Enterprise Security in a mobile-first, cloud-first world

Company Participants

- Julia White, General Manager, Cloud Platform
- Satya Nadella, Chief Executive Officer

Presentation

Satya Nadella {BIO 3224315 <GO>}

Okay. Good morning, everyone. And it's great to be here this morning. I'm going to spend my time this morning talking about perhaps one of the most pressing issues of our times of our industry, cyber security. In fact, if you look at the history of computing or history of all information technology, starting from when we start -- started to store data, transmit data and communicate, we've always had attacks on trust. With mail came mail fraud. With the telegraph, radio and television came wire fraud. And now with the Internet, we have cyber crime.

And each time we have been faced with this, we've come together collectively as individuals, companies, organizations and governments to respond, to use the very technology to be able to respond to the challenge. And that's what we're doing with cyber security. And today, I want to talk about Microsoft's contribution, Microsoft's approach.

When we start to talk about cyber security, I want to first start with Microsoft's mission. Our mission to empower every person and organization on the planet to achieve more is what drives all of our technology innovation agenda, how we interact with our customers, how we show up with our customers, how we partner with the broader ecosystem. It drives everything that we do.

And trust is at the core of this. Because in the mission, is -- the mission captures our optimism for the future. Optimism for how digital technology can play a positive role in every walk of life and in every sector of the economy. There isn't any aspect of our lives, how we entertain ourselves, how we do commerce, how we educate our boys and girls, there isn't a part of the economy from retail to healthcare to energy that is not using digital technology today to drive innovation and transform itself. So it's become the core of not just tech industry but the core of every industry. But customers are not going to use this technology if they can't trust it. And that's why trust for us is central to our mission of empowering every person and organization. And we're taking a principled approach with strong commitments to make sure that our customers can trust digital technology that they use.

We have four pillars to this. When it comes to privacy, we will ensure your data is private and is under your control. When it comes to compliance, we will manage

your data in accordance with the law of the land. We will also be transparent about both the collection of data and the uses of data. And lastly, we will ensure that all your data is secure. These are the four strong commitments that we will make in everything we do, all our products, all of our services, how we work with our customers, both proactively and reactively. It's grounded in these four principles.

And today, I want to talk about security and cyber security. In fact, it's been a year -- even just 2015 has been a tough year around cyber security. Just the top eight or so data breaches have led to 160 million data records being compromised.

In fact, one of the biggest challenges that we all face is the time to detect an intrusion, it's something like 229 days between when you have been intruded versus when you know and you can start to respond. The cost of all of this in terms of lost productivity and lost growth really adds up. It's estimated that it's something like $3 trillion. Now, in a global economy that is challenged for growth, this is really a huge issue for all of us collectively.

So now the question is, what is Microsoft going to do about responding to this challenge and what is our approach? But before I talk about our approach, I want to start by describing the changing environment that we have. There was a time when we could talk about our environment with a very strong perimeter around it, where we could talk about our data, our applications, our computing end points all being secure within the four walls of our environment.

But over the last two decades, we have taken advantage of a more connected world, a more connected economy. We've extended our network to touch our customers directly -- they could be through business-to-consumer e-commerce or through business-to-business e-commerce. We have things like customer relationship management where customers are directly electronically connected with us. We've optimized our supply chains, so that we can have inventory levels throughout the supply chain constantly updating because of the connectivity that we have between our systems.

We not only stop -- we have not stopped there. In fact, in the last couple of years, we've increased the pace of this connectivity. We are increasingly looking to public cloud services for our infrastructure, be they infrastructure as service or platform of service. We are increasingly turning to SaaS applications for our mission-critical business applications of CRM, ERP. And given that pace of change in fact, one of the other things that we are also doing is, we are incorporating devices that are owned by our employees inside of my network. So we are letting people bring their own phones, their own computing end devices into our environment.

And of course, all this is set to even further explode with the Internet of Things because, computing is going to be ubiquitous, it's going to -- general purpose sensors are going to be in every room, every conference room, every living room. And so therefore, now we live in a world when the attacks can come from anywhere.

The attack vectors can come from anywhere. The attackers themselves are a lot more sophisticated and lot more organized.

So it's a perimeter-less world, it's a world that is constantly evolving, it's dynamic, and you're under constant attack. That's the environment that we have to deal with.

