Before we get into the show, we want to ask you, our listeners and the SharePoint community to help us make the Intrazone the best podcast it can be. The episodes you've listened to are derived by Chris and myself coming up with what we think are good topics to discuss. The point of the show, however, is to provide insights, answers, and knowledge to our customers and partners, and in order to best plan for upcoming episodes of the Intrazone, we've created a brief survey for you to fill out. We promise it's nothing overwhelming or too time consuming. The survey is for you to tell us what you'd like to hear. Take the survey. Go to aka.ms/Intrazonesurvey. Let us know what you think. We will read everything submitted and we'll do our best to shape the show in the way that you want it to be.

Welcome to the Intrazone a show about the SharePoint intelligent intranet. I'm Mark Kashman here with my cohost, Chris McNulty.

Thank you very much. We'll also be joined today by Bill Baer, Matt Swann and Debraj Ghosh.

So in this episode we're going to focus primarily on security and compliance and we're going to be talking about it at a number of different levels. Certainly we want to paint a really broad picture of what it is that you get when you invest in Microsoft 365, and then what happens actually when you get down to the levels of SharePoint and one drive. And we're going to be talking with folks on the marketing side and hopefully at the end of the episode you're going to walk away knowing everything about security and compliance that Microsoft has to offer.

And we are pleased to have Debraj Ghosh who is pretty close to being on our same team, but you focus on a number of different things. Can you tell us a
little bit about who you are and how you got here?

Debraj Ghosh

Yeah. So my name is Debraj Ghosh, I'm a lead product marketing for Microsoft threat protection. It is a solution that we announced at Ignite this year, which really helps secure the modern workplace across different attack vectors. And we'll talk a little bit about some of the components of it I think during this podcast today. Uh, how I got here. Uh, so basically I've been in Microsoft almost two years now. Uh, I actually used to be the product marketing manager for Office 365 ATP. Before that I also worked at another security company semantic, which is obviously now one of our competitors. Um, and then I actually have a weird background. I actually started off doing science, so I used to be a material scientist. I worked in the solar industry, uh, and then I sort of switched fields and came into tech.

Mark

Nice. So you've been protecting your own secrets before he came here and now you're helping other people and you said ATP, which is advanced advanced threat protection.

Debraj Ghosh

Correct. Like, so that's keeping everybody busy. So you often talk to the security officers? I do. And they give you the tough questions. I bet. Uh, yeah, they do. I mean, most of the time or the questions that we get on the Office 365 ATP side is if we actually hear from folks sometimes it's about, hey, they want to make an investment in the service, do they actually need it? So that's usually the biggest thing is that why would I actually spend this money to actually use something like Office 365 ATP? And so we of course talk to them about some of the reasons why it's useful to have something like that. Okay.

Chris

You know, one of the things, going back to our original announcement of Microsoft 365 last year, Satya Nadella, our CEO, said something to the effect of, I love seeing marketing lead innovation, which translates as we haven't actually made the products work together and it's 18 months later and we're starting to see some of that union. I really think, you know, when we think about security and threat protection, um, when we were thinking just thinking about it an on premises terms, there is threat protection, SharePoint or threat protection for Exchange. And we've been blending all of the user services with Office 365, and now Microsoft 365. Um, how do you see that playing out with threat protection and security for a unified Microsoft 365 percent?

Debraj Ghosh

Yeah. So for example, with Microsoft threat protection, it's really, there's three main aspects of it. Uh, I think folks who are familiar with Microsoft security are familiar with the Microsoft intelligence security graph. If you're not, it's essentially a pool of signal which we have from all across all across the globe from all the different capabilities that we actually offer our customers. So there's stuff from Windows or stuff from office or stuff from Azure, uh, and it's essentially all of our security services are built off the intelligence from the Microsoft intelligence security graph and then the two that actually the three main drivers for Microsoft threat protection and what we sort of envision as the future of security and how we sort of position, uh, what we can do with security that really we think differentiates us from others is that we have this massive strength of signal, which is from the Microsoft intelligence security graph.

Debraj Ghosh

Uh, we then, to your point, can unify all of that signal. So what we can do is we can take signal from an endpoint and connected to signal from email and actually understand how they correlate and then because we can do that under, because we had that understanding, we can better secure our, our,
uh, our customers. So integration across these different types of systems is another unique differentiator for Microsoft threat protection and Microsoft security in general. And then the third piece, which I think customers are going to start seeing more and more of, they can already see some of that in Windows Defender ATP, which we have to protect endpoints is a lot of the security will become automated. So essentially this will reduce the burden on a lot of it teams. They can actually focus on more important things where we will actually automate some of the basic tasks and so they'll see more and more of this automation across an office and Azure in the coming months, uh, over the next year as well. So it's really the security services that are really driven by and supported by intelligence of which we probably have more than almost any other organization in the world, uh, this integration across these very different services, but then unifying all of that into something that's easy to understand and easy to have visibility and control over. And then this automation aspect, which is going to light up more and more.

Mark Kashman

When you say endpoints, a lot of it I think of is where is the end user, what are they logging in from? And sometimes the end user might have some male intense, so obviously understanding those patterns, but a lot of that is inside the data center, outside of the data center, what are people are looking at, what we have third parties, obviously they're reporting issues and things to watch out for and bringing that altogether. Just to unpack the security graph a little bit more. It is an intelligence service that's essentially monitoring everything that's being tweaked and learned every day. Yeah, both by humans and by the.

Debraj Ghosh

Yeah, the intelligence security graph is, like I said, that this pool of signal, all of it is obviously anonymized, so we never know where that signal is coming from. We just have that signal. Uh, and then, uh, in the intelligence security graph is something that all of our analysts have access to. So I think we have something like 3,500 security specialists within Microsoft. Uh, and so they actually analyze a lot of that signal. We actually apply a lot of our machine learning algorithms or AI onto that signal and it's essentially a sort of a feedback loop, so all the different security services, that's where some of that signal comes from, goes to the intelligence security graph where we actually make sense of that signal so we remove all the noise we get to the things that are important and then we funnel that information back into those same services so they can then protect those threats later on and who I should they come out and impact the customer.

00:07:08:00

Mark

So both with your customer hat on, you know, before you came to Microsoft with what you were doing both at semantic and before that with your science, you know, again, I'm assuming you protected some science details before they came out. Um, there is what we have put up for a long time. The trust center and within the trust center, their security compliance, privacy and transparency. From your perspective, I think, especially in the transparency side, how would you say in the last couple of years we've evolved to maybe land on what it is that our trust center in our strategy implies to our customers?

Debraj Ghosh

I think we actually are one of the most transparent organizations in the glow across the globe. So I'll give you some examples of our transparency, not just from the trust center, but how we actually try and be as transparent as possible even with our security offerings with customers, with our customers. For
example, in the world of Office 365 ATP advanced threat protection, this is basically a, a form of email security that we offer customers. Um, folks in that industry oftentimes will send out reports about how they actually measure how effective they are on catching malware and stuff. However, no one has up to, at least to our knowledge up until about a month ago had ever actually reported how they do the measurements. And so what we actually did was I wrote a blog with one of the engineers on, hey, this is how we actually take all of our measurements, uh, and we really went under the hood of what we do in Office 365, so we've never seen any other organization, at least in this space, be that transparent with the customer and saying, Hey, just so you know, this is exactly how we do these measurements.

