Microsoft Ignite
The Future of Security with AI
Charlie Bell; Vasu Jakkal; Scott Woodgate; Sherrod DeGrippo
Thursday, November 16, 2023

CHARLIE BELL: Great to be here. I'm super excited with what we're about to talk about.

VASU JAKKAL: Good morning, everyone. I hope you've had your coffee and tea, and are well hydrated. It's great to be here with you all. Charlie and I are excited to talk about security and what we're up to here at Microsoft.

CHARLIE BELL: I've been in this industry for more than 40 years; I joined Microsoft two years ago. In my prior role running a large public cloud, it was very clear that the cybersecurity problem was growing at an alarming rate, and it's very difficult for customers to deal with this incredible challenge. We don't have to look further than today's headlines to see the impact from ransomware, espionage, and even the use of cyber as a weapon in war. What the headlines make clear is that there's an ever-growing sophistication in the anti-economy of cybercrime. Every day, cyber criminals are launching sophisticated and targeted attacks on organizations and individuals, exploiting vulnerabilities in systems, networks and devices. Not too long ago, we saw the exposure of an HR department in one of the cybercriminal organizations. For God's sake, they even had an employee of the month. Ransomware is truly becoming a gig-economy.

VASU JAKKAL: That is so true, Charlie. This whole anti-economy and the speed, the scale, the sophistication of these attacks has really become exponential. We're seeing 10x the increase in password-related attacks, growing from 3 billion to 30 billion in the same timeframe year over year. Along with the number of attacks, the number of attackers is also growing really fast. Microsoft is now tracking 300+ significant actors across financial crime and nation states. That's up from 200 just last year. The consequences of these attacks can be devastating.

If that was not daunting enough, we are also facing unprecedented complexity. Today, on average, organizations use 80 security tools. Yes, 80. Talk about fragmentation. And not only that, they're expected to stitch these tools together, they're expected to make sure that the data and the insights flow seamlessly from one tool to the other, and they all work effectively. They have to do that while there's a massive global talent shortage. We have 3.4 million jobs worldwide unfulfilled in security. With the dawn of AI, nearly one out of three business leaders are worried about data loss due to improper use of AI. The odds surely, are definitely not in the favor of defenders right now.

CHARLIE BELL: You're right, Vasu. Globally, the cost of the cybercrime anti-economy is expected to reach over $8 trillion. To put this in perspective, if the drag on the world's GDP through cybercrime were itself a world economy, it'd be ranked No. 3 behind the U.S. and China. The cybercrime anti-economy is growing far faster than the fastest growing economy in the top 20, that’s India. Think about that for a moment. Cybercrime is the third largest economy and the fastest growing economy.

VASU JAKKAL: It’s mind boggling. The speed, the scale, the sophistication of these attacks combined with the security talent shortage and the operational complexity that we all are dealing with, are giving attackers an asymmetric advantage over defenders today. Attackers only have to be right once, but we, defenders, have to be right 100% of the time. No wonder cybersecurity is one of the most pressing challenges of our time, and this requires a paradigm shift.

CHARLIE BELL: There’s no question that Microsoft is the leader in this shift. We bring together three critical advantages that exist nowhere else. Large scale data threat intelligence, the most complete end-to-end protection, and industry-leading responsible AI.

VASU JAKKAL: These three advantages really power a flywheel of innovation. As security becomes more connected through cloud, greater visibility spins the signal processing part of the flywheel, which in turn generates insights leading to better threat detection. From threat detection, we drive better detections, which give us a deeper understanding of proactive actions we can take in the administration of our security posture, and this creates greater safety, which attracts more cloud adoption. This flywheel has been spinning for a while, but now, it has been turbo charged with AI rotating it from the center at machine speed, and we’re all becoming safer and safer. Shall we talk more about the flywheel, Charlie?

CHARLIE BELL: For sure.