One of the things that drives us to the kinds of solutions that we are building and that we will talk about today is a pretty unique perspective we have in all of this. We today run some of the biggest Internet services, both on the consumer side with things like Xbox Live, as well as on the business or the commercial side with services like Office 365 and Dynamics and Azure. And that gives us a pretty unique perspective in what's happening, a great sampling of what's happening in terms of both the attack vectors and how one responds to them.

For example, we update Windows a billion times a month. A billion devices are upgraded each month for security patches, for compatibility, to make sure that that ecosystem remains vibrant. We run the world's largest anti-malware, antivirus service as part of Windows.

We also inspect over 200 million emails as part of the Office 365 service for malware. We're looking for these attachments that may have malware associated with them. So we take them, we detonate them, we inspect them before we deliver them to the inboxes of people.

The fact that we run this gamut of services spanning consumer and commercial. And it's very, very key to think about those two aspects because all of you have services that reach consumers as well as business-to-business services. And so you need to be able to think of that intersection, and you need to be able to have a sampling of traffic that really helps you get visibility into both aspects of it.

And we have something of the order of 300 billion authentications every month that we see, so identities of consumers and businesses that we see in our network.

Now, all this unique perspective has helped us develop a very different security posture inside of Microsoft. In fact, 14 years ago, Bill Gates wrote about Trustworthy Computing as a priority for Microsoft. And we have made a tremendous amount of progress on it. But with this changing environment it's no longer just about our code and the threat modeling and the testing, but it is in fact about the operational security posture that we have in this constantly evolving environment, this constantly under attack environment. So the operational security posture to me is where it all starts. It's like going to the gym every morning. Every hour of the day you need to be prepared. And so that means you have to exercise this operational security posture in a continuous basis.

This framework of protect, detect and respond has been there with us for many years. What is new is that posture. For example, what we protect no longer is just computing end points or applications. It's all of that. It's computing end points, it's

the applications, which may be inside your premise, it will be the cloud services that you're using, it is all the sensors, the HVAC system and the datacenter infrastructure. So everything from sensors to datacenter is part of your environment that you need to protect.

When it comes to detection, it's no longer, for example, waiting to detect a signature and then coming up with a response and then deploying the remediation. We now have moved too much more of a behavioral approach where we can detect based on the behavior of the attack vector. And when it comes to response, this is perhaps the area that is going through the sea change in terms of how we respond, we're using the transformation of an as a service base, even with Windows, we think of Windows as a service so that we can ensure both compatibility and security of Windows end points continuously. Office 365 as a service means it's no longer just about giving you the tools but it's about actually ensuring security of your data, of your tenant in the service.

And it doesn't -- it's not limited just to the services we run. In fact, the knowledge we gain is something that we share broadly with the industry and with our customers, because it's going to take us all to come together to combat this. This operational security posture is perhaps been the biggest sea change inside of Microsoft to get us to come up with new solutions, new technologies that in turn help us really secure your environment. So the approach that we are taking has three key elements to it. The first is building out a comprehensive platform for you to be able to run that loop from protection to detection to response.

Second, we complement that with this intelligence fabric that we have, and this operational security posture that we have, as well as a set of proactive and reactive services that we will have in the field so that we can help secure your environment on a continuous basis.

And lastly, it is about partnering broadly, partnering with the rest of the IT industry, because we know that we don't live in isolation, you all have a heterogeneous environment, and we need to operate within it.

When it comes to the platform, one of the things that I personally do is sit in security review meetings every month where we look at all the incidents. In fact, every time there is an incident, when I call the CEO of the company that has had this issue, I ask two questions. How can we help, and what can we learn? Because that's the posture that we need to take once you start with an operational security focus.

And that has helped us ground ourselves in the real incidence, the real attack vectors, the mobility of those attack vectors, and then the responses we have come up with. So what we want to walk you through today is how we've built this platform to be resilient under attack.

Accidental data loss, this is perhaps one of the biggest issues we have, especially with bring your own services and bring your own devices. It's unintended in many

cases, but can be devastating. So how do we help you get to a control plane that allows you to avoid accidental data loss?

Phishing attacks, social engineering is perhaps one of the biggest sources of attack vectors, so how we deal with that.