Debraj Ghosh
When we tell you that this is what we're catching, this is how what we may miss, we let you know and we want you to know that this is how we do this stuff so that when we actually report these results will give you full. You have full disclosure on how these results were a sort of taken in.

00:08:56.00
Mark
I would make a Las Vegas bet that you get really good feedback, that you're being that transparent and open and probably pleased more and more and more.

Debraj Ghosh
Yeah. So for example, uh, just a week or two and a half ago, I actually had a customer pinged me on linkedin saying, Hey, we've been reading your blogs, were really happy with how transparent you guys are with all the things that you're talking about. We would love to actually talk to your team and learn a little bit more about all the security products that you guys have and in fact, so we connected him with one of our account reps and then we're starting that process.

Chris
So, Debraj, When we think about, you know, that broadening of the Microsoft 365 security and compliance needs, I also want to return us to our roots with SharePoint and today we're also joined by our colleague Bill Baer. Hi Bill.

Bill Baer
Hello. Thanks. Thanks for having me.

Chris
So I think we know what you do, but just let's have a quick refresher for our audience on, on who you are and what your role is here.

Bill Baer
Hi. I'm Bill Baer. I'm a product manager in our SharePoint product group, working alongside Chris and mark. I focus on security and compliance and administration and server and hybrid and migration and this little thing we call SharePoint spaces and spaces, mixed reality and office.

00:10:04.00
Chris
So over the past year and a half we've watched coming out of the EU, the EU general data protection regulation, GDPR. And GDPR imposes requirements on any organization which is handling personally identifiable data privacy data about individuals who are citizens of the EU. Um, it's a really interesting topic because it's very similar to what we watched two decades ago with Y2K, even though it relates to a very narrow slice of some organizations operations, it really can be something that infiltrates, expands and hopefully improves the whole way. Organizations approach handling private data, how they do their data processing in the first place. How do they contract, where do they keep their information and so forth. So how, how have you all seen GDPR influencing the way that we approach our product solutions?

Bill
Well, I think, I think from an influence perspective to take a more holistic view of how GDPR has influenced privacy in particular. It hasn't just been Europe,
it's actually something that's occurring more and more on a global basis and we can look to California as a great example of somebody who has adopted a GDPR like strategy in order to provide greater data protections for both citizens as well as consumers of various software products. I think from a Microsoft perspective, we have always had a keen eye towards data privacy and that's what made us well prepared for GDPR. We've always taken customer data seriously and that's one of the statements that we always make when we talk about data. We always say it's your data and the reason we say it's your data is we don't own your data. We're simply the custodians of your data and that philosophy had really accelerated our journey or our ability to respond to GDPR.

Debraj
Yeah, and I'm at a product level. For example, we've introduced several things, so we have customer lockbox, which is a great way for us to like. It's a great way for us to make sure that our customers are fully transparent in any access to their data. In fact, we can touch their data unless they actually give us that access through of the services like customer lockbox, a specifically for when the GDPR launch happen. We also released a product called compliance manager within Office 365. This actually it was a great tool that actually enabled most organizations to have an assessment of all of their different things that they have within the organization. Understanding all of those different files, all of those different users if they were compliant or not, and this is a free service that we have actually been offering for the last year and a half so any customer can go and check it out and determine where they are in terms of their compliance profile. A profile, and we sort of did all of these things as we saw GDPR coming along, but it wasn't just because of GDPR. We actually felt like these were the things that we needed to do to help our customers become more compliant in a world that actually needs to be more compliant based on all their different rules in regs.

Chris:
I feel obliged to insert here the obligatory disclaimer, None of us are lawyers or attorneys. We are not offering any legal advice. This is for novelty use only. For actual mileage, please consult an actual attorney.

00:13:03:00
Bill
I would say one thing that we probably couldn't state clear enough is that your ability to be compliant with GDPR is due to the cloud. And I think that's just probably one of the clearest statements that we can make. Having been with SharePoint seemingly forever in my career, I saw customers struggle with concepts like PCI DSS on premises and trying to meet various regulatory and governmental compliance obligations and we've made it that much easier for you.

Chris
We've kind of taken the thought out of it and have just allowed you to run your business. I think we need to take a look at, you know, especially for those of us in North America are casual understanding of GDPR. If we have one at all, it's usually the right to be forgotten to being able to go to, you know, some organization on the continent and say, Hey, I want you to get rid of anything I've ever done with you permanently. But GDPR is actually a lot more than that. And I think we probably should reflect back to the audience, the distinction between the North American common law as it relates to PII and the European common law. North America we, especially in the US we have a profound tradition of free speech and people have the right to say anything they want as long as it's factually correct. That extends to organizations and...
corporations. The EU has a very different understanding of PII and it's not a bad one. It's just a different one. Is that the data about you were you were me. Me Is always the property of me and that's irrefutable. So if I am dealing with contoso Europe and they have my address and social security number that belongs, you know, that information still belongs to me and I have a right to control how it gets used.

Bill

Well, one of my favorite parts about GDPR that we haven't mentioned is your ability to assume a pseudonym. So that way data can't be attributed to a particular data subject. And for my own purposes I'm going to be Chuck Norris. Yep. Just to throw that in there.

Chris

Well, one of the things with GDPR and officially stances, you know that regardless of what it officially stands for, it can be thought of whether you're in the EU. We're not as general data processing recommendations. And one of the things that many organizations see in that journey is where is your information? What kind of information is it? How is it classified and why do I have it in the first place? How have you seen some companies kind of responding to that?

Mark

Well, and I want to kind of pile onto that because maybe just to combine the two questions, you know, you joined just at the right time in terms of when GDPR was kind of a hot topic and then maybe now not as much when you would talk to customers both before and after. How did you their response change based on what's coming, what we did about it and now what's in place?

Debraj

Yeah, so I think before GDPR, I think a lot of customers, and if this is going back to your y two k analogy, I think a lot of customers were very, very worried about what it would have as an impact to their organization. I actually think especially when in the EBC they actually felt like Microsoft not only was providing them with products, but Microsoft as an organization is, is one of the largest organizations in the world. We're obviously all over the globe. We actually had to deal with all the same things that all of these customers we were talking to had to deal with. Um, and so they actually almost looked to us as consultants about how are we doing this as well, um, and not only how are we doing it, but then also having the products that we could surface that could help those customers go through that same journey.

Debraj

And so I think that nowadays when I have that conversation, like we don't really have that topic of GDPR as often, obviously just because that first wave has already happened. Like people sort of have realized, okay, my business closed down, but I am like getting adjusted to this new norm. I do think they still are asking like, Hey, are all of your, all, are all of your capabilities GDPR compliant? How has Microsoft enabled that to happen? And I think if you look at industry, any sort of reading industry reports or even talked to other colleagues within the space, uh, you'll find that Microsoft actually took a very strong leadership role as GDPR was rolling out. And I think we're actually a not only just ahead of the game, we're actually an organization that other organizations sort of look to in terms of, hey, this is how they went through this process and this is what possibly the path, this is possibly the path that we should also take.

Debraj

So I think the conversation has gone from customers being like, oh my gosh, what are you guys doing for GDPR? Not only the, what are you guys offering
us, but what are you guys actually doing yourselves to now? Like, oh, okay, so you guys actually have all these capabilities that are GDPR compliant. Now tell us how you guys went through this process so that we can sort of follow suit and make sure that we, uh, also fall, follow the guidelines.

