**Satya Nadella: Introducing Microsoft Security Copilot**
**March 28, 2023**
**Vasu Jakkal, Satya Nadella, Charlie Bell, Holly Steward, John Lambert, Jessica Payne, Bret Arsenault, Emma Smith, Brad Smith**

**VASU JAKKAL (Narrating):** Your world, the world is made up of your people, data, ideas, and everything valuable to your organization can't exist in isolation. It needs to move, connect.

Every day, security gets more complex.

You need a way to defend your world wherever it goes. So your people can work confidently from anywhere.

The answer is here. It's all of us working together to keep each other safe across the entire digital journey.

Getting ahead of threats, putting AI to work, using a comprehensive approach to do more with less, a way to protect it all, so your world and the people who are part of it can keep moving forward, fearlessly into tomorrow.

**VASU JAKKAL:** I'm so thrilled to welcome you all to Microsoft Secure, our inaugural event designed to bring together security thought leaders and professionals from around the globe, as we look at challenges facing organizations today.

Over the course of our program, we'll explore best practice strategies to empower defenders in this highly dynamic security environment, share insights into the current threat landscape, and outline our vision for the future of security. We'll also be making some exciting announcements that will reshape the way defenders think about security and strengthen your organization's security posture.

Following our mainstage program, you'll have an opportunity to go deeper into a variety of topics in our breakout tracks. All the content is available to you on demand, so you can take advantage of it at your convenience.

Now to get us started, I'm delighted to introduce Microsoft's chairman and CEO Satya Nadella.

**SATYA NADELLA:** Thank you very much, Vasu, and thank you to everyone for joining us today.

We are here today to discuss one of our most pressing challenges: cybersecurity. And we'll talk about this of course in the context of the new era of AI.

The contours of this next platform shift are becoming clearer by the day as more and more people have had a chance to interact with these powerful new foundational models like OpenAI's GPT-4.

At Microsoft, we are excited about what's possible when we can combine these advanced AI models with domain specific and task specific data, context and skills, and to help remove the drudgery and improve the effectiveness of our work and actions.

That's how we have fundamentally transformed developer productivity with GitHub Copilot, low-code/no-code code development with Copilots in Power Platform, every business process from sales to marketing to customer service with Dynamics 365 Copilot, productivity and knowledge work with the Microsoft 365 Copilot, and the way millions of people synthesize information through conversational search, changing our daily web and search habits with the new Bing and Edge Copilot for the web. Across all these copilots, our design center has been to put humans and human agency at the center of the product and to ensure that they are as empowering as they're powerful.

Of course this empowerment does come with greater human responsibility. As we move into this new era, all of us who build AI, deploy AI, and use AI have a collective obligation to do so in ways that foster positive impact and promote trust.

When it comes to security innovation. This means three specific things. First, your data is always your data, yours to own, yours to control, yours to use as you see fit.

Second, your data isn't used to train foundational models that others can use. It stays within your organization.

And third, we protect your data and AI models with the industry's most comprehensive enterprise compliance and security controls.

Frankly, the cybersecurity threat landscape has never been more challenging or more complicated. Today, cyberattacks cost the world $6 trillion annually, and that number is projected to rise to 10 trillion by 2025. And as digital technology becomes more pervasive, it's a place where all of us will need to do some of our very best work.

At Microsoft, we're helping organizations of all sizes adopt a zero trust architecture that spans all clouds, all platforms, while reducing complexity, cost and risk. But it's also a real-time intelligence game for us. It's about how we translate our products and the trillions of threat signals we see every day into one feedback cycle to improve operational security posture.

This was our motivation to build that integrated set of end-to-end tools, spanning identity security, compliance, device management and privacy, that both feed and are informed by the 65 trillion signals each day.

Today, we take the next big step forward into the new world of cyber-operations that augments every security role by combining advanced AI models with security optimized infrastructure, threat intelligence and skills, to reduce complexity, deepen understanding, and quicken the response times. This, we believe, will open doors to entry level defenders at a time when cybersecurity workers are sorely needed, empower highly skilled analysts to focus on the next

level of cyber risks, and transform every aspect of the SOC productivity from threat detection to hunting to incident response.

Together, we can give the agility advantage back to defenders to build a safer and more secure world.

And with that, I'll hand it over to Vasu to share our Copilot for Security.