VASU JAKKAL: Let’s take a look at each of these sections of the flywheel, the three advantages. Let’s start with signals. Signals matter deeply because you cannot protect what you cannot see. The large-scale data advantage is what Microsoft security brings to the table. We bring the insight of 65 trillion signals every single day, and these help us understand exactly what the attackers are doing, and it helps empower you to protect yourself against these attacks. Now, we couple that with the expertise of global threat intelligence and the insight of attack behaviors from more than a million customers and over 15,000 partners. The next section of the flywheel, our next advantage, is end-to-end protection. To protect your digital estate and your organization comprehensively, you need to secure everything. You need to secure your data, your identities, your apps, cloud, infrastructure, and so on and on. It was just like locking a door with six locks and having your windows open, that’s not great.

Microsoft security helps you protect your environment from every angle: security, compliance, identity management and privacy. Integrating 50 categories to form one end-to-end Microsoft Security Cloud composed of six product families: Defender and Sentinel, our Threat Protection Family and cloud security solutions; Purview and Priva, our data security, compliance and privacy solutions; Entra and Intune, our identity and access solutions. These products together form a flywheel of protection where each one builds on and strengthens the other.

CHARLIE BELL: As Vasu pointed out, we've made a ton of progress on end-to-end protection, but with generative AI we can take a giant step forward, one so large that will finally tip the scales in the favor of defenders. We can now harness everything we see and everything we own, with AI expertise that transcends the knowledge that any one individual could amass. As you heard from Satya yesterday, Microsoft has been all in on AI for a very long time and is the leader in bringing generative AI to organizations worldwide.

We understand the full stack both what is required to create AI applications and operate them safely and securely at scale. By the way, I'm sure you're going to hear a lot of noise from legacy security vendors who'll be AI-washing their current products. I do expect that this will be largely chat applications, but Microsoft Security Copilot is much more than that. We started with the most advanced AI model from OpenAI, which today is GPT-4, but will be constantly improved. We then add a Microsoft-developed security specific model, constantly revised Dynamic Threat Intelligence, an ever-growing library of cyber skills and promptbooks all running on Microsoft's secure and reliable AI infrastructure.

In general, chat apps handle your request by making a single call to a large language model, we call it an inference. Typically, one request results in one inference. For security, we make up to a dozen inferences, or even sometimes more, to handle the breadth of data, the complexity of the data, and to make sure we answer accurately and with an answer that's well grounded. Security Copilot isn't just summarizing a prompt, it's reasoning over multiple data sources to do at machine speed what would take hours for a human to do. You heard from Satya how Microsoft is announcing more than 100 updates today across the entire stack. We introduced Security Copilot last March, and today, I can't wait to show you how we're bringing those AI capabilities into every part of our security portfolio.

VASU JAKKAL: Super, super exciting, isn't it? But before we get to these announcements, for those of you who may be new to Security Copilot, our new generative AI solution purpose built for security, let me take a moment to do a brief introduction. Security Copilot, as Charlie said, is the first and only generative AI security product that builds upon the very latest models of GPT-4 AI to defend organizations at machine speed and scale, which is really important. It's continuously learning from Microsoft's unmatched global threat intelligence, our security data, and the security skills usage to deliver users tailored insights for their organization to harden their defenses and enable much, much faster response.

With Security Copilot, you can ask natural language questions to quickly and easily understand what's happening in your environment. You can ask Security Copilot anything about security, from what incidents you should focus on, what is the impact to your organization, and most importantly, what to do about it. It will recommend next steps.

CHARLIE BELL: So cool, Vasu. Look, I got to tell everybody, I've been in this industry for a while, I lived through many disruptive changes in technology, I'm so proud of the Microsoft Security engineering team. We've innovated around this new capability of artificial intelligence. What the team has done building this technology is frankly astounding. The teams of security professionals in Microsoft deal with attacks every day. They defend our customers, they defend Microsoft, and now they brought to life Security Copilot to help IT and security professionals supercharge their skills, collaborate better and catch attacks that may be missed due to tool fragmentation and talent shortages.