Chris

I think we need to kind of reflect back under article four Microsoft is officially defined as a contract data processor. And so that means that customers come to us and we handle some of but not all the roles. And so there is an obligation. One of the nice things about the GDPR, if nice is the best way to describe it, is it really sets up a framework for the organizations who contract with us to handle their data. It makes clear what their responsibilities are and some of that relates to security and breached notification. How do you see the need for. One of the things that GDPR says under articles 32 to 34 is if there’s a security breach, you need to be a proving that you’ve taken measures to detect and contain it and b, if something is breached, you’re notifying people. How do you see our tools helping in that?

Debraj

Yeah, so our tools are right now working towards a more capabilities that will help with the breach notification. So we, we obviously have tools in place. Insecurity that actually will let and let you know if you have been reached in terms of the breach notification piece. We actually have our own services internally that will reach out to the Admin for that organization and let them know that, hey, we saw that this has happened. A unique to actually address this as quickly as possible and obviously with GDPR, I think you have a 48 hour window in order to make sure that that are reported, so we actually try and make sure that we, as soon as we hear about it and we let a customer know that hey, there has been this breach that’s occurred and you need to take these following steps and then essentially though we still actually have, there is that responsibility of the customer to follow through with those steps once we let them know that there has been a breach.

Bill

I have to commend you both on using the word breached versus hacked. It’s a very good reason for that term. Breached versus hacked. Would you like to expand on that a tier? The versus definitely no. Breach breach does a legal definition. That's what you want to be able to say. You never want to be able to say you've been hacked. Hacked has a completely different definition and a different set of responsibilities and actions need to be taken place. When you say hacked, I was just. I was just surprised that you both had used breached.

Chris

You know from the GDPR is the idea of data integrity both within the customer and geographically, um, how do we approach the idea of data sovereignty and being able to, you know, the, the GDPR says that you can't allow transfer of personal information outside of the eurozone without certain things happening. How do we help drive that protection?

Bill

I think, I think the answer there is pretty simple, Multi Geo. And that has been a critical investment for us as well as a critical differentiator when you just look at the services that we offer, whether it's multi Geo, one drive for business, whether it's multi geo, upcoming with SharePoint, whether it's multi Geo with exchange, we have a set of capabilities that can help you isolate your data to a specific geography. So effectively you're working under the premise of a single tenant that spans multiple data regions and then the data itself is isolated to those regions. In the case of one drive and exchange, it's more or less a one to one relationship between the user and the service. A user has a singular
relationship or affinity to one drive. A user has a singular relationship to a mailbox, whereas with concepts such as SharePoint, it's one to many, many to one and even in those cases we can do multi Geo because in a data residency scenario, really what you're looking at is data residency itself, not necessarily the runtime and that's what enables SharePoint to work as well.

Mark
So a lot of what we've been talking about today is the investments that we make for everybody, regional data centers, huge investment of course, that we do GDPR to get compliant with that before the date reached. We beat the deadline. We're now set for that. But there's a lot of additional tooling like DLP and we'll talk about DRM and just governance in general of choices that customers can then make to make themselves more secure, maybe not for everything that they do, but if there's a specific project, campaign set of documents, the document center that has to play by different rules or be treated that not everybody there is going to know what all those rules are. So to protect themselves. Um, so you know, you're short definition of DLP and I'd love to throw it to build a c. How does that apply for SharePoint?

Chris
I want to ask both of both of you, what does the “p” stand for and DLP according to you?

00:21:40:00 Bill
Prevention and why? Well, that's exactly what it is. It's, it's, it's not the ps not necessarily actionable. It's not, it's not a reaction. It's effectively an action that you don't need to take. Prevention is, is protecting yourself in advance of any kind of potential leakage or a loss.

Mark
And it can be a soft prevention. Hey user, you're on a site that has specific materials that it needs to be treated in x, y way or actually blocks actions, you know, you try to put an attachment to a document that's coming from a zone that has some policies, is head to it and attach.

Debraj
Yeah, I mean I, I think it's prevention for me as well, and I basically look at it as sort of the product I manage is basically trying to protect you from letting bad things in. And dlp is tell you, trying to prevent you from letting good things out. So it's basically the high level of the way I look at it. So prevention is the,

Chris
I think it's important to understand that these are tools that um, there is no absolute protection, no guarantee that if you click this box, you're hundred percent guarantee that this will never happen.

Debraj
And that's why in our world for threat protection, we always talk about protect, detect, and respond or detect and respond is just as important as protecting.

Bill
Part of prevention is classification. There is, there's effectively this discovery piece. You can't, you can't prevent loss of something that you don't know that you have, and that's probably one of the most important steps is identifying what you have so you can protect the good information from leaving the system, but you have to first identify the good information. That's where we've made investments through sensitive information types, uh, and, and other policies that you can configure inside of SharePo

Mark
nt in order to do that.

Debraj
And that's why in our world for threat protection, we always talk about protect, detect, and respond or detect and respond is just as important as protecting.

Bill
Part of prevention is classification. There is, there's effectively this discovery piece. You can't, you can't prevent loss of something that you don't know that you have, and that's probably one of the most important steps is identifying what you have so you can protect the good information from leaving the system, but you have to first identify the good information. That's where we've made investments through sensitive information types, uh, and, and other policies that you can configure inside of SharePo

Mark
nt in order to do that.

Bill
Part of prevention is classification. There is, there's effectively this discovery piece. You can't, you can't prevent loss of something that you don't know that you have, and that's probably one of the most important steps is identifying what you have so you can protect the good information from leaving the system, but you have to first identify the good information. That's where we've made investments through sensitive information types, uh, and, and other policies that you can configure inside of SharePo

Mark
nt in order to do that.

Bill
Part of prevention is classification. There is, there's effectively this discovery piece. You can't, you can't prevent loss of something that you don't know that you have, and that's probably one of the most important steps is identifying what you have so you can protect the good information from leaving the system, but you have to first identify the good information. That's where we've made investments through sensitive information types, uh, and, and other policies that you can configure inside of SharePo

Mark
nt in order to do that.
Bill labels, labels, labels, labels. Yeah, so the more labels

Mark Tell us a bit more about labels, it's a recent announcement for us, so maybe a lot of people aren't fluent on it. Give us a little sense of what it is and, and how that'll be nice tool in the toolkit

Bill I mean a broad viewer labels as effectively. There's two types. There's sensitivity and there's retention and each serves its own purpose now and in the conversation that we're having about protection of data, that's where you want to look more on the sensitivity side. And again, it's identifying that set of information that's critical to your business or could cause your business substantial loss if it leaves the boundaries of the system and that's where you apply your sensitivity levels. You're sensitive labels can protect your data and inform your users. And that's probably one of the most important pieces is that user education piece. Um, you know, you don't want to make labels something that are so abstract that users don't have visibility. You want to provide that visibility so they understand the nature of the data that they're working with. It helps educate them, which is one way to prevent the loss of information. And then, and then secondarily can apply policies in order to help prevent that too. So you have kind of two ways to do it. There's the programmatic aspect, but there's also just the user education aspect, which is important.

Mark So one of the things that we wanted to get to is, we kind of jumped into, one of the things we announced recently was to just, you know, since we have you here in the studio to ask you what is new, what's the most new thing that we're doing GDPR, you know, is in our rear view mirror and will always focus on it and meet that complaints along with all the other certifications and different things that we've been offering. We'll also just get better or we'll add some new features and functionality, but I'm gonna throw to Debraj first just to talk about whether it's just been announced or something that's just landed in the service that's new. What can you share with us?