Malware continues to be a big issue. It's just that it's getting much more sophisticated in terms of how malware shows up in your computing end points, in your email. Pass the hash, how do you take access to one account and access others?

And, of course even the core hygiene, which we sometimes take for granted, is so important, because once you start with the operational security posture, you recognize that more often than not most of the issues have to deal with the lack of patching and the lack of strong credentials. And it's so important for us to not only improve the technology but the security posture you have around the basics.

It is that security platform that we are building across all of our products, and I felt that it will be great for Julia White to come up onstage and give you a quick run of all of the capability in our platform. Julia?

Julia White {BIO 20496259 <GO>}

Thanks, Satya. Now, Satya spoke about the different types of security threats. I'm going to show you how some of the built-in Microsoft technologies, working in partnership with the security ecosystem, can help address these threats and help you achieve this new security posture that Satya spoke about.

Now, I'm going to first start talking about protection technology around identity theft, which is certainly a big area. So today, users' identities are being stolen and misused at an unprecedented level. And the solution frankly is to move away from passwords completely. But up until this point, you really only had the choice of smart cards or other similar type of technology. But unfortunately, the user experience, the IT cost and complexity has been a barrier to broad adoption of this technology.

Well, now with Windows 10 Passport we've addressed this issue by giving you smart card level of threat detection and capability and protection, but using the device as the first factor of authentication itself, making it very simple, simpler than the card, and the second can be biometrics, using Windows Hello. And that can be fingerprint, facial or iris.

Now, just to be clear, this is not just a front end to your password like other devices give you, this is actually a password replacement, so it's a very big deal. Now, here I have my Surface Book and it's set up with Windows Hello for facial recognition. I'm going to step in front of it and it happens fast, so watch how quickly it authenticates me into the system using biometrics. Just like that, incredibly simple user experience, and yet more secure than a traditional password.

Now, Microsoft's also working to enable this technology to be an industry standard. We're working with the FIDO Alliance, with support of other companies like AMEX and Intel, to be able to have all platforms benefit from this type of technology in the future.

Now, certainly beyond the hardware level of identity protection, you also need to secure and manage identity around your SaaS applications that we're increasingly all using. This is where Azure Active Directory comes into play. It enables single sign-on to over 2,500 pre-integrated SaaS applications, as well as lets you integrate any of your existing applications as well. It enables conditional access, so enables -- lets you preconfigure apps to require multifactor authentication, or you can determine it based on the user, the app type or even the device health. So I'll show you what that looks like.

So I go in here, and I have my app portal, excuse me. And I see that I have a bunch of different SaaS apps I can use. And I'm going to go into sales force here. And when I do that, it's set up for multifactor authentication, and so it's going to prompt me for a phone call, if I look over here, see that and I'm going to get a phone call on my phone right here, because it's set up for that on a preconfigured fashion. And when I do that, I get a phone call, I'm just going to answer that and I just have to push the pound key to say that it is me and acknowledge that request. If it wasn't, all I'd have to do is press zero and it automatically reports fraud to my organization directly. So logging me in on that phone.

Now, I'm going to switch now from talking about protecting the identity to moving into protection from malware. Now, we know that email continues to be a primary place where malware comes into the organization. As Satya mentioned, we scan over 200 billion emails a month, looking for malware and within Office 365 we of course look for known malware, but we're also looking for unknown malware, also known as zero day attacks. And this is when a hacker unfortunately discovers a vulnerability before it's patched.

So, and then, of course newer attacks are coming in as actually links in emails that as they come in are legitimate, but then they're updated after the fact to become malicious. So this time-of-click technology is increasingly important to protect for malware.

So let me go into my Outlook experience here, and I have an email that has a number of different links in it, and one of them is malicious, it was updated after the fact and I'm going to go ahead and click on it and show you the experience. Now, when I click on it, this is what Satya spoke about, we take that link, we actually put it in a detonation chamber, and we conduct analysis on it, behavioral analysis, looking for any characteristics that might make it malicious, things like is it an executable or are there elevated privileges on the -- looking for elevated privileges on the device.

And if it sees any of that, it takes me to this user page that lets me know that I've been protected and this is important, right, so the employee knows what's

happened, it means that they won't work around the system or take other risky actions as well. So I'm actually going to call for James from my demo support team here to get my machine set up for my virtual machine, actually, let me switch over here. Let's see if I have it here, okay, great, all right.

