience. Learn about Microsoft's own Zero Trust journey and discover how a few simple steps towards Zero Trust can make a big difference in your institution's security posture. We are delighted to be joined by Steve Faehl, US Security CTO at Microsoft. He incubates and evangelizes new security strategies to disrupt emerging Cyber threats. He focuses on proving out what approaches work best when it comes to Cyber defense tactics both to help customers accelerate their Cyber maturity and to help influence future product direction at Microsoft. He works with leading security experts from all areas of Microsoft and has unique insights into Microsoft's comprehensive approach to security and the emerging threat landscape. He works with US customers across all industries, from Education and Retail to Defense and Financial Services, partnering with them on a regular basis to ensure that Microsoft’s approach to security is based on real-world evidence. He also actively engages in Cybersecurity research projects to help advance the practice of Cyberdefense. And with that, let’s begin today’s Industry and Campus Webinar: "Zero Trust Strategy: Enabling the Hybrid Campus Experience my proliferative and the consistent experience. It doesn't matter where you are accessing services from. You always have that same service. That makes documentation similar and provides a great user exercise. We can look across both institution and personal devices in a single pane of glass. Next, built-in controls really help protect the date tau without interfering with the user exercise.

One of the case studies that I read that we'll be talking about is around the agility that they
were able to experience through a move to hybrid campus with Microsoft teams. This was an exciting case study. 56,000 students, three different campuses and help. They had help-related security needs as well and they were able to implement those using Microsoft Teams and were able to roll out a telehealth program in three days. So really exciting example of agility. I have some internal stories that I can share. One of my favorites is actually our move to Windows virtual desktop that we planned to undertake over the course of six months. We were starting -- we had things underway. We planned to roll out a couple of thousand of these over the course of six months. It we ended rolling out desktops that they could secure work from their remote devices. We did that in two days. We were able to undertake that because of the framework and the Zero Trust that we could use as a foundation. We see that our customers are able to pivot as well. This requires some ability, security is a huge enabler of that. When we have security at a point where it agile and the user can work anywhere, we enable all of these other streams and all of these other (Indiscernible) for the rest of the organization. Let's talk about what is Zero Trust? I've had the privilege of working with first as they are developing their -- with NIST. As they are developing. It's a paradigm, a way of thinking out security. In this paradigm we're focused on users, assets, resources. The second point that this makes that I think is applicable, the consent of Zero Trust can be difficult to wrap your head around in a practical sense. It's actually easier to talk about implicit trust and we can think about that through cap zero and that's the whole. So wean we think about the goals and devices there's a lot of implicit trust in your networks and security controls and we're looking to rout that out. So while Microsoft is a strategy, we actually need to look at the resource level. So moving from this to Microsoft. What does Microsoft think about Zero Trust? Based on our experience, we believe that Zero Trust is a strategy and should be woke woven in architectures, operational processes and culture. When you think of the impact of Zero Trust, it's more than just changing a network-based paradigm or more than just device. It's all of the components that you need to rule out implicit trust from. If you have implicit for your password process, you have a problem. This is place where we can reduce risk. Let's take a quick look at what it means to move from implicit trust to zero trust. So in this scenario, what we see in an implicit trust scenario, there's static policy designing access control. In a zero trust, we have dynamic policy and we don't trust the policy as is. We introduce monitoring. This is a policy that can change and there's continuous monitoring as well. If we look at the request themselves.