Debraj So for example, Microsoft Rep protection was just announced at Ignite. Essentially, as I mentioned, it is our way of securing the modern workplace. The way we look at Microsoft threat protection is that in the modern workplace, there's several different attack vectors. I think one of the things that people have thought about insecurity for many, many years is that email is always the way that someone comes in and attacks you. Uh, what we found out is that's not always true. There's many different ways that someone can attack you. And so Microsoft threat protection actually has solutions that help protect your credentials. It helps protect your machines, so your end points, it helps protect everything in your email and your documents. It helps protect all your cloud apps and it also helps protect all your infrastructure. Some of the new things that are lighting up for Microsoft threat, a threat protection is the new Microsoft 365 security and compliance center.

Debraj Customers will start seeing aspects of that in January. Of course, it's gonna be a journey like everything is at Microsoft. It's gonna. You're gonna see more and more features roll out. But the first set of features was going to start rolling out this January, people are also going to start seeing more automation and all of our different services. So they'll actually see capabilities where we do automatic remediation. Um, so for example, right now in Office 365, and since we're talking to the SharePoint crowd, uh, many of you may already know Office 365 ATP actually helps a secure files in SharePoint. So we detonate
files and we make sure that they're not bad. Um, we're now actually adding services across Office 365 where we will actually take automated remediation function. So for example, if someone clicks on something and we find out that it's bad, that's going to trigger an entire investigation path and we're going to see more and more of those types of capabilities.

Debraj In fact, they'll start seeing that in Microsoft threat protection starting in January as well. So you'll start seeing this unified console, which is the Microsoft 365 security and compliance center. From there, you can surface signal from all those different services that you have. So if you have stuff in Azure and office windows, all of it comes in one place and you can actually control it and have visibility across all of that in one place and then we'll also see more and more of that automation in terms of each of those different services, uh, so that you can become more secure and it, you actually have reduction of that burden of trying to map everything out and sort of keeping an eye on everything.

Mark This is what I like about ATP is it may have started in zone, like email, and then certainly what we offer to our customers primarily stays, is not just a workload. Do you get a lot of stuff when you invest it? Office 365 lever. If you go up to Microsoft three, six, five, and I think the beauty of that that people should know is then that's a ton of learning. We've got a ton of intelligence from what happens in email. Exactly. We're now adding a ton of intelligence across workloads, content types, teams, just different teams that are now mind sharing what we do, and I think may or may not say this as the most true statement, but I think of it as a very true statement that security is one of the biggest, best integrated offerings that we offered out to our customers that we think about securely, holistically. We think about it obviously across the different vectors.

Debraj If you think about it once again, Microsoft being size and scale as we are as an organization. Our greatest testbed oftentimes is ourselves. So when we actually talk about all these different services that are working together, our own IT teams are actually using these things. And uh, this is basically they're using these things for a multiyear organization with over 100,000 employees across the globe and enabling that security for an organization of that size and scale. And so when you think about that, if it performs at Microsoft and it does the things that we believe all these security capabilities can do, then obviously it's something that our customers can also then leverage. And sort of use.

Chris So when we think about build the future of what we're doing and what we're supporting both internally and with the product, what are some of the things that our customers should be looking for that we've announced recently?

Bill I think one of the big things that they should be looking for is there's a number of items that we've been working on. Um, one of my favorite items is less to do with security, but I'll get to that here in a minute is, you know, obviously I work on mixed reality in SharePoint. That's been big for us. One of the things I'd like to announce today on the zone is we're actually working on a new concept now to when you open a new document, you get the new car smell. It's going to be amazing.

Chris / Mark That aside, I was wondering where you're going with that man. That's just virtual smell vision.

Bill Probably. Probably one of the most exciting things is a site classification labels
at the surface. That doesn't sound exciting in the. To the extent that labels have existed in Office 365 for a good period of time, but you know, labels have always been something that have applied uniquely to content itself. And if you had a SharePoint site, you were, you really had to be deliberate about labeling the content that resided within that site to apply those sensitivity policies to it to protect your information, whether that's, um, you know, industry regulations or your own internal corporate compliance. And with SharePoint site classification labels, we've really simplified it and effectively taken it up a level. So now you're not applying labels to those subordinate objects. You're actually have that ability to apply labels to the container itself, to the SharePoint site, to the Office 365 group, and then have that policy cascade down throughout that content.

Bill
And that's probably a fundamental investment of ours because we know how organizations are using SharePoint. You generally have a marketing site, uh, you may have a legal and corporate affairs site, you may have a research and development site and you want to protect that information in a number of different ways and established policies to secure that information in a number of different ways. So really what we're enabling you did you to do is use the, the security and compliance center to create those policies and apply that label at that site level and protect its information holistically. So that's probably one of the more exciting investments, label analytics, again, as another one to help you understand how labels are being used across your organization. And I know you have experienced as well, Chris had label analytics.

Chris
Yeah, I do think that that's really important and exciting. There's another security announcement. We made it ignite, um, for some of our advanced customers about auditing. We haven't spoken much about auditing, but you know, you think about the continuous cycle of you establish a policy or you're looking at behaviors and you set controls around it. You'd want to go back and be able to get the full audit trail to see how effective you are to continue with dancing. That policy. And I believe we've extended our audit log period by about 400 percent, right?

Bill
Well. So. And that's been another critical ask of customers is many of our customers from an audit perspective, we're, we're dumping the audit logs after a period of time, so we give you the capacity to be able to take those as a blob and ingest them into your own systems on premise. And many of our customers were doing that as a process in order to, uh, for audit log preservation purposes, they wanted to retain a much greater period of audit logs then we had provided in the past and that effectively 400 percent increase really gives them the ability to sustain their audit logs inside of the system itself.

Bill
So yeah, to answer your question and brief auditing is fundamental to your security and compliance practices and an organization and the more data that we can give you, the more successful you'll be from just understanding how information is being used both inside as well as outside of your organization.

00:32:40:00 Mark
And Debraj, as you mentioned earlier, obviously Microsoft being one of our own largest customers and we of course put a lot of information around what other customers are doing and I just was going to read a quote from one of our customers a Good Year. This is from their chief information officer, our legal department, risk management group and human resources organization.
Thoroughly reviewed our options to make sure the system we chose would support continuous adherence to all of our requirements like other global companies. We must comply with other local regulations. Office 365 gives us confidence that we can remain in compliance from a data privacy and security standpoint. And that's Sherry Neubert from Goodyear tire and rubber company. Bill, I know this is your case study. Any couple of thoughts on, beyond what Sherry's saying here, what good year, uh, the benefits that they're seeing from security and compliance.

Bill

I think Goodyear, Goodyear represents a great example of a customer who was looking across a variety of different systems to meet their business needs and their objectives. And they made a choice based on our ability to secure and protect their content. And I think that's an important statement as important statement that can be made. Many of many customers will look towards capability sets. Can I synchronize content? Do I get a hub site, do I get a comm site? How extensible is the system? But it's, it's a really great show when a customer chooses an environment based on its ability to secure and protect their content and that's kind of, you know, representing their fundamental decision as to why they made a choice and that, you know, statement couldn't come across any louder as to, you know, how secure Office 365 is.