Now, moving from email certainly security from that perspective, we're going to go ahead and move to the other threat vector which is, of course, downloading apps from the web and another vector that malware comes into the organization. Now, to show you, to do this in a different way, we certainly have done a bunch of work within Windows 10, effectively a generational step with a new technology called Device Guard. Now, there's long been security around app control to protect malware from running -- running unauthorized applications on the device. But as attackers have gotten more sophisticated, they've been increasingly able to bypass that.

Now, with Windows 10 we've actually leveraged the latest in virtualization technology, as well as partnering down to the design level of the hardware to stop hackers from being able to run malware that even have gained admin level control of the machine. So it's a big shift.

Now, to show you that comparison what I'm going to do is look at it in a Windows 7 experience, and then look at this in a Windows 10 experience with Device Guard.

So here I have a local virtual machine running, and I have on this side a website with a malicious app. I trust it, but it's actually malicious. And on the other side I have my system security showing.

And I'm going to go ahead and download this app, and it has a never-seen-before malware on it, so my antivirus is not going to detect it. And I get a prompt, but I'm going to go ahead and accept it because I trust the system. But now unfortunately, the malware has gained admin level privileges, and it's disabled my firewall and my AV solution. So unfortunately, not protected in this situation.

So instead, I'm going to move over and open my Windows 10 virtual machine system and show you that with the Device Guard protection.

So same scenario, I have my apps over here that I'm going to download and my system security on this side. So let me go ahead and run that same experience. And again I'll accept that.

But now Device Guard is actually checking to make sure the digital signature is both valid, but also signed by a trusted authority like Microsoft or your own IT organizations. And when it shows that it's not, it's blocked. So in this case I'm protected from this malware thanks to Device Guard.

Now, speaking of malware, I certainly need to talk for just a second about pass the hash. Now, if you're not familiar with pass the hash or pass the ticket, this is unfortunately what enables a hacker to go from a single compromised device to being able to penetrate multiple devices across your environment.

Now, with Windows 10 we are literally ending pass the hash with a new capability called Credential Guard. Now, I realize that's a big claim, so let me explain how this works specifically.

With Windows 10 for the first time we're using hardware-based virtualization to isolate the most critical Windows services such as authentication. With this new isolation-based architecture, it's with sensitive Windows processes are secured, information as well, using credentials that are defended from hackers, thus preventing a pass the hash attack. So it's a very big step-function change and making a very big leap around ending those kinds of security threats.

Now I've talked a lot about protection from an identity perspective and from a malware perspective. Let me switch over and talk about protection from data loss, also a big area of concern. We know people are increasingly working in a mobile environment. That means we all need to do that in a secure way and enable that experience in a secure way.

Now with Intune, which is Microsoft's cloud-based mobile device management and mobile application management solution as part of our Enterprise Mobility Suite, we can protect data across all devices. So if you're enabling bring your own device, or whatever policy you might have in place, what Intune does is it uses conditional access to control the flow of email and other corporate files that are going on to the device based on the policy that IT sets.

Now unlike the legacy MDM vendors that you might be using that require you to deploy cumbersome hardware and that type of thing. Intune as a cloud service is really ready to support that new security posture that Satya spoke about.

And I'll show you what this looks like. Here I have my personal iPhone, and I want to use it for work. So I've gone through the simple steps of enrolling this device. So now IT has defined what I'm able to do on this device with corporate data and applications, like where I can save information and how I can share information office device.

So let me share what that looks like. I'm going to go into my Outlook experience and email and get some work done as many of us do, and I just have to enter my PIN, again, because this is a managed and secured app by my company. Now here I'm in Outlook, and I have this email from STAR here with an attachment that I want to get some work done on. So I'll go ahead and open that. And again, Word is approved by my organization to use for business purposes. So open that up.

But maybe in this case, I want to save it to my personal Dropbox account and share it. That would be unauthorized way, but I'm going to try it anyway, maybe I don't know better. So I'll go ahead and make a copy there and choose my Dropbox account. And when I try and save it into my Dropbox account, I see that I'm blocked, because this is an approved method for this device. They have this controls over it. So that's okay.