**VASU JAKKAL:** Thank you, Satya.

As Satya noted, security is a defining challenge of our times. Just since September of 2021, the number of password attacks per second has risen from 579 to 1,287, and the median time for an attacker to access your private data if you fall victim to a phishing email is only one hour and 12 minutes.

Add to that a global shortage of 3.5 million skilled security professionals, and it's no wonder that security incidents have become an everyday occurrence in organizations of every size, in every industry, and in every part of the world.

So how do we tip the scales in favor of defenders? How do we scale humans more effectively, and utilize them more strategically? The answer is we need a paradigm shift.

Human ingenuity and expertise will always be a precious and irreplaceable component of defense. So we need technology that can augment these unique capabilities with the skillsets, processing speed and rapid learning of AI, technology that can work alongside us, detect hidden patterns and behaviors, and inform their response at machine speed with the latest and most advanced security practices.

That's why I'm thrilled to introduce Microsoft Security Copilot, the first security product that empowers defenders to move at the speed of AI. It will radically accelerate defensive capabilities against threats, provide critical insights when you need them, and help you anticipate and act before an attackers next move.

Microsoft Security Copilot is the first and only generative AI security product that builds upon the full power of GPT-4 AI to defend organizations at machine speed and scale. It continuously learns from Microsoft's unmatched Global Threat Intelligence, security data and skills to deliver tailored insights, hardened defenses and faster response.

With Security Copilot your data is always your data. It stays within your control, and it is not used to train the foundational AI models. In fact, it is protected by the most comprehensive enterprise compliance and security controls.

To help us understand more about how Security Copilot can empower defenders. I'd love to welcome my dear friend and colleague, Executive Vice President of Security, Charlie Bell.

**CHARLIE BELL:** Well, thanks Vasu. It's so great to be here with you and to be able to make this exciting announcement.

**VASU JAKKAL:** Charlie, it would be great for you to tell us what makes Security Copilot different from an AI chatbot.

**CHARLIE BELL:** This is really a better together story. Security Copilot combines the most advanced GPT-4 model from OpenAI with a Microsoft developed, security specific model, powered by Microsoft security's unique expertise, Global Threat Intelligence, and comprehensive security products.

Now, if we look specifically at what Microsoft has built, you can see that Security Copilot is running on our security and privacy compliant hyperscale infrastructure that's unique to Microsoft and brings the full benefit of being on the Azure Cloud. Then we add our cyber-specific model. This creates a learning system that has an ever growing set of security specific skills.

Additionally, cyber-specific model uniquely combines Microsoft's evergreen Global Threat Intelligence informed by 65 trillion daily signals. And finally, Security Copilot integrates with the end-to-end Microsoft security portfolio of solutions. And over time, it will work with a growing ecosystem of products from third party vendors.

So you can see how Security Copilot is not only an open AI Large Language Model, but rather it contains a network effect, enabling organizations to truly defend at machine speed.

**VASU JAKKAL:** Charlie, this all sounds amazing. So let's take a look at what Security Copilot can do and how it works.

Meet your new Microsoft Security Copilot. If you've ever been involved in a security operation center investigation, you know it's a complex process, more open screens and tabs than you can count, alerts and incidents popping up all the time.

Security Copilot is different. It helps you simplify and focus. At the center is the prompt bar. You can ask a natural language question like, what are the latest trending security threats this month, or you can ask about incidents in your enterprise. You can also ask it to summarize a vulnerability. You can just type a prompt, or you can feed in a file, URL, or code snippet. You can also ask for information about incidents or alerts from your other security tools. And this is important: Your data is your data. What you input here stays within your control.

**CHARLIE BELL:** These buttons above the prompt bar are suggestions from Security Copilot based on its observation of your work.

Now, this is a first run experience. So these are preloaded for the sake of this demonstration. We're going to click on this one to understand more about this vulnerability.

Now, as I've engaged this prompt experience, I've started an investigation. All investigations can be organized and accessed at any time.

Core to Security Copilot is an immutable audit trail, so that an organization can always go back into the investigation to understand exactly what data went in and what came out. This is an important part of transparency for Responsible AI that has been designed in from the very start.

**VASU JAKKAL:** Security Copilot uses AI to generate a response to the prompt based on what it finds externally and internally to your organization that is relevant to your prompt. Here we can see a succinct summary of a vulnerability, and we can see where this information was so strong.