VASU JAKKAL: These are really important things for us to solve, and we are innovating rapidly to integrate Copilot into all of our security and compliance experiences, as well as expanding our end-to-end capabilities because we want you to have the best. To show you how we are empowering each of these important roles as part of our unique, comprehensive approach to security, we will take you through an imaginary threat. Let's start with security operations, the team that uses Defender and Sentinel daily to analyze and investigate incidents.

CHARLIE BELL: Let's get there. This is a typical phishing email that many of us have seen. Vasu, have you ever seen one of those tricky emails that Brett uses to test us all?

VASU JAKKAL: I believe I have, Charlie. Brett is our CISO, so he's trained us well not to click on any links.

CHARLIE BELL: A single click can result in any type of compromise, from identity theft to malware injections, to network intrusions. If our user, Jonathan from sales, is compromised, that could give attackers access to sensitive customer and financial data. Every suspicious activity, every click on phishing email creates a flurry of alerts for the security operations team. They have to triage hundreds of alerts per day. Alert fatigue can result in undetected threats that fly low and slow under the radar. The problem is often multiplied because alerts are spread across a bunch of different security tools, from identity and access management to email security, to endpoint management, to cloud security, and so on. For decades, security operations teams have been dealing with siloed security tools.

VASU JAKKAL: To add to that, in recent years, we have seen the rise of these threats. And as a result, we're seeing the rise of Extended Detection and Response, or XDR, to consolidate some of these signals, and their Security Information and Event Management, or SIEM solutions, which aggregate these security signals from other sources, both really important. In many organizations, XDR and SIEM are the two main tools that the security operations team use, but wouldn't it be wonderful if we could bring them together? I'm thrilled to announce that we are bringing together Microsoft's XDR solution, Defender; and Microsoft's SIEM solution, Sentinel, to create the industry's first unified security operations platform.

We're taking the industry from a world of many to a world of one, breaking down these silos. We're bringing the power of Microsoft Security Copilot to bear, so defenders can have a generative AI companion, the Copilot, with security-specific skills. Sherrod DeGrippo is now going to come out and show us how this all works. Now, Sherrod has a deep history as a defender. She has led red teams; she has led threat researchers. These are people who are on the frontlines of security. In many ways, they are your first line of defense for the world. Let's bring Sherrod over. Sherrod.

SHERROD DEGRIPPO: Every second counts when it comes to an active incident. Analysts and security operations centers are always working to reduce their mean time to respond. To help them, we've reimagined security operations with a streamlined workflow that delivers the best of Microsoft's SIEM and XDR capabilities, enriched with more AI, more automation and more guidance. This is what that looks like. All the highlights and capabilities from your SIEM, XDR and Security Copilot are right here. I have one view of all the active incidents across all of my tools alongside threat intelligence, so I can get the threat intel that I need quickly, and I have one unified list of incidents to work from, spanning SIEM and XDR.

Now, if you're a security analyst, you know this is gold. If you are not a security analyst, let me tell you, this is gold. Each incident combines alerts from SIEM, XDR and cloud protection into a comprehensive package that gives a full view of how an attacker moves across an organization. This means more meaningful insights brought to the analyst automatically. Let's look at this incident at the top. This is a financial process manipulation on SAP. Microsoft Sentinel has a fantastic solution for protecting SAP, out-of-the-box monitoring, no manual playbooks to run. This is new. We're bringing SAP events collected by Microsoft Sentinel together with Microsoft Defender XDR, which has automatic attack disruption capabilities. What we get is attack disruption that extends to SAP.

What this means is that my threat was stopped even before it turned into an attack. That was never possible before. So Jonathan, the user that Charlie just told us about, seems to be at the center of this attack, but it was stopped on two levels. First, his SAP account was locked to keep the threat actor from taking actions like redirecting payments to themselves. Second, his Active Directory account was locked to keep the threat actor from using it to access anything else in the organization. Security practitioners will call that lateral movement, it can be really dangerous. This was done all automatically for me.