>> We would have unauthenticated factors. You can think about that, what is the Ip address. These are unidentified identifiers. They don't have a high level of assurance. All it takes for a threat actor to get in is land a bit of malware on an E-mail into your device and execute the code. Because of that, we can't really tell if this is traffic that should be allowed or not. And so that static policy is useful. Think of the Zero Trust paradigm, what we find is a much richer request contest actually gives you, many, many advantages when this comes to writing the policy that's appropriate and it allows you to a lot of different options to cater to the application you are trying to. We can look at the device or the data itself or the types of data. We call this the six pillars of trust. It's not that you have to implement everything with all six of those pillars, but realize that you have six opportunities to provide input to the zero trust framework. We'll take a look at
some. These examples on the next slide. The difference when it comes to the policy itself, we also look at the level of assurance around the particular identifier. If the identity is a user name, we take a look. Is this user known? Was there multi-factor authentication, are they accessing from places they accessed previously? It could be is the user’s password placed somewhere on the dark web. All of these things would introduce doubts in those factors and would help us to understand -- what degree of confidence do we have that entity is actually known. The next, is this anomy list activity? Does the user done things previously that their activities would make that they are not acting like themselves. They could be that they have an impossible travel scenario and so it is not only the relative understanding of do we know this entity, but what level of trust do we have around this? What type of risk factor do we? And then we do the calculation, is it allowed? We take a look at what data is being requested. Is it sanctioned? And answering those questions, really give us the full request context to make a much more informed decision. When it comes to permitting access, we also have a number of outputs. Anything from full access to a limited assertion where only non-sensitive data is loaded and the sensitive data is blocked. It could be we make the user go back and provide more authentication. There could be no access. And it could be that the data that we receive is so risky that we kick off remediation of. We have a full range of activities that we’re able to undertake to assure that the appropriate level of access is permitted. Let's take a look at something less abstract. Looking at how do we build? If we look at something like a learning management system or a financial aid system or creative access to production system itself, there are different levels of trust that we require. When we look at across the six pillars, we have a lot of opportunities to pick and choose, what are the metrics that will grade this particular interaction by? That's actually supposed to be medium trust. Taking a look at -- it looks like that one was missed. I will gill in the fans. For financial aid, the ones that we would pick was multi authentication used, how risky is the user’s activity? That's one of the dynamic pivots. We may not permit the user to access financial aid. Is the device that they are using compliant with policy. Is this a device that we can manage? Is it one that we can see is up to date? We may allow them to view financial information. Especially if it's a staff member, we can put these in place where we say particular users on devices. We're going to prevent information from traveling back to that device. And then ADMIN access, to the green bar and in that scenario, we're going to ask all of the gets. There are three sample questions that I think we had for each of the pillars and here they are just in plain English. I want to know if this admin has been doing something -- maybe they are copying secrets, mare they are accessing many more privileged resources than they do. Maybe they are accessing from unusual locations and staying logged in for very long log-in times. And that is assessed for what level and if there's questions I will take a piece. We're about halfway through. We'll pause here for questions.

>> There's a couple of questions. Does Microsoft use Zero Trust internally?

>> That's a great question. We have been on this journey for a long time. Although it was by different names. Microsoft has had a number of initiatives starting with the trustworthy computing where we started to route out that trust from our process and products and that led to a
lot of secure controls that we start sort of take for granted today. That was the start. After that it was -- a few years ago we undertook the very specific move to switch over our internal I.T. infrastructure to a more Zero Trust or related strategy. And we started removing VPN and making internet first and some apps internet only as well. And we used that VPN as a scoreboard. You think about the number of tasks of engineering and all of the virtual machines involved and all of the process we've been able to keep a steady drumbeat. Microsoft is 95%.