I can edit the prompt if I want to correct or adjust a single Copilot response. And if I find something that is useful to my team, I can pin it to my pin board. My pin board holds the responses that I'm finding through my prompts as I work through the investigation. And once I pin things here, they dynamically update. I can share my findings, export them, and collaborate on them with others.

**CHARLIE BELL:** That's right, Vasu. You can invite team members to collaborate. As you bring them in, they can see your pin board. They will also have their own private workspace for their investigations, and they can contribute back to the collective understanding in the final report.

Now, we've had one prompt and response here, but this is an ongoing investigation. So I can ask further follow-up questions that refer back to previous prompts. When I say, which devices are impacted, Security Copilot knows that I'm talking about the vulnerability that I asked about just prior in the same session.

**VASU JAKKAL:** Now, Security Copilot doesn't always get everything right. Here, Security Copilot has come back with an answer that includes Windows 9, which doesn't exist. AI generated content can contain mistakes, but Security Copilot is a closed loop learning system, which means it's continually learning from users and giving them the opportunity to give explicit feedback.

I showed you earlier how you could adjust a single prompt and response, and I also told you that your data is your data. Here, we've made it easy for you to decide when you want to share the feedback with us, so we can make Copilot even better for your continued use.

So here I'm able to give you a correction. I can indicate whether the response was incorrect, unclear or maybe incomplete. I sent it off, and Security Copilot expresses appreciation. How cool is that?

So there we are, Charlie. Now that we understand what Security Copilot is, let's take a look at how an investigation can be performed using it.

For that, I'd love to welcome our awesome research analyst. Holly Steward. Holly, welcome.

**HOLLY STEWARD:** Hey, Vasu Hi, Charlie.

**CHARLIE BELL:** Holly, I know you have done a lot of this kind of investigative work. Will you show us how Security Copilot could boost you and your team?

**HOLLY STEWARD:** Yes. I'm going to show you a ransomware example that Security Copilot helped navigate. Normally, getting to the bottom of a ransomware incident, as you can imagine, requires a lot of complicated investigative work just to understand what happened, much less mitigate it. So this is a great example that demonstrates just how Security Copilot can help me deal with an immense amount of information and get what's important in just a few steps.

These are real Security Copilot responses related to ransomware that was delivered through OneNote attachments. You may have heard of that about a month back. As I walk you through this, I'll give you a summary of what was happening behind the scenes, essentially all of the work that Security Copilot can do for me.

Okay, so we start this investigation through an alert from Microsoft Defender for Endpoint. They see the machine that was potentially compromised, some details about the attack and how it played out on this machine. I even have a nice visual graph that's automatically shown to me in case that visualization is easier for me to process mentally than text.

You can see Security Copilot put together the story of what happened using data by interpreting and summarizing log files and alerts and threatened diligence. Normally, I'd have to manually pull this data from many places, summarize the indicators, and then correlate them to the threat actor by searching blog posts and Intel sources; then use visualization software to create the chart. All the while, I'm hoping that I haven't missed something. At least a few hours of work, Security Copilot can do for me in seconds.

**CHARLIE BELL:** So what you're seeing here is a new capability with Security Copilot to bring all available information into one session, eliminating fragmentation across various security tools and information resources, so that security teams can catch what might otherwise have been missed by today's siloed approach to security.

**VASU JAKKAL:** Holly, that visualization is really cool. Is it being generated on the fly?

**HOLLY STEWARD:** Yeah, it is. And I'll show you another one in a minute.

Okay, so that was a good high level summary of what happened, but I need more than that. How far did this attack go? Was it actually successful? Not all attacks are. Was there an account compromised that I need to worry about?

Security Copilot has this feature called Prompt Book. It's a collection of prompts, essentially steps or automations that either I or a person on my team has developed to learn more about an incident like this. It actually suggested that the Malware Impact Analysis Prompt Book would be a good next step in my investigation. So let's run it.

In this example, it's helping me identify other indicators of compromise that occurred on this machine or from this account around the time of attack.

**VASU JAKKAL:** So this is kind of like giving you additional processing superpowers, right, Holly? All these investigation steps you would have normally done yourself; you're now asking Security Copilot to go do all at once.

**HOLLY STEWARD:** Exactly right. So now all I have to do is focus on deciding what's most useful to compile in my pinboard. I pin the useful results and share them out to the team.