The power of SIEM and XDR together, you get more automation, more confidence and ultimately a more secure organization, and I have the power of Copilot built in. Copilot guides me through the investigation, helping me catch what others missed. First, it analyzes the incident, and provides me with a detailed description. It looks like Jonathan, our user, clicked on a malicious URL in a phishing email. His SAP credentials were stolen, but now Attack Disruption has already done its work, so this specific threat was contained.

However, Copilot knows that threat actors often launch multiple attacks. And it's important to hunt for additional damage from this particular threat actor. Copilot has a skill to identify attackers from IP addresses. It matches the IP address for this incident to the cybercrime group tracked as Storm-0928, but it doesn't stop there.

Copilot then builds a hunting query in natural language to find any more damage caused by Storm-0928, and it automatically prompts me to run it. I will take that suggestion, and Copilot finds an additional PC that was attacked. And now, I can add that into the incident.

This unified platform makes it super easy to manage my operations. I'm not doing any copying and pasting between tools. I don't need to keep track of anything in my head. I don't even need to write a query using a query language like KQL. Copilot figures it all out; it guides me through the process. And in a recent study we did to measure the productivity impact for early-in-career analysts, participants using Copilot demonstrated 44% more accurate responses, and they were 26% faster.

Here, I see a script was downloaded to the device. And it's important to understand what that script actually did, so I can be on the lookout for any other potential impacts from the threat actor. Understanding malicious scripts is an advanced skill set, but not a problem. Copilot does this analysis for me. It gives me an easy to understand description of what this script did, so it's helping me get better at my skills.

We go back into the incident. Copilot guides me to remediate the issue, get Jonathan's account back to a clean state. And from there, I run my remediation playbooks to revive Jonathan's account. When I'm done, Copilot resolves all the related alerts. It gives me a comprehensive incident report. Incident reports used to take hours to write. They always seemed like something was left out.

But remember a minute ago, when I said every second counts during an investigation? Well, as all of you know, every brain cell counts, too. With this unified SOC platform and built-in Copilot, it's not just about saving a few clicks here and there. It's about reducing the mental burden for analysts so that they can do their best and most creative work. We want them to be able to make an impact to the overall security community. Remember, security is a team sport.

(Applause.)

VASU JAKKAL: Well, thank you, Sherrod.

CHARLIE BELL: That was awesome, such a game changer for security operators. Super cool.

VASU JAKKAL: That was awesome, and I just love, love, love, Charlie, how Copilot and how our tools are helping analysts really expand their skill sets.

CHARLIE BELL: Well, now, the job is not done when we complete this investigation. Imagine our user, Jonathan, who was the center of that incident, has his account restored and gets back to work. But he's asked to present a second factor of authentication when he logs in. He thinks that's a little funky, and he's a little sensitive after being fished. So, he puts in a helpdesk ticket.

By the way, you guys should all cheer that, because you want your people to file helpdesk tickets, right?

VASU JAKKAL: And that ticket is now routed to the IT admin responsible for managing identity and access. They use Entra, Microsoft's multicloud identity and access solution that allows you to protect any identity and provide secure access to any resource. Think about that, any resource, that's a really big scope. But things start getting complex really fast.

But I have great news for all of you, especially all our identity admins. We are embedding Copilot in Entra to help simplify and speed up your work. And to share more about this, let's welcome Scott Woodgate, who has been working on security products for a long time and is awesome, on stage.

Scott? There you are!

(Applause.)

SCOTT WOODGATE: Hey! Now, troubleshooting user access issues quickly is instrumental to ensuring that users are productive, but sorting through lots of logs can be difficult. Let's see how Copilot and Entra simplify the complex for better identity access.