Well it turns out, I'm a very savvy user. I'm very committed to try and share this information even though it's stopping me. So instead, I'm going to try and copy this information and I'm going to go back and try and send it in email, it's another way to do that. So I go back here. Now because I'm savvy I'm actually going to switch and go to my personal email identity within Outlook so I'm now sending it as a personal user, trying to create that email. And as I go in here I'm going to try and paste that but you see there is no paste options, it's been blocked.

Because when I'm using my personal identity, I don't have privileges to work with this business data. But it's sophisticated enough. So if I go and switch now back to my work credentials, where I do have permissions to send this information and I go back to paste, there in fact a paste and it works. So even within the application down to the identity level, you can decide what is and isn't appropriate for work use and protected from being sent to the wrong way and the wrong place.

A great example of how you can keep that rich Office experience that people love and be able to use it both personally and work, but still get the right protections and controls from an IT perspective. Here we also have a number of partners that have done the integration to have a similar type of experience. Some examples here I have are, Adobe and Box and SAP that provide that same level of control in their applications on the phone too.

Now what I showed you on this device was an enrolled device experiences. It was enrolled with Mobile Device Management. But we're also taking that Office -- Outlook and Office app experience I showed you and we're enabling that without device enrollment so you get that application management without having to do device enrollment. This makes it easy from a bring your own device adoption perspective very simple. But also it means you can run that great Office experience side-by-side with a legacy mobile device management vendor you might have in place already.

Now, I'm going to show you the same scenario, but in this time, I'm going to show you is Windows 10 with our built-in enterprise data protection capabilities. And because it's built-in, you get a nice, seamless user experience. And you also get some more granular IT controls as well. So first of all, I'll walk this here, so I can show you that we can authenticate in, of course, using my Windows Hello. Let's go here. Another use of the biometrics, so let me just hold it up here. Looking for me. And you see, again, better than passwords, and more secure, too, and a similar experience.

So here is my Windows start screen. You see I have a little icons on the corner of any of the applications that have been approved for business use. So as a user I see what's OK for business use versus what's purely for personal use, making it very simple. But if I go into the file explorer, you see that goes down even to the file level, not just at the app level. I have some personal documents as well as work documents.

So if I go ahead and open this work document here, similar to what I showed you on the iPhone, I'm going to go ahead and try and copy some sensitive information. Let's go there. In this case, I'm going to try again and send it in an unauthorized way.

This time I'm going to use Twitter. You see it doesn't have that icon. So I'm not supposed to be using it for work purposes, but I'm going to try anyway. And when I go in here and try and paste, you see this time I actually get a pretty nuanced message. I see exactly what's happening. In this case the policy IT set is that I can go ahead and send, but I'm going to be monitoring this action.

Of course, you can block this completely. It's fully configurable. But you see on Windows 10 with that nice user experience I can get a nice rich message, it's not just the paste is missing, as well as very granular controls around how I want to manage that, too.

Now we talked about some protection capabilities right around identity, around malware and around data loss. Now let's switch over to talk about detection which is, again, as Satya mentioned, increasingly important, because we know with all of the great protections we have things like identity theft continue to be a reality. And unfortunately that specific case is a primary way that hackers are getting enabling breaches.

Now we need to be able to have tools that both monitor and protect when an identity attack happens. And the way you do this essentially is you monitor the capabilities and you learn what is normal authentication actions, and then you can identify what is abnormal. And when anomalous is happening, combine that with known threats. And then you can detect when identities have been compromised, and when an attack is taking place.

Now for many of you, it's a little bit like when you get a call for your credit card. They see some abnormal behavior, and they think something is up. It's the same idea, but applied to identity in that way of learning normal behavior so you can detect anomalous behavior on that front.

Now in the cloud, you get this with Azure Active Directory. It's filled right again, but we heard from many customers you want the same level of control in your on premises environment. And that's where the new Microsoft Advanced Threat Analytics capability comes in. Here I'm in my Advanced Analytics dashboard. It essentially gives me a timeline view of different identity-based threats that I might want to consider and understand. Essentially it lets me know kind of the who the

what and the when and lets me get the signal through the noise of a lot of different authentications.

So let me start here. I see that I have a bunch of guesses in terms of looking for a user name. Someone is trying to guess a user name in my organization. As I go up I see now they're using a brute force attack to get from a user name into a password. They've figured out the user name of Michael Dubinsky and unfortunately he didn't have a strong password it looks like, so in 450 guesses they've now secured his password, as well.