>> We're not looking to prevent collaboration or cause harm or pause. We really want to be an enabler. Moving to Zero Trust should be an enabler for the organization. Not a lock blocker. It's going to look very different for every organization. But for us, some of our projects, very, very rapidly adapted in the span of a week or two. We've had other project, that that have taken six months -- this will provide a solid roadmap. So to talk about what the rapid adoption looks like. We have a simple scenario called beyond VPN. A lot of what we are hearing in terms of security and reliability are all around VPN. We charted out a simple scenario. It can be a simple layering. It doesn't mean that you have to completely change processes. This type of interaction we've done for a very long time. But it is managed deteriorized. When we take a look at moving the user to an anywhere user, they may be inside the firewall or outside. It doesn't matter, it's going to be the same experience. We (Indiscernible) a then application for the user in this case. And that's just with Azure AD. You are probably very familiar with active directory as your AD. It's the cloud verse of that. You don't have to change the source or the resource. We're able to make that highly available when we take a look at that, we have a Zero Trust policy that gets layered on top. We're doing preauthorization. We ask all of the we can implement this design better. The central policy governs resources. In then cases, we will have resources because they don't want to miss anyone and don't want to maintain then. They give too broad of access to the users. in in 24 case. With the central policy we're able to restrain that. If we restrict this, in the central policy, the resource policy will never come into fact. Here's where the identity team and security team not only have a control point, but they have a window into what's going on. Before we didn't have Telemetry on how the items were being accessed. We can take take a look at the network data. Again, we're looking at trusted assurances before we allow connectivity and the level of access that we want to permit is very flexible. To answer the time question for that, you can roll that out in about an hour. Implementing that to make resources highly available, very, very straightforward and simple. We had a few healthcare providers that came to us a few moments ago and needed to roll out applications very quickly and key portions of their organization would actually go down and they would not be able to maintain the services that they provided. We partnered with them and had all of their applications available to hundreds of thousands of users in those cases. So the way you can roll those out, is a very simple pattern. We think more broadly about how do you roll out Zero Trust and how do you enable to secure hybrid interesting? I would take a look in phases. Everyone's journey is going to be different. That's okay. But there are some commonalities and in phase 1, you can prioritize this and monitor the portions of the strategy. Looking at things like, do we have strong authentication. Do we have centralized identity. What you can do is say, is it the same asset? We have the signal from the user but we also have the signal from the device. It was a false positive. So the ability to be able
to take a look ability those scenarios and that and know is this an asset that I managed. I know which user does manage it. Taking a look at the hybrid. Whether it is a clad resource, whether it is on premises application that's -- it doesn't matter. We want to have have a continuous Telemetry that has the same aspect to track any of these issues across the premises and finally looking at the identify monitor, discovering and register applications themselves so that we know is this an application that's been vetted and approved by the organization. Maybe you are not going to block it if not. Is this a known trusted application. It helps some of those investigations move along quickly. And you identify monitor is to reduce risk and that's around adding protection, also enabling secure methods to -- we don't want the ability to download information and maintain it on a personal device. In an investigation scenario, knowing the sensitivity of the data that's involved, if I have a lap top with a gig of sensitive information, I'm going to investigate my priority. This is a great signal, if we don't use it for full flown data -- the ability to that the sensitive data, it see the data flows to ensuring that the level of trust and we can begin to look at those flows and determine if what's going on is appropriate. And increasing protection. This is after we have the data we can step it up a match. We had registered devices now we have compliant devices you are not allowed to download personal data. This is a popular feature. It is one thing you want to enact after you have all of the data, and the final one, you have policies in many cases where you may be provided additional signals. As you enable it for enforcement so we're sure We're not going to disrupt the activity of the Users. So to give you an idea of what this let's take a look at phase one. We started off identifying the users, registering the devices and that's a great first step. We can do that from in the cloud. And that allows us to have the same identification and registration process whether the device is sitting on my network or whether the device is at Starbucks or somebody's home. You can use Windows hello and you can have Mull fi function capabilities that are very seam useful. And the -- single sign-on access from anywhere to softwares of service, cloud on premises sis app. Higher education institutions, I've been doing this a lot longer than most organizations. So probably no surprise here.

>> As you move to the zero trust strategy. And reducing risk. E-mail protection is still -- the number one trifecta for attackers. So having this protects both users and identifies. And then enable identity, we can change the authentication of a user. -- if the user becomes more risky, we can openly go ahead and layer in more control. We can enforce multifactor and all of those scenarios are possible in a dynamic way. We give the user the least frictional experience possible and that we can still reduce risk with. At the first pay if your labels are not 100%, maybe you have an 80% true POSITIVES rate. That's okay. All we're doing is looking at add quit data flows. So they important to note, this does not have to be a comprehensive program, it does not have to be comprehensive protection. You don't have to block data. Just start to label it and you will understand your path to securing data much better AT a result. The next phase, increase protection. And so enrolling personal devices, it can be a great next step. You are looking to create even more secure environments and more -- this may not be required for everyone. Enforcing data and application policies, as we take a look at your data that will tell you which ones are ready in a way that won't disrupt the users. You can add the proxy that's in the cloud, you can say what data is able to flow in. And then enforcing information protection. If you know
that information is flowing and you have the device in place that's reliable, go ahead and enforce protection on it. That's going to enforce your data. It doesn't matter if it's on a completely different, if it's put into a different cloud provider. You still maintain that around the data and are able to revoke access to it -- Access to it at any time. As we look across the six pillars, we kind of had the top (Indiscernible) connect chur look. This is really a user look. With our ArKiKi connect our add Higgs. We're able to secure to the degree. We can see with identity management and that's the first ting that the user is going to encounter to secure that experience as they -- (Indiscernible) look. This is really a user look. We're able to secure the device. We can see with the identifier. And you may have a third level of access for administrative workstations. Moving down to the applications, we look at the threat protection and application policy. We can make a policy just for teams. Look at the traffic analysis. Usage analysis that the network and the behavioral an analysis checks out fine. Sequel.