Mark

So I think Goodyear represents obviously a big voice obviously with the focus of why they chose to go to the cloud. And of course as a us, as their vendor. Microsoft I know has a lot of information out on the IT showcase, which will put a link out specifically. They've got some segments that they shared around what we do around security. Um, I think January is a really just around the corner coming up. Um, I know there'll be able to use some simple urls like security.Microsoft.com compliance.Microsoft.com and that'll take them into the new security and compliance center. There's a lot of things that people can do to review what do you get, what do you have, what state am I in? And I actually think that there's some guidance to help them further protect different zones based on what we have available to them to make change in control. Um, but just to wrap up, when people want to learn a little bit more about what we offer at the broadest level, security and compliance or where would we send them?

Debraj

So they can go to the Microsoft secure website. Uh, and if you go to that website that actually talks a lot about all the different security capabilities.

Mark

And on twitter if people are going to follow the latest announcements, whether you're active or not, uh, if you want to share how people can get ahold of you.

Debraj Ghosh

If people want to get ahold of me on a, I guess twitter. What is my handle? I got it here. Go ahead. DebrajG_78 underscore seven Eight. There you go. I'm guessing I know how old you are now.

Chris

So Bill, where can our audience go to learn more about what we're doing with security and compliance through SharePoint

Bill

The good news is we have a dedicated security and compliance center for SharePoint and one drive you can go to Aka.ms/SharePoint-security. That'll take you to our resource center on the Microsoft technical community. You can find a ton of security and compliance resources there. We have a monthly monthly newsletter that we publish each month that'll help you understand
from a roadmap perspective what shipping, what has shipped into which ring, so you can best take advantage of new capabilities that are coming to the service. We also have case studies such as the Goodyear case study. We have some demonstrations, so if you want to get hands on with security and compliance, we have some great demonstrations and then we also have some materials that you can download. So kind of your one stop shop for SharePoint one drive if you want to keep up with me and my, a team and Chuck Norris references. You can follow me at, @WilliamBaer. My parents had a bout of dyslexia when I was born, so that's William Baer.

Mark

Thank you very much for your time Debraj, for coming in and sharing a little bit more about what you do and certainly what we offer our customers. Bill, same. Thank you for coming to the show. I'm hope you both stick around for FAQ at the end. Uh, and with that, thank you very much. Thank you.

#3

GUEST PERSPECTIVE – MATT SWANN

I'm very pleased to have this next guest, not only in the studio but just on the team in general. It's a, it's a relief to me to thinking through how safe of our customers. It's like, oh, Matt Swann's there. Oh no problem.

Matt Swann

Thank you. I've been at Microsoft for 14 years and I've had the pleasure of working with SharePoint and SharePoint online pretty much my entire career. So I've gotten to grow up with other leaders in the organization. I've gotten to see their, you know, integrity and transparency and the way that they take protecting customer data seriously, kind of from day one. So, uh, it was a real pleasure to have you raised in that environment, you know, essentially as an engineer, um, and then get to turn that around and serve our customers.

Chris

You know, one of the things I really want to explore today is, you know, what security means at planet scales. We like to say sometimes, because I remember my first SharePoint 2001 server, I had a password protected screensaver audit, but I mean obviously we need a little bit more than that. When we do this in the cloud, what does that kind of security scale mean to you? How do we achieve that?

Matt Swann

Great question. So we have over 250,000 virtual and physical machines and these are distributed across data centers all around the world. So at that scale, our traditional it management techniques no longer apply, right? If you want to do apply a patch or run a query across every machine, you can't for each across each one of those machines and expect that to finish, there's going to be machines that are rebooting machines that just came online, machines that are misconfigured somehow. And so our job is to kind of invert that scenario and find a way to distribute the work in parallel in a way that's resilient to reboots a resilient to new machines coming online. And so solving security challenges that that scale is my team's core competency.

Mark

So we talked in a previous episode about data centers and certainly there are data centers around the world. There are hundreds, thousands, hundreds of
thousands of machine, whatever that number is. It's a huge, massive scale. And they really talked about it, this hyper scale. So security at hyperscale, you know, we touched on it a little bit in the intro of the show with the brush and bill around how security is course always on the lookout and there's this intelligence on the back end. But when you think of that at scale, what are the best benefits if we do at scale, right? What are the benefits that come back from doing security at scale properly?

Matt Swann

So one of the things that I like about doing security at scale is that each time we make an innovation or we find something new, a better way to protect customers or the data that they've entrusted to us, it accrues to everyone whether you are a small business or the largest enterprise as part of Office 365. And so you can almost think of it as a continuous improvement program where every month, every week we are making things stronger. And our commitment is to do that in a way that scales. So it's not something that we only apply to, you know, customers in a certain market segment. And we protect every customer's data equally.

Mark

A lot of times when you talk about these topics, uh, you know, at our executive briefing center of the people that come there often are Fortune 500 larger customers that are going to spend a couple of days with us. And they go across a lot of topics. Obviously security is always top of mind. But when you go to some of the regional events, some of the local events, a lot of those folks that come or come from smaller companies and they ask a lot of questions, do I get this, do I get that? And the best to answer, which is what you just gave is yes, you know, you are just as secure as we can make the Fortune 500, you know, you're 50 Pearson, 10 people, five people, whatever the number, same rules apply.

Chris

But I want to keep going back to scale because I think back to something, you know, one of the first ceos I worked for back in Boston 20 plus years ago gave me some advice. He said, given a sufficiently large workforce and sufficient amount of time, someone will eventually try everything. And he was thinking in the HR perspective, but I think that's really true in security. Like eventually just about every exploit is going to be seen somewhere, isn't it?

Matt Swann

That's a really good. That's a really good point. You're right. That had large scale. The long tail happens, right? So if something happens one out of 100,000 times, well it's going to happen two times a day and in our fleet, so we'll get a chance to see it and react to it and build processes and systems around it. I also liked the customer perspective because if you're in a cloud where you have very large, maybe demanding or heavily regulated customers, their needs become part of our requirements which means for every other customer on that same infrastructure, on that same service, they're getting that same protection. So as our external market pressures or external customers ask us to be ever more rigorous and find and close more vulnerabilities and and be more rigorous, really fat accrues to everyone.

Chris

I remember seeing the way that we described under a prior regime for European data, safe harbor acts and like when we explained yes, we will enact this for you because we're already enacting it for everyone else. And I think that that's just, you know, a rising tide lifts all boats. I want to jump ahead a little bit with that level of scale. It really gets into statistical significance and materiality and that's a place where a machine learning and ai can really start
coming together like how do you see the intersection of we have massive scale. The cloud is growing at exponential rates. How do we use machine learning and artificial intelligence as a scale engine for that?

Matt Swann  
Great question. We have a couple of secret weapons that we use to our advantage. They're not going to be secret if you talk about how that's been fully disclosed weapons. The first is that the engineers who run the product, SharePoint online are the engineers who build and monitor the service for intrusion detection, so we have all the context that we need about how the service is designed to run, what changes are occurring and how the fleet is changing, what new features we're rolling out. And second, our fleet is deployed in a way that is almost completely homogeneous, so across 200 to 300,000 machines, they all look the same. And so even if I don't have a SPEC that says that each machine is supposed to be configured this way with these registry keys, if I ever see any deviation across the fleet, I know that that's an anomaly that could be security impacting that I should dig into.