**CHARLIE BELL:** Security Copilot is a bit like an interactive notebook. You're building your company's knowledge base as you go.

**HOLLY STEWARD:** You got it.

So the first example pulled together information about the threat, saved me hours of reading, processing, synthesis, but I have those skills. I could have done those queries myself.

But this next example is different. And honestly, when I realized Security Copilot could do what I'm about to show, I was astonished.

So I don't have a reversing background. And by reversing, I mean bisecting malicious code to understand what it does. One of my coworkers asked Security Copilot to reverse engineer an obfuscated script, and it did it. They saved that prompt into a prompt book. So now, I or anyone really on my team can use it.

In this example, it reverse engineered the PowerShell script that downloaded the malware, explaining what it did step by step in a way that pretty much anyone could understand. I don't know about you, but when I saw that Security Copilot could do something like this, it just felt like a game-changing moment for our industry.

So the full impact of this attack is getting clearer now as new data is rendered into this graph. You'll also see how we can use a Containment Prompt Book to isolate compromised devices from the rest of the network, which saves a bunch of steps, as you can see, and finally search for and remove any remaining malicious mail related to this attack.

**CHARLIE BELL:** What's so exciting about this is that Security Copilot is assisting with certain work, so Holly's expertise is better scaled and optimized towards solving the problem at hand. It also has great benefits for skill building. The tool can help experienced analyst adapt their role. It can help a less experienced analyst to execute a Security Prompt Book and build their tradecraft and skills by learning in a very hands on way.

**VASU JAKKAL:** And one of the things I love is that over time, AI technology like Microsoft Security Copilot can help to level the playing field for entry into the field of cybersecurity by breaking barriers such as language, access to data and training. It's exciting to think we can use

AI to develop and grow a larger and more diverse community of security defenders, a cause that's certainly close to my heart.

**CHARLIE BELL:** The skills built into the model are what makes Security Copilot so different from an AI chatbot. It's one of the most exciting aspects of this technology.

Let's keep going.

**HOLLY STEWARD:** We're getting to the final stages now. You can see the full complexity of the attack taking shape. It's one thing to respond to and contain an incident, but putting together information to share with my team and leadership takes a long time, too. In addition to the incident itself, it's critical to learn from this incident and make security improvements to defend against something like this in the future. Security Copilot helps me with that, too.

Here's the full incident in graph format, and this highlight here shows just what we started with. Everything else on here is something I may have missed if I didn't have Security Copilot.

And as the final step, I can create a PowerPoint deck to share even more broadly with my organization.

**CHARLIE BELL:** You can see how Security Copilot can simplify the complex by assembling information end-to-end across individual domains to create a complex, complete incident graph. And as you build trust by working with it over time, you can begin to enable it to take action on your behalf, subject to your approval, of course.

**VASU JAKKAL:** Now that you've seen the new Security Copilot in action, let's go behind the demo and explain more about how it works.

To start, Microsoft Security Copilot is not only an OpenAI Large Language Model, working with your security technology, as Charlie said before. It's so much more. Microsoft Security Copilot builds on the latest innovation in Large Language Models and uniquely goes beyond that, harnessing the foundational power of Microsoft's Security expertise, intelligence and technologies, to deliver tailored capabilities for security specific use cases.

As you saw in the demo, the first thing you do is ask a question or give a command through the prompt. Security Copilot makes your prompt better with a system, which has a rich set of growing cyber skills. The Copilot's underlying models are security specific and built on deep Microsoft security knowledge and continuous learning. It further adapts to the security domain using techniques like fine tuning, including the feedback you've chosen to share with us.

The system then grounds your prompt with fresh threat intelligence, informed by Microsoft's 65 trillion signals and human intelligence. It also connects directly to not only insights, but also to the end-to-end Microsoft Security product portfolio, which helps strengthen the data and reduce mistakes, to close the learning loop.

Finally, it translates the response according to your prompt instructions, using the capabilities and magic of Microsoft's sophisticated system. This can take the form of text, code, or a visual that helps you see the full context of an incident, the impact and the next steps you should take to deepen understanding or take action directly for remediation and defense hardening.