As I go up I see now it's moved from yellow to red, this is a really important and high threat, because now Michael Dubinsky's user name and password is being used to sign in from a number of computers and resources he wouldn't normally and trying to access into also a number of resources across the company that are unusual for that user name and password. Again, it's comparing normal activity and learning that and being able to detect when it's abnormal.

And then as I scroll up here I see, again, a high alert around a pass the ticket attack that's now taking place in my organization. This is the moment where we'd really love that new Windows 10 credential guard to stopping this action in this case right here.

Now with these new advanced threat analytics insights I can immediately now go take action to stop this breach. To remember what Satya said, the number -- the days between when an attack happens it sits on your network for over 200 days. Now you can identify this right away before it has opportunity to sit on your network for all of that time.

Now we talked about from an identify perspective around detection and threat. Let's also now move to an infrastructure level to talk about that detection and respond level at all up infrastructure. Now as infrastructure continues to move to the cloud in Azure, we've now built a comprehensive security system with the Azure Security Center.

The Azure Security Center provides a central view of your security settings across your entire Azure environment, with live monitoring of your security configurations to make sure there's ongoing good security health. We're analyzing your security settings even as they change and bringing back policy-based recommendations, as well as guiding you through the steps to ensure your environment is secure.

So I'm going to take a look at this. Here in my Azure Security Center, click right in here, you see I have a number of recommendations that suggesting to me based on my security posture. I go in here, and you see I have a few things, a few actions it's asking me to take. In this case I'm going to choose this adding a web application firewall.

As I go in there I see there is actually a number of web application firewall partners integrated right into the security center. So I can just choose the one I like. In this

case I'm going to choose this Barracuda, web application firewall. And you can go down and I see that I can actually right here deploy the solution into my Azure environment. It significantly streamlines the process of provisioning my partner solution, as well as enables you to bring whatever your preferred security vendor is with you to the cloud in a very simple way.

Now in addition to the partners shown here, we're also working with folks like Trend Micro, Cisco, Fortinet and Checkpoint, as well as many more to come around anti-malware, as well as next-generation firewalls.

Now recommendations are great and important, but it's also about identifying security alerts within your Azure environment, as well. So next I'll go down here to my security alerts. You see I have a number of things showing here. And if I go down I see a few different things happening and I can drill into any one of these within the security center and find out what's going on.

In this case I see I have a SQL injection attempt being made. But I go in, it's against my Virtual Machine One, but luckily that Barracuda Web application firewall that I just deployed is protecting me from this attack, which is fantastic. So let me go up and see what else is going on.

Here I see that I have traffic going from the Virtual Machine One to a malicious IP. Now again, this is tapping into that intelligent security graph that we have at Microsoft that has a broad view of what malicious IPs are. We can identify this quickly and proactively notify customers about what's going on. And then within here I'm also giving recommendations about how to remediate the security situation, as well. So I can just right here go and fix this, take that insights, and move it into action.

Now this is great from a Azure perspective and a cloud perspective. But we also know that most of our customers are running in a hybrid configuration, meaning you have infrastructure on premises, or in a private cloud, as well as in the cloud with maybe AWS, as well as Azure, of course. And you want to have that same kind of security view across your entire enterprise estate. That's where the Operations Management Suite comes into play.

It's a powerful new solution that collects massive amounts of machine data across your on-premises datacenter, as well as in the cloud, and it brings it together to search, correlate and visualize this massive amount of data so you can detect security threats across your entire estate from cloud to on-premises, as well.

So for example, I could use the Operations Management Suite to identify, if I had other virtual machines in my own datacenter communicating with that same malicious IP. I notice that in Azure I can look across the entire organization to find it, as well.

Now I've shown you just a few examples of Microsoft's built-in security technology, working in partnership with the security ecosystem across the globe and tapping

into that intelligent security graph that we have to help make all of our customers safer.

With that I'll turn it back to Satya. Thanks.

Satya Nadella {BIO 3224315 <GO>}

Thank you so much, Julie. Thank you. So that gives you a good feel for the depth and breadth of the technology that we are building into the core of our products. In fact, we spend over a billion dollars of R&D each year in building security into our mainstream products, so Windows 10, Office 365 and Azure, because we don't think of security as being a separate piece of technology. It has to be core to the operational systems that you use where your data resides, where your most critical application usage is.