Chris  
And what's interesting, I remember prior to joining Microsoft, we at MVP summit had a briefing where someone came in and was talking about how we run the service and you know from the outside you would think that there's an alarm bell that goes off and immediately someone goes running into the data center, they find thus server, they log in and they fix it. And that's not actually the approach that we see in terms of anomalies, is it?

00:43:20.00 Matt Swann  
That's right. So our team's job is to abstract away the scale that we operate at and make it feel like you're responding to an intrusion or an incident on just one machine. And so all of the tools that we build to collect process memory dumps to investigate servers to collect the state of the server or ask questions about the fleet, hey, who has process x or who has these bytes in memory or these files on disk, they operate the same way whether you're asking that as a question of one machine or have the entire fleet and automation is probably a big part of that as well. Automation is a huge part of that. So wherever possible our goal is that when an alarm or an alert occurs, all of the investigation actions that we would perform as humans are triggered automatically. So rather than our job being to run tools, our job is to evaluate the output of those tools and make decisions about impact. And so that helps us get closer to our commitment of interdicting and disrupting any kind of attack before it ever reaches customer data.

Chris  
And if you see something that's interesting like it philosophically, if you see something happening, when do you allow it to happen to learn from it as opposed to not allowing it to happen?

Matt Swann  
I love that question. One of the things, the rubrics that we use to decide whether to take action or not is how close that adversary behavior or that anomalous behavior is to impacting customer data. Right? If we see activity impacting customer data, destroying data, taking data out of the data center, we're going to cut that off immediately, even if we haven't investigated the rest of the scope yet. But if we see an intrusion maybe at the beginning phases and the adversary has not gotten access to customer data yet, we're going to spend that time determining how he got in, what he's doing next, what he knows, what he doesn't know, and we're going to take steps to disrupt him or deceive him or slow down his access while we finish that investigation.
And I remember seeing a statistic, um, back when I worked principally in cybersecurity for a couple of years, that the average on premises system, the length of time between the initiation of a breach and awareness and disclosure was, is massive. It's something on the order of not nine months. Um, that's not something that we would typically allow to persist that long is it?

That's right. That's right. Our goal is detection from initial foothold of an intrusion, uh, within an hour and disruption and eviction within 24.

And uh, let me, let me keep going with this because this is a really fascinating topic. So you gather all this data, it helps us govern the service, but there's also, I'm not just our obligations to single customers, but to all do you have a point of intersection with our cybersecurity prevention centers that we run here at Microsoft?

I don't actually see we trade threat intelligence a little bit, but that's mostly through Microsoft's threat intelligence center that collects ios indications of compromise or things that are external. Customers are seeing that we need to educate ourselves,

but it, it's, it is fair to say that there is a separate entity within Microsoft that's available for ourselves, for our partners, for, for governmental organizations to all work on the much bigger global question of cybersecurity.

Ah, I see what you're asking. That is certainly true. Yes.

So one tactic that I've always loved and, and I'll be honest, you probably were doing it before I became aware of it, but you did a talk online and I will definitely put this link in the show notes because it's a really fascinating, not only topic with the way that you structure through it, um, but at the blue hat conference in 2017, you shared this tactic that your team does and just to put a little context to it, I'm going to use my best agent Smith from the Matrix Voice Mr. Swann. So you give a talk and a lot of what you focus on is this value of the red team blue team. Do you take the red pill? Do you take the blue pill? Um, and I really love the talk in terms of how it unpacks what you really do in terms of tactics and almost like war games on ourselves to better learn to better guide and coach. But share a little bit with, with us a little bit about the red team blue team approach that you guys do.

Absolutely. I love the red team. So their job is to tell us the truth about ourselves even when it hurts. So this is a set of full time engineers that are within our organization and we operate with full disclosure, you know, we give them all of our source code, they know where our design docs are, they talk to our engineers, they collect information over time as they learn things about the service and what's weak and what's strong. And their job is twofold. First, it's to find unknown unknown vulnerabilities that put customer data at risk that we didn't know about yet, so that we can find and fix those as quickly as possible. And second, their job is to simulate an intrusion so that we can proactively detect and respond and kind of. I like to think about them like a personal trainer, right? Their job is to exercise us so that we grow stronger so that whatever competition we're going to be faced with in the future, we can win.

You know, I had a personal intersection with that about two years ago. I went to a red team briefing about virtual machines security and one of the things in the presentation was, you know, some of the most doesn't, the doesn't most frequently used and known passwords that you should never put on a vm. One
of which I wrote down as a reminder, the password I wrote down, never use this password. Onenote stored in one drive and it was pretty soon thereafter that I got to flag that like you have a known bad password in this file.

Mark

So we also internally something we're actually thought you were just going to pop out at the very end and say that, ah, this has been a production by Matt Swann. But for our FYA 19 standards of business conduct course, which we all have to take. And uh, usually it's pretty simple listening and, and kind of fun. But this year they ratchet it up to like Netflix series style. But at the end the outcome was essentially there was a red team doing their thing all the while through as a viewer. Up until that point, you thought it was really malintent and people from the outside. But it turned out that they were just running these exercises. Great, great series. Just as an employee of Microsoft. That was a great way to spend a required couple, about a half an hour. But when you see that, I know you've seen the video, I could just assume that and Chris, you've seen it as well. Um, how did that relate to, you know, basically, uh, maybe even representing the red team and what they do.

Matt Swann

I loved the twist at the end, right? Finding out that the adversary is actually an employee at Microsoft, working on Microsoft's behalf, right? Doing sanctioned activities for the good of the customer and for the good of Microsoft, I think that video really captured a red teaming at its best where you put yourself in your adversaries persona, you learn how he or she works. You use their tools, their techniques, their practices, and you as closely as possible resemble that adversary on the Microsoft network. Because if we can detect and respond to that simulated adversary, that gives us a proxy for how we will perform when that adversary is really on the network. And there's such an element of fun to it too, right? How often do you get to break in and be the bad guy and you know, poke holes and try to disrupt things?

Mark

I think they saw your, I think they saw your talk and then thought, we've got this great idea for next year. So hopefully you got some consultation fees.

Chris

As mark knows my secret wishes to eventually turn this entire thing into sports talk radio in NFL football, there is something that not every NFL team has is called the scout team. And their job is to study the tendencies of the team they're going to play next. And so in practice, the scout team are usually the second or third string squad. They're job is to simulate, you know, whoever the Patriots or whatever team are going to be playing next. See I have to throw the new. And I like it. I like it. Um, and when you talk to the players about it, they say it's one of their most, in some ways the most fun things. Like, you know, we're going to be playing against Aaron Rodgers, the packers. So your job is to act like Aaron Rogers for a week. It must be kind of fun to be on the red team. That's exactly right. Yeah.

Mark

Is there also, you know, after the red team does their, their deviance without any effect to have a debrief and to have, you know, the hey, here's what we aim to do, here's how you came about it, you know, that sort of. And that must be just an ongoing learning conversation.

Matt Swann

Our perspective on that has evolved over time. When Red Team was first introduced into Office 365, it felt very adversarial, not because the red team's attitude was wrong, but because the blue team was afraid that it would be perceived as a test writer, as a quiz that we'd pass or fail over time. What we realized was that, you know, the red team is giving us the most valuable
perspective that we could possibly have. And so really we should work with them both ahead of time and after the fact to maximize how much we learn. And so some things that changed. We call this going purple, right? Red plus blue together, so ahead of time, we work with a red team and tell them, here are some areas that we think might be weak that we would love for you to exercise. Here are some capabilities that we’ve built recently. We’d like to test those against you.