**CHARLIE BELL:** And it all comes together with Security Copilot at the heart of the Microsoft Security product portfolio. We deeply integrate Security Copilot with our existing product experiences and workflows across defender, Sentinel, Intune, Entra, Purview and Priva so that security professionals will see the full benefit of Security Copilot's assistance as they go about their daily work. And it will work with third party security products and data as well. We expect to share more about that soon.

**VASU JAKKAL:** So as we think about the value that Security Copilot can bring to organizations is threefold, like you said before, Charlie. It simplifies the complex, it catches what others miss, and it helps you address the talent gap.

**CHARLIE BELL:** That's right. Security Copilot helps you be more effective and efficient at all the roles you play. It helps you enhance and grow your capabilities and skills, while also supporting the workflows and teams you collaborate with to solve security challenges.

**VASU JAKKAL:** And we absolutely believe that security is a team sport, which is why we've made significant investment in expanding the protection of Microsoft security products across a broad ecosystem of more than 15,000 technology and managed services partners. They are a critical part of our business strategy, and essential to our commitment of helping customers protect everything. We're looking forward to giving our partners access to the world's leading security AI platform, so that together we can deliver better security outcomes.

**CHARLIE BELL:** That's absolutely true. Vasu. We'll be talking more about this in the coming months.

**VASU JAKKAL:** Charlie, now I'd love for you to highlight a really important thing, how we are employing Responsible AI principles in the development and the usage of Security Copilot.

**CHARLIE BELL:** We take a people-centered approach to the research, development and deployment of our AI-powered products. That means embracing diverse perspectives, fostering continuous learning, and being agile in our responsiveness as AI technology evolves.

**VASU JAKKAL:** Charlie, it's such a privilege to work with you every day. Thank you so much for being here with me at Microsoft Secure.

**CHARLIE BELL:** Thank you, Vasu. It's been really exciting.

**VASU JAKKAL:** As Charlie mentioned, Microsoft Security Copilot is a game changer. empowering you to defend at the speed of AI and helping you meet the challenge of the mission we share to protect one another, to protect our communities, and to create a safer world for everyone.

To learn more about how this technology can help you and your organization, I encourage you to take a look at the resources listed here.

Now, one of the most exciting aspects of Microsoft Security Copilot is its capability to integrate the power of evergreen threat intelligence with the speed and scale of AI. Here to help us understand how the two together have the ability to reshape the future of security is Microsoft's Distinguished Engineer and the head of Microsoft Threat Intelligence, John Lambert.

**JOHN LAMBERT:** I'm John Lambert, Corporate Vice President and Distinguished Engineer of Microsoft Security Research. I'm excited to be with you today. I want to tell you how threat intelligence and artificial intelligence together are sending your security folks some sorely needed reinforcements.

If you're an observer of cybersecurity, it's often hard to see the progress. Reports of doom and gloom abound. And yet every day, there are stories of success. Defenders are quietly sharing information, raising costs for attackers, and evicting them earlier and earlier.

And the world is fighting back. One of the perpetrators behind the ransomware attack on Kaseya was arrested when he traveled. Microsoft contributed critical information to that law enforcement case. In another win, the FBI infiltrated the Hive ransomware gang. Now, this ransomware gang had targeted over 1,500 organizations around the world. The FBI was able to use their access to provide decryption keys, preventing over $130 million in payments. So law enforcement action and the cooperation behind the scenes is helping bring some of these threat actors to justice and relief to victims. In another case, Microsoft took Strontium, a Russian threat actor connected to the GRU, to court to seize domains that we're using in attacks. Strontium didn't show up.

So threat intelligence is having an effect. Dwell Time in networks by adversaries is down from hundreds of days to around 20 days. This is much better than the months that they were able to lurk in networks undetected in the years before. What's making the difference? Better tools and better threat intelligence. So there has been progress. And there are reasons for hope.

In my 20 years at Microsoft Security, I feel like this is a special moment. We're in kind of this liminal state for a long time where we're going from one world to a new world that we're starting to see today. And often these new days are a result from a coming together of several forces. Let me explain what I mean.

So some practices stack together, like if you get good sleep, you'll have more energy. If you have more energy, you can exercise more. And if you can exercise, you'll have better health. Each one is good, but they all help each other. And the three stack forces that compounded together to accelerate each other for this moment is data at scale, threat intelligence, and artificial intelligence.