Now, here in Entra, I ask Copilot in natural language to explain why Jonathan was forced to use MFA. Copilot figures out what is happening, why it's happening and what I should do about it. And it brings me the answer in natural language with all those important details I need to solve the problem, like policy information, and sign-in data.

Then Copilot recommends that I explore failed sign-ins that happened in the last 24 hours. Now most likely, that's related to risky users. It used to take me a long time to figure that step out, but Copilot can do that for me, too. And so, now, I can fix user issues before they become a problem.

With Entra and Copilot, I can give users what they need faster than ever before.

VASU JAKKAL: But Scott, I love how Copilot applies identity-specific skills to suggest the next step there. It's not just really saving you time; it's helping you get something that you may have missed. And that is a big deal, because up till now, Copilot has been focused on helping security operations, helping teams do incident investigations. We are expanding it to help identity admins do their work.

But let’s keep going, because we are now looking at that next thing on how can it help device admins do their work. So, that’s exciting.

CHARLIE BELL: Yeah, that’s another really critical member of the team, the IT admin who manages devices. Enforcing the right policies on your endpoints can eliminate whole categories of threats to keep you compliant.

Imagine the team is concerned about that phishing campaign we saw, and we’ve been looking at, and they decide they want to add some protection with stronger device management policies. They need to make sure they aren’t going to disrupt everyone else in the company.

VASU JAKKAL: Well, we are so excited that we are making Copilot available to device admins by embedding it in Intune.

Scott, will you show us how that works?

SCOTT WOODGATE: Of course. Are there any device admins in the audience?

My management policies are so important, of course, for both governance and security, but understanding the impact of these changes on existing environments can, frankly, take IT or device administrators hours and result in misconfigurations. Let’s see how Copilot and Intune simplify the complex for better device management.

Now, here in Intune, I asked Copilot in natural language to create a new policy to block users, using these guys, removable drives. Copilot guides me right to the removable drive storage policies. But here’s where it gets really interesting.

Copilot runs what-if analysis, pulling data from multiple sources to understand the current users of the policy and the impact on my organization of turning this on more broadly, so that I can address potential issues up front. How cool is that?

Let’s look at an example.

Here, Copilot figured out a previous admin had deployed an override policy to enable removable storage for the marketing division, which, of course, conflicts with my new policies. I can now get together with the Marketing team and figure that out, and keep my users productive.

With Copilot in Intune, I can roll out policy changes with more confidence than ever before.

VASU JAKKAL: Well, that’s awesome. That’s really, really cool. Having that impact analysis before you roll out a new policy is almost like being able to see into the future.

And talking about seeing into the future, let’s talk about Purview and Copilot.

CHARLIE BELL: Yeah, there's one more potential consequence of that phishing campaign. Imagine what would happen if we didn't have attack disruption, so the attack wasn't stopped. And the attacker was able to use stolen credentials to access customer data. Now we've got to do a data loss investigation.

Everyone in the organization needs access to data, and it's scattered everywhere. For many organizations, that includes multiple clouds. Data loss investigations can be super complex.

VASU JAKKAL: And that's why we are embedding Copilot in Microsoft Purview, our data security and compliance solution, to make it easier than ever to protect your data.

Scott, let's take a look at that.

SCOTT WOODGATE: All right, Purview, let's go.

Data security is critical, and teams need to quickly understand and, of course, resolve high priority alerts. Let's see how Copilot and Purview can catch what others missed for better data security.

Now here, we have many high priority data loss prevention alerts. And I need to understand this specific alert about an Excel file that contains customer data. Let's see how Copilot can help us.

Copilot figures it out for me and uses its skills to bring together information from multiple sources, including things like credit card information, and also user insider risk levels.

Now while I'm here, let me show you two more compliance scenarios where Copilot can help very briefly.

Here, you can see Copilot helps me quickly address insider risks, bringing me the details that I need. And here, Copilot actually quickly evaluates a meeting transcript, and it finds policy and violations, in this case, stock manipulation, all for me.