Matt Swann

Here are some areas where we’ve been weak in the past that we’ve bolstered. I’d like to know whether that’s getting better and then after the fact, right, if we maybe we see them trying to get some work done and it’s not working for whatever reason, we’ll help them craft their exploit in a way that more successful because if we stop them or they can’t get in or they are confused, then we’re not really maximizing the value that we’re getting out of that time. And then you’re right after the fact. We get a full writeup. We get defects, vulnerabilities, uh, advice from the red team about things we could have done to either slow them down, disrupt them, prevent them from getting into the first place. So that’s a goldmine of new work.

Chris

When I hear you talk about that, what’s interesting is when we’re looking at the things that we can detect in the service, do we ever discover another red team at a customer organization that’s trying to test our, what’s going on out there?

Matt Swann

Often, Microsoft does an exercise called that we call one hunt, so cross Microsoft red blue engagement where we get all the blue teams together. We get all the red teams together and we do a hunt across all of our Microsoft networks, whether that’s 65 or azure or our corporate network simulating adversaries and seeing how quickly we can find them and detect them and disrupt them. Oftentimes because of the heightened watch and the additional scrutiny that we’re applying to our networks. We do find other red teams at the, at the, at the company in the middle of their engagement that happened to overlap with, uh, with 100. Interesting. That gives us some confidence, right? That are detections are working

Mark

Nice. I love, I love that. It makes us, you know, you’re, you’re doing these very tactical, very human things, but at the same time we’re really building this data model in this inner intelligence arm and that the two together obviously work in concert and you learn from one and he sometimes build the rules into the other, which is I think fascinating. Um, we had talked earlier a little bit around lockbox and I think we got a definition of what is lockbox. Maybe we’ll start there just for the sake of it. It is sometimes a new concept. I want to know how locked box comes into when you think of it, is that a tool for our customers and in context with what your team offers and what you do, how do you describe lockbox and in certainly the benefit that you see from your perspective?

Matt Swann

Yeah. I love customer lockbox. So the way I described that feature is customer lockbox puts our customers in the approval workflow so that in the exceedingly rare instance when a Microsoft engineer needs access to a customer’s contents, that customer gets to approve or deny that workflow. This is exceedingly rare occurrence because we’ve designed the service in such a way that we can operate it, we can provision new machines, we can split customers from one database to another all without ever having an engineer directly interact with their contents. Um, and it’s more than just a policy, right? We’ve actually designed the service so that no engineer has the ability to
directly access content and then we monitor their access, whether that's an
engineer, you know, maybe trying to find a new way to access content or
bypassing an existing control. We applied the same monitoring there that we
do for intrusion detection, looking for an external adversary. And if we see
something we reach out, if we see a vulnerability, we go patch it.

Chris

So for the security colorblind in our audience, can you just talk a little bit about
what it means, what is a white hat, what is a black hat, and what is the blue
hat?

Matt Swann

Great question. A white hat is someone who has the talent, the skills, the
techniques to find security vulnerabilities in a service or a system, and he
reports those vulnerabilities to the owner of the system for the purposes of
making that system better, right? He's focused on an outcome that is positive,
a black hat as someone who has those same skills, the same talents, but uses
them to gain unauthorized access to customer data or to harm a service, right?
He's doing something with malicious intent. A blue hat is a conference that
Microsoft runs. It's Microsoft engineers who are insecurity professions or
they're passionate about security even though maybe it's not their day job. Uh,
and we gathered experts from around the world, from other security
conferences and from inside of Microsoft to educate our engineers and help
them better protect customer data.

Chris

Great. Thanks. So Matt, where can people go to learn more about you and
your team and what you do for Office 365?

Matt Swann

Great question. We've given a couple of talks, right? I think Mark mentioned
our talk defending the cloud at Ignite 2018, we gave a talk at Blue Hat Israel in
2017, also called defending the cloud and that was a 45 minute deep dive just
on our strategy and our journey to build intrusion detection and incident
response. We also did a um, a talk called incident response at scale here at
blue hat in 2018 and that was focused on how we abstract away the massive
scale of our data center so that our engineers can detect, interdict, investigate,
and respond whether they're working on one machine or one hundreds of
thousands of machines. And then for more kind of ongoing information, we
publish on the Office 365 security blog and you can find me on twitter at
@MSwannMicrosoft.

#4

FAQs

TRANSITION

00:56:45:00

Mark

So with this topic, I think it's actually a really great time to hear what other
people have as their frequently asked question. I'm going to be in learning
mode here for sure. I've got one to share. I'm going to start with you to brush.
What is your most frequently asked question these days?

Debraj

Right? So it's sort of one question, but it's got two parts to it. One is, since I'm
on the security side, he said, hey, I didn't realize Microsoft did any security.
What are you guys do? And then the second part is, wow, you showed me all
these great security capabilities that Microsoft has, but it seems like most of
the securities from Microsoft services, what do you guys do beyond that
Microsoft ecosystem? So the first one is an easy one because it's basically
like, yes, we are definitely a security company. We do all these different, uh,
we have all these different capabilities. We have windows defender Office 365
ATP, uh, Office 365 threat Intel azure APP. So we have several different
services and not only do we have these several different services, almost all these services are now actually leading their industries and actually many customers are using them.

Debraj We also have Microsoft cloud app security for the KGB services. In terms of the other question, that's actually where it gets really interesting where they say, hey, you guys are only securing Microsoft products. What do you guys do beyond that Microsoft ecosystem? So that we actually do a lot of things where we secure a beyond the Microsoft ecosystem. For example, the Microsoft cloud app security product actually secures 40,000 different apps across the entire app ecosystem, 40,000. I think that number and that number is obviously always growing. Windows defender ATP obviously has partnerships with other organizations so that we can actually protect beyond just windows devices. So we're actually doing a lot of different things that are actually helping us protect our services and security capabilities that are not actually Microsoft only. And then on our roadmap we actually have several different things.

Debraj So we have something called azure security insights that we'll be launching sometime soon where it's actually going to be a dedicated sim, which will be able to look at signal from all different security services, analyze it, and give you a basically recommendations and other things that you can do that. So Microsoft is not only just protecting Microsoft's services, we are actually now a already having services that go well beyond the Microsoft ecosystem. And our roadmap as an organization is to actually realize that hey, security is obviously across an entire ecosystem and now we're working towards protecting all of those things.

Mark So security mapping to the realities of how all customers probably including us have apps, solutions where they store their data spans, of course beyond us as a single vendor. So Bill, you must get a lot of questions and specifically in the security and compliance area or just the one that's sort of burning everybody's minds these days, what's your most frequently asked question?

Bill I would say the frequently asked question I receive is when we talk about security and compliance, I think a number of customers come up and say, do I have to be effective and to take advantage of some of our greatest security and compliance capabilities and our most advanced cape capabilities in the service is definitely the best bet. However, even if you're not an e five customer, you can definitely take advantage of labels. So you can definitely take advantage of our limited access policies. So if you want to be able to control what level of access a request from an unmanaged or noncompliant device has to content inside of your, uh, SharePoint sites, inclusive of team attached SharePoint sites, we do have capabilities that are [inaudible] that can help you along that journey. Probably the next question I get is how do I, how do I validate security within my organization? How do I, you know, test what my security looks like with an emphasis on the user themselves. And that's kind of where attacks simulator comes in. So you want to understand kind of what's the impact of a password spray attack, what's the impact of brute force? How do I, how do I deterministically understand how my users are going to react to a scenario inside of the service? And I think a tax simulator is a great example of one of
those capabilities that we have to enable you to actually, uh, you know, play red team, blue team, uh, with, within your organization itself. And you may have some more to add to that.