So data – data is how defenders see. Cloud competition has driven down the costs of holding querying data, permitting higher resolution sensors across the digital estate. The rise of XDR

plus SIEM has expanded data and signal from endpoint to app to identity to cloud, and that signal provides more surface area for threat intelligence. And then TI feeds AI, acting as labels and training data, helping to predict the next attack from today's attack. So what TI can find, AI helps scale. The intuition and experience behind an intelligence win can be modeled digitally with today's algorithms that use millions of parameters against our 65 trillion signals.

So let me zoom into TI. At Microsoft, we take an adversary-centric approach to threat intelligence. We're tracking 300 groups, including 160 groups that we linked to nation-states, 50 gangs that we linked to ransomware, and many hundreds more that we're tracking.

We take a multidisciplinary approach. We have cybersecurity SMEs working alongside applied scientists with expertise in data science and machine learning. And then we're complemented by geopolitical experts and experts in disinformation. This allows us to take a whole of adversary approach where we can understand the cyber-technicals, the what of an attack, the why it might be happening, enriched with geopolitical information to help predict where an attacker might go next.

So one great example of threat intelligence in action is Ukraine. We've just passed the one year anniversary of the invasion of Ukraine. Microsoft's greatest area of effort has been defending their digital infrastructure. Microsoft has provided over $400 million in assistance to Ukraine, and we've taken our actor tracking approach. We were the first to report on a wiper attack in Ukraine the month before the invasion. We began a threat intel airlift and have sent over 250 actionable intelligence tips to the Ukrainian government and private sector.

In one case, we saw Russian groups targeting a power plant in Ukraine, and that same night we were able to get in contact with those defenders at that power plant. They immediately went into action. They contacted the Ukrainian Cert and ESET and was able to contain the attack. That is the attack known as Industroyer2. Honestly, it was incredible to see defenders half a world away intervening in real time to prevent an attack intended to turn off the power.

We've also reported as Russian attacks related to Ukraine have spilled outside of Ukraine. In a recent report, we talked about how the prestige ransomware malware attack transportation companies in Poland. So TI in the right hands can make a difference.

Now, you could ask, how does Microsoft threat intelligence get into your hands? Well, let me talk about operational, tactical and contextual TI.

The best thing that we can do is prevent an attack or interrupt it automatically from happening to you. So every day, threat intelligence comes down and is built into the security products to block attacks. Let me give you a concrete example.

So, what if an attacker finds a weak link in your network and a user runs something they shouldn't? In this case, the Raspberry Robin worm had used an infected thumb drive as its initial access factor. When the user ran it, it was attempting to download a payload from a command and control domain. Now this is the moment where a ransomware operator could come and get in and begin an escalation.

That endpoint was protected by Microsoft Defender for Endpoint's Network Protection feature. Network Protection integrates deeply in the operating system. It doesn't matter what browser or application is doing the connection. Network connection – Network Protection can block that command and control, and in that case, it blocked that malware from downloading a TrueBot download. So this is an example of operational TI connected to products, helping stop attackers from progressing further in their attack.

Let me give you an example of tactical threat intelligence. As I mentioned, we're constantly hunting threat actors. If we find an organization has been targeted or compromised by a nation-state actor, we send a notification to that customer, a nation-state notification. We have sent over 67,000 of these in total. These notifications are beyond an alert, and they serve an important tactical role because a nation-state is likely to try over and over again if they were targeting somebody.

And then we know defenders benefit from context, like what attacker is behind this attack, and how do I start with what Microsoft already knows about them? So context can help defenders understand and then prioritize their approach to attacks.

So Microsoft Defender Threat Intelligence now comes with the latest intelligence profiles. It integrates into Microsoft 365 Defender, and it's been enhanced with an API to help enrich incidents, automate response, and integrate with the best of the ecosystems tools.

So those are some examples on how operational, tactical and contextual threat intelligence from the Microsoft Threat Intelligence community helps your defenders. There's a session later today on Microsoft Defender Threat Intelligence with Dean and Elda, and they're going to go into a lot more detail.

So turning the page to ransomware, organizations are not just up against a threat actor; they're up against an entire economy of access brokers, affiliates and operators. We use our 65 trillion signals to build a detailed map of these groups and all of their interrelationships.

Jessica Payne is here to share some insights.

**JESSICA PAYNE:** Hi, Dan.

**JOHN LAMBERT:** Hi. We often hear what's not working. Can you tell us about some practices that are working? What are some things defenders are doing that is working?