With Purview and Security Copilot, I can diagnose data security and compliance alerts faster than ever before.

VASU JAKKAL: Thank you so much, Scott. That was awesome. You're awesome.

SCOTT WOODGATE: Thank you.

(Applause.)

CHARLIE BELL: What you've just seen is how we're taking Copilot and putting it in the hands of both security and IT professionals to help you do your work. From identity management to device management to data management, Copilot is here to help you figure out what's happening, and how to fix it and what you've got to do next.

VASU JAKKAL: And in addition, we are expanding our end-to-end security capabilities with investments across the whole portfolio. Now, there's so many of these, and we wanted to share some of the big ones with you right now.

Everything we do in security, we do it with an eye to a protection for your entire digital estate, all your clouds and all your platform. As such, we're extending all of your data security capabilities to cover your data, structured and unstructured, no matter whether it lives in the Microsoft Cloud, or another cloud.

(Applause.)

CHARLIE BELL: Yeah. Continuing the multicloud theme, in Microsoft Defender, we're investing to give you all the security controls and insights you need to keep your systems protected from the first line of code to operating in the cloud, any cloud.

VASU JAKKAL: And in Microsoft Entra, we're expanding the capabilities of our internet access and private access products. These, you may remember, are the Security Service Edge solution we announced earlier this year.

CHARLIE BELL: And in Intune, we're introducing new solutions for advanced device management analytics to help you manage PKI and enterprise applications.

VASU JAKKAL: Charlie, there's no better way to show the power of our end-to-end security portfolio than to hear directly from customers who are using it. We are so thrilled to hear from WTW, how they are using the Microsoft Security portfolio. Let's take a look.

(Begin video segment.)

VOICEOVER: WTW is a global business services organization, which looks at risk mitigation and risk strategies.

We are protecting a lot of personal information, as our clients expect us to monitor, protect and secure their data. We have 55,000 workstations. We have about 17,000 workloads operating as infrastructure as service. But we also have platforms of service capabilities also running on Azure.

WTW technology has been going through a significant transformation exercise over the last couple of years, so much so that we've moved the majority of our technology stack into Microsoft Azure. Greater than 90% of our applications are all running in the Microsoft Cloud estate.

WTW’s technology strategy and security strategy is very much moving towards zero trust. And from an identity management perspective, the Microsoft Entra ID suite of tools is how we are going to manage identities, going forward.

Our security tooling is really based around the Microsoft Defender on both workstation and cloud. And we feed that into Microsoft Sentinel as our SIEM of choice.

As we migrated into the Defender and Microsoft Sentinel ecosystem, away from our legacy tool sets, working with our partner, we were very conscious of the amount of data that we were storing and processing. And we changed the profile of data going into our SIEM from almost 15 terabytes a day to less than 3 terabytes a day, which completely changed the cost profile of processing our security data. If you look at the ecosystem, which is the monitoring and telemetry ecosystem, we saved to the order of magnitude $5-$6 million a year.

Microsoft Security Copilot, I envision as being a change accelerator. It’s going to allow me to really change the metrics in how I measure my security operations. One of the real advantages that we get from the Microsoft Security Copilot is the ability to do threat hunting at pace, which means that I’m able to reduce my meantime to investigate. And the quicker I can do that, the better my security posture will become.

We are embedding security practices and principles within everything we do. And that, to me, is success, because if I can get the whole organization thinking that they need to think securely, and they need to protect data, then actually, we’ve won the battle.

(End video segment.) (Applause.)

VASU JAKKAL: Well, I hope you enjoyed that. We are so grateful to WTW for being part of our journey.

Now that we’ve seen how generative AI is supercharging your work in IT, let’s take a look at how we secure and govern the use of AI across our organizations.

CHARLIE BELL: We talked a lot about how we use gen AI to do security. But you’ll use gen AI across many facets of your work in life. To help you innovate confidently using gen AI, we have to ensure that security is built into the foundation as you develop new gen AI capabilities, and you have the security tools to protect them. As Scott shared in his keynote, Microsoft’s Responsible AI framework ensures that we are building, deploying and using AI with safety, security and privacy at the center.