Debraj: Yeah. And, well the other thing is tax simulator is part of a broader services Office 365 threat intelligence and the point you made right now, password sprays one of the attacks, but one of the most popular attacks that it's part of a tech simulator is phishing campaign. Uh, so my love fishing, so we see that phishing is basically the predominant attack attack that we see through emails and so attacks to me later can actually simulate a phishing campaign. So you can target different users in your organization with the phishing campaign, find out how they behave, the admin will get a report that tells them, Hey, this is how this person reacted so you may actually need to educate them more or you actually realize that hey, these folks actually know how to deal with this type of stuff.

Bill: Yeah. The reason I bring up password spray, so many customers are still putting so much emphasis on, you know, brute force protection. So a certain number of failed log ons within a certain period. I'm going to go ahead and just deny, uh, you know, that request outright, but you know, password spray different fundamentally, you know, that's taking a known password or, or a perceived known password and then just using that across the organization with the hopes that one individual within the organization is actually going to be using it.

Mark: Matt, what is your most frequently asked question of the answer that you give Matt Swann: So at the end of all of my talks, I'll always have a customer ask. It's great that you do love this monitoring unconvince, but will you notify me if my data is compromised during a data breach? And our answer is yes. Like Microsoft's commitment is to notify every customer who has been impacted in that breach within 72 hours of a data breach being declared.

Mark: Wonderful. Great. Chris, what is your most frequently asked question these days?

Chris: Well, one question I get and it's much more esoteric and it relates to some of our new compliance labels and in particular around retention and records management. We're now giving you the ability to manage a hierarchy of those labels and we get questions about how many labels and particularly how intricate can I build my data protection regime, and the answer is you can build it up to at least seven layers deep and hundreds if not thousands of labels and associated policies can be incorporated into that. So we've really been built as a skilled service. Mark, what's your most frequently asked question.

Mark: I'm sometimes not the right guy to get this question, but a lot of people have been asking since we're now sometimes presenting at a broader scale to present Microsoft 365 and then get into topic du jour. Um, and the thing a lot of people have been asking about. And to be frank, I had to go and get a little bit up to speed for myself is when something does happen. Not just breaches, not just significant things, but just somebody shares a document that they shouldn't have or DLP detects, but they went ahead and did something anyway because they didn't have it as a blocking event. The question is how do I report on all of this and we have a wonderful answer. I'm assuming everything in your world is auditable, audited and tracked, but we have these
great usage databases that we now provide a lot of insight into the, You can then generate reports in excel, you can take it into power bi and there's a lot of data and the most common question around reporting is we're opening ourselves up to external users in areas so people are being invited on purpose and they just want to know at the end of the day what are they doing? They've been invited into a specific site, specific team for Microsoft teams, whatever that place is. Part of that question is how secure is that zone, but then when people do things, share documents, create a new list item, create an app that does something internal, external, and so we're doing a lot of work to be able to monitor what's going on, but we're doing also a lot of work to give people a proactive reports and of course a lot of reactive things they can do with powershell to munge against that audit or that log of data to then essentially tell somebody, here's what happened, here's what person x from outside bid. Um, so we've got a really great reporting story and there's a lot of great articles that we can point people to in terms of documentation. But I'm glad that we have a good answer in that. You know, what happened? I don't know. It's a terrible answer. So our answer is much better than I don't know.

#5

## UPCOMING EVENTS

<table>
<thead>
<tr>
<th>TRANSITION</th>
<th>Time</th>
<th>Speaker</th>
<th>Event Details</th>
</tr>
</thead>
</table>
| Mark       | 01:04:25:00 | Always, always, always. There's a ton of stuff to learn and of course a ton of stuff to share. If you want to share your insights and your feedback really to keep up with what's going on, we encourage you to join a SharePoint Saturday near you. They're free, they're easy to find. If you go to spsevents.org. So coming up on December first, there is a SharePoint Saturday in Gurgaon that's near New Delhi, India, and Vienna in Austria on December six with sort of breaks the mold a little bit, at least according to their website. From what we can tell, there is a SharePoint Thursday, Thursday, new technology. So if you know, we have share pint in college. We had thirsty Thursday, so I think there's gonna be a new #SPTGeneva, so there's a SharePoint Thursday, December sixth in Geneva, Switzerland, and then right after that on SharePoint Saturday, December 8 in Detroit, Michigan. Always check their website, always reach out there. They're happy to answer questions about what's going on in those individual regions. They always list the person who's managing the event, uh, but they are great free events to plug into, ask questions and do a lot of learning. You know, as we get into the holidays, it's always good to take a respite and be able to go someplace warm. And that's why we have office in SharePoint live coming up in Orlando, Florida, December, second through seventh, three days of workshops and three days of breakout sessions with friend of the show, Matt McDermott and a cast of dozens of extras. Focus principally on Office 365. There'll be SharePoint. It's co-located with visual studio, live cql server, tech mentor, ai live and modern apps. All of them are live. And uh, just at that same time, December fourth through the seventh, if you want to go inland just a little bit, their SharePoint fest, Chicago. This is a three day conference with a lot of breakout sessions, a couple of keynotes and of course a couple of workshops including the keynote from our friend here, Chris McNulty. I should write it. But what I'm most excited about is we're going to be recording.
a live studio audience episode of the interests on there.

Mark
So we'll have a couple of guests have a couple of topics. We'll go through that and it's going to be mapped to the closing AMA. So we also will have a time where you can ask Microsoft anything. Chris and I and others will be there to answer any questions.

Chris
One of the things we'll be talking about in the live show is a prediction for 2019 and we're already predicting 2019 is going to be a huge year. We're in the midst of planning SharePoint conference at May 20, first through the 23rd at the MGM Grand in Las Vegas. It's a coproduction between Microsoft and the conference organizers. That SharePoint conference team. Um, there'll be 150 speakers or more, hundreds of sessions, workshops, exhibitors. It will be the spring event with Jeff Teper and leaves us through all of our announcements for next year. So registration is open now. You can learn more @SharePointNA.com.

Mark
Very much looking forward to seeing you at any and all of these events. Chris makes a good round of a lot of events. Will certainly be at a number of them. And hope to see you there soon.

#6  SHOW WRAP + OUTRO

TRANSITION
01:07:24:00
Mark
Thank you to our guests. Matt Swann, Debraj Ghosh, Bill Baer. And of course, my cohost today, Chris McNulty.

Chris
We encourage you to check out our show page for links to everything we talked about today and more go to Aka.ms/theintrazone

Mark
If you have any questions, thoughts, SharePoint stories, please share them with us. Reach out via email@theInterzoneat.com, or via twitter @SharePoint, @mkashman, and @cmcnulty2000, which is not with a k.

Chris
And remember to rate review until all of your friends and family about the show. You know, a subscription to the zone is a wonderful holiday gift. And it's free. Subscribe wherever you find your podcasts.

Mark
Absolutely. We'll also have a link to take a survey. We'd love to hear from you. We want to tell you, thanks so much for listening. This has been The Intrazone, a show about the SharePoint intelligent intranet.