And, in fact, we have built these three products to work well with each other. When you think about something like conditional access it builds on the capability in the device. It builds on the capability in the Office 365 service and things like Active Directory.

But we also recognize that is not just us building all of these technologies together, but we also need to interoperate in a heterogeneous environment. So that's something that's first class in how we deal with identity, how we deal with device management, how we deal with data protection. So those are all key to our design, key to how we are building these technologies.

In fact, in Windows 10, we have great technologies that Julia showed from Device Guard to credential guards, to Microsoft Passport, to Windows Hello, these are all core security technologies. In fact, the virtualization infrastructure coupled with all of this is what makes Windows 10 the most secure operating system.

And last week, we had a big update for Windows 10, which also added more management capability, great performance, so the combination of performance, world-class management and security make Windows 10 ready for deployment in all enterprise situations in all organizational contexts. So we're very excited about Windows helping us all move to a new frontier of efficiency when it comes to security.

When it comes to Azure, there are two capabilities that Julia showed, which I think are very, very critical. One is, what is encapsulated inside of Enterprise Mobility Suite. We brought together a new control plane which brings identity management, device management and data protection together, because that control plane becomes critical in handling accidental data loss, conditional data access, conditional application access in this current world where we have BYOD devices, as well as bring your own SaaS applications.

So EMS perhaps is one of the most strategic security products that Microsoft has had that really helps enhance the security posture that you have inside of the enterprise. The other side of it is of course, the Operations Management Suite, which is around infrastructure, not limited, again, just to the infrastructure that you have with us on Azure, but true hybrid infrastructure, so that you can manage the security around all your virtual machines, all your containers, irrespective of where they are, where the estate is, on premise, in Azure or other cloud providers.

And in Office 365, we are again building security into the core of the product and the service. The Advanced Threat Protection service is what gives you that capability to be able to detonate enclosures or detonate these attachments before you deliver them to the inboxes. The lockbox gives you the capability to secure your data, to encrypt your data and give only key access when required.

So we are building all of this rich technology into the core products. And that's what we refer to as the platform. But, the second aspect of our approach is the intelligence aspect, because it's not just the technology that we deliver, it is the platform technology coupled with intelligence.

We're building out an intelligent security graph. Historically we've always had something called the Digital Crimes Unit, which has worked with law enforcement in fighting cybercrime, bot-nets, many of the issues some of our more vulnerable populations, children and older people, face when it comes to cybercrime. And we have worked with many in the industry and law enforcement to fight those.

Now we're even bringing together the operational security people across our company, people running everything from Xbox Live to Office 365, to Azure, to Windows Update, to Windows Defender, and bringing them together in one operations center. We call it the Cyber Defense Operations Center. So this is so that like any intelligence operation, we don't have silos. We actually have people who are able to in real time connect the dots between what's happening across all of these services.

That operations center and the output of that operations center is this intelligence graph that is being used then in turn by our products to create security in the products themselves. And we share that intelligence broadly with our customers, with our partners.

We are, in fact, not stopping there. We are also putting resources right in our field so that our cyber security specialists can proactively and reactively work with customers using both our products as well as this intelligence to help secure your environment.

And as I said, partnership is very key to everything we do here. This is not just about Microsoft. This is about us working together as an ecosystem. In fact, in our both Digital Crimes Unit as well as in our Cyber Defense Operations Center, we use a lot of the third-party technology to defend our own estate. And so we want to

interoperate with all of the tools. We want to be able to take advantage of what each one of these partners brings so that we can collectively secure our environment.

So this is our new approach, our new platform, new intelligence and new partnership. And all of that starts with our own new posture with our own operational security. That's really what I wanted to talk about this morning.

And I want to close out where I started. For us we have optimism in what digital technology can do to every walk of life and every industry. Digital technology is at the core of everything going forward. And, therefore, when we talk about empowering every person and every organization on the planet it becomes even more paramount to build trust into the core of computing. And that is what we endeavor to do, that is what we will partner with everyone. In fact, customers tell us that what they want is to maximize the value of new digital technology while preserving the timeless values that we all share. And our mission is to deliver that.

Thank you all very, very much.