In addition to the work we are doing on responsible AI, we also have to make sure that we are building foundational technologies, and we are really looking around the corners. This is the secure future initiative that we recently announced. It’s not just about threats we see right now, but anticipating the future threats, and building the security we need today to prevent those attacks tomorrow.

The first part of this is that we’re transforming the way we build software and making sure that we build securely as it’s just built into the process. It’s a dynamic, secure development lifecycle. As you know, we launched the Secure Development Lifecycle 20 years ago, and now we’re evolving it for the new age of AI.

We’re also strengthening identity protection, and we’re setting a new standard for the speed at which we address vulnerabilities. As I said in the beginning, attackers are moving much more quickly, and our ability to move even more quickly than they do is critical.

In addition to the security at the heart of our product development, we’re also investing in tools and guidance to help you manage AI specific risks, and build AI applications securely. And we, at Microsoft, uniquely enable you all to securely govern AI, including Microsoft Copilot and third-party generative AI, with new capabilities across our security product portfolio.

We’re excited to share all this with you today.

As organizations worldwide adopt generative AI in their work, their security teams are in a unique position that they must decide which apps are best for their users, as well as the protections needed to keep their data safe. This is a broad spectrum of generative AI applications, and they need different protections based on the risks these pose.

For example, some apps might not meet your security standards, and you may need to limit the use of those apps. For others, you might need some controls to enable organization-wide adoption. You need to understand your use of AI, protect the data it uses or creates, and govern the way it is used.

VASU JAKKAL: Let’s start with understanding the use of generative AI, so critical for us today, because we are all using it.

Yesterday, we announced that Defender for Cloud Apps has extended its rich discovery capabilities to over 400 generative AI apps. Now, Defender for Cloud Apps lets you see all the AI apps news, understand the associated risk with it, and you can approve or block the use of an app.

And the new AI Hub in Microsoft Purview gives your security team valuable insights into AI activity, including an aggregated view of the sensitive data flowing into AI, and the number of users interacting with AI. That’s for both Copilot for Microsoft 365 and other commonly used consumer AI tools.

So Purview and Defender together help you understand your use of Microsoft Copilot, as well as non-Microsoft AI.

CHARLIE BELL: Right, Vasu. Next, you need to think about how you protect the data that AI accesses and creates. In Microsoft Purview, we continue to strengthen AI-specific capabilities to do just that. Purview's protection capabilities are built into Copilot for Microsoft 365. The output of Copilot inherits the same sensitivity labels as the files that were referenced when you draft with Copilot. And similarly, in Copilot Chat, the conversation also inherits the label.

VASU JAKKAL: That's great, Charlie. And last, let's dive into how we govern what users do with AI.

In Purview, we're also providing compliance controls for Copilot, so that you easily comply with business or regulatory requirements. As an example, you can detect policy violations and communication compliance for Copilot prompt and responses. These are just a few examples, and this is just the start.

We, at Microsoft Security, are deeply committed to helping you protect your data, no matter where it lives or travels, including your AI data.

As you heard from us today, AI is changing our world forever. And it's empowering us to achieve the impossible, to elevate the human potential. We are thrilled to use generative AI for security and to provide security for AI. These innovations will usher in a new era that finally tips the scale in favor of defenders.

CHARLIE BELL: Security is the most defining challenge in our world today. It's the No. 1 priority for organizations. And perhaps, we have one of the most consequential technologies on our hands in AI, which is going to change the future. But we're at the very beginning, and it's going to take a village to build it, to use it and to support it.

Microsoft is privileged to be a leader in this effort and committed to a vision of security for all. Now more than ever, let's secure the world together.

Thank you all for what you do and thank you for being here.

VASU JAKKAL: Thank you.

(Applause.)

(Video segment.)

END