>> We have privilege the identity -- you don't have standing admin access. Still, management and protection are absolutely key. Real source policies and application policies to protect the workload are essential and then traffic analysis to ensure that something doesn't change. Threat protection and use average analysis at the workload level. In teams we had it directly in teams. If there's a malicious link or file, we can find that. On the sequel side, it's through Azure. All of the capabilities are there. We look at the framework within the six pillars. It's not about the products. It's not about the particular needs. It's about the overall strategy. What have I chosen within each of the six pillars? when we look at teams, that's something that's taken off, both within education institution and with teams university and also within the private sector around the public sector, more broadly. I was talking with a security operations center director recently and they said that teams has worked wonders for them in their D.O.D. environment. They are able to clash rate as a security team better than when they were in the conference security. So sharing intel to work on - - if you are using Azure and you consider collaborate everyone on call gets that message. That kind of immediate access and response has been phenomenal. When we look at Teams, secure it according to zero trust guidelines, it's not just about the devices. We really look across all of those elements to say do we have those sign-in policy. Is there less friction on it? We know there is a positive culture. Inside this application. That's a great benefit that can say these types of communications were concerning. We really need to protect user and sometimes it lies at the -- the consequences lie outside of I.T. itself. The ability to give someone a device that can be deployed with autopilot, comes straight from the factory, they sign in. Guiding users as we talked before with policy tips. It can be across all six pillars. So with that, take a look at protecting our assets. This is really is around only trusted people, using trustworthy sources to access apps. We have a number of solutions within these categories. We'll make this slide available to you. If you are interested in the pivots, we have the six pillars around the identities, defines, the data and the operations and Microsoft has a number of projects to help you. Plugging into that six-pillar version. What are you doing to secure your access? We have solutions for you in each respect. You may have solutions. We can operate with many of those. We have a great industry partnership and work with a lot of partners to integrate solutions. If you have a great solution that's working. Look to see how you are augment it? If you find that you have a gap, know that
we do have solutions. If you want to find out more about zero trust, near are a few things that I
would recommend. There are some events coming up. Notably three presentations that you
should be aware of. We also have some online resources. We launched our deployment center
which was put tooth in collaboration with our public sector team with our engineering teams and
the Microsoft resources. So these are very practical, we believe they will be very helpful to you.
It's brand-new. We have our particular case study from the organization. You can read more
about that. We have hybrid learning classroom resources that go beyond just the zero trust and
can help your organization more body, have a fantastic hybrid learning experience and if you
have question, sometimes people directly are the best way to get answers. Reach out to your
team. If you don't know who that is, talk to someone in procurement. They probably do. Talk to
somebody in the I.T. shop. They probably do. You did reach out to the help center where you can
reach out to us directly. I believe that's the last slides. Maybe we can answer some questions.

>> Yes, we have some questions. I think some of them were answered. We do have one -- early
on, you mentioned when a profile is created and there was a question around how the profiles
were done? Is that through A.I. or --

>> Yeah. Great question. We found a complication, we start out with the (Indiscernible),
anything we can solve that way, we do that. If it's not straightforward, we're just going to write
the rule and there's a combination that we have that do a great job. When there are attacks from
one country to another. That's something that we have a threat intelligence team and sometimes
it's just -- there are other scenarios where we'll have an A.I. model. Oftentimes we have an
ensemble and determine what the risk should be and we all vote together and they come up with
the score. And then you have the ability to choose not only what models you want to use, but you
can take a look at which roles you want to enact. It's that layer of things that you know about.

>> We have two more. The next one is -- can you use ADFS and take advantage of Azure
features or do you need to think past the hash.

>> Great technical question. Love it. You can use ADFF and still implement many of these zero
trust capabilities. Where you have a hash sync or pass-through authentication, there are some
things that you can do, such as looking for happen matches that were displayed on the dark web.
If we don't have a sync of the hash, we can't do that. But there are others you can take advantage
of. While it's not 100%, we still support that.

>> And the last question is, if we implement duo, can we use duo in conditional access policy
and for password -- instead of the authenticator.

>> Yes. If you do have our Azure directory license, but if you have that particular license, we
can use duo. You can use duo for that and use it with our authentication.

>> Okay. Perfect. With that, Steve, thank you. Before signing off, please take a look at the
session evaluation link. Your comments and feedback are very important. The session is recording and presentation will be posted to the website later today. Please feel free to share it with your colleagues and finally, please join us for our next Webinar on October 8th at 1:00 P.M. eastern to hear can, connect it, protect in a remote working environment. This is Brian Kelly. Thanks for joining us today.

End of Webinar