**JESSICA PAYNE:** I'm a security optimist, so I love this question. The good news about ransomware is it's a largely preventable threat. No matter what payload they're using, they're all taking advantage of the same common security weaknesses. If you can see where those threats overlap, you can then apply mitigations for them.

Almost every ransomware attack involves attackers gaining access to highly privileged credentials. So it doesn't matter if the attacker is using BlackCat or Revil or Hive, they're going

to be using the same techniques. And the good news is that you can solve these things with built-in tools like group policy and event logs.

Attack Surface Reduction Rules are another thing that really help out here. These are again, something that's built-in with Defender Antivirus. Blocking Office from creating child processes is one of these Attack Surface Reduction Rules. And these opt-in rules allow you to harden your network so that when new attack techniques come out, you're not going to actually experience them.

An example of this with blocking child processes from Office was when OneNote was discovered to be able to launch malware recently. Customers who had enabled that Attack Surface Reduction Rule actually didn't have that impact them at all. We see a dramatic reduction in incidents and alerts in customers who have turned on Attack Surface Reduction Rules.

We have this and much more in our hardening guidance in our Ransomware as a Service blog at aka.ms/RansomwareAsAService.

**JOHN LAMBERT:** This prevention work is just essential. I often say that prevention and detection, they're not peers. Prevention is detection's guardian, because it quiets the network and allows defenders to find the most important things.

What would you say to a customer who's just having a hard time staying on top of all the changes to this complex ecosystem?

**JESSICA PAYNE:** I always say that good threat intelligence is as much about what you don't have to worry about. If you've already taken care of the technique that an attacker is using, you don't need to worry about it.

Threat intelligence reports come out daily. There's hundreds of thousands of them. Our approach with Microsoft Defender Threat Intelligence is to share the insights of our researchers, alongside of the techniques that the attackers are using, using the insights that we can gain from M365D with threat analytics, so that you can see whether or not the attacker's techniques have already been mitigated in your environment, so that you don't necessarily have to worry about it, or if the attack is already in your environment.

We use that intelligence also to power contextual alerts that let you know which is the most important alert to respond to in that day. So we demystify it, letting you know what happened and how you can harden your network to prevent it in the future.

**JOHN LAMBERT:** Thank you, Jessica.

And is there a way that people can hear more about this later today?

**JESSICA PAYNE:** Yeah, absolutely. In Microsoft Secure today, I'm doing a breakout session with my friend Jeff from Defender Antivirus about how TI and AI work together. We'll also be

hosting an Ask the Expert session with some of my colleagues and me where you can ask us questions about ransomware.

**JOHN LAMBERT:** Thank you, Jessica.

**JESSICA PAYNE:** Thank you, John.

**JOHN LAMBERT:** This is how the Microsoft threat intelligence community is hunting actors across the globe using the 65 trillion signals to find the attacks that matter most, provide intelligence context to help prioritize them, and build protections into the products that you're using. The threat intelligence reinforcements are here.

One of the things I've said over the years is that attackers think in graphs. They understand connections and dependencies and pivot points in your network. What if AI could view the network as a graph and turn low confidence signals into an early warning system? Let me walk you through an example of that.

To disrupt human operated ransomware early, we've enhanced the AI-based protections in Microsoft Defender for Endpoint with a range of machine learning techniques that focus on incrimination. Incrimination is determining malicious intent and underlying behavior, and it reasons over files, processes, users and more.

Now normally, investigators would piece together these individual things from clues, but in a ransomware escalation, there's just no time to do that. But with the same mindset, AI can use incrimination to do it at machine speed.

What makes incrimination possible is linked context. Humans think on multiple levels. Microsoft Defender for Endpoint combines three kinds of AI-informed inputs. At the organizational level, it uses a time series analysis and statistical analysis of anomalies. At the network level, it constructs a graph view to identify malicious activity across multiple devices. And at the device level, it's using monitoring of behavior and threat intelligence hits to identify high confidence activity. These are all used together to find ransomware attacks at the very beginning of escalation. So TI feeds AI, and AI scales in real time at machine speed.

We're at a new era in artificial intelligence. ML is commonplace, but it's often deep inside the tech. Customers benefit from it, but they couldn't really interact with it directly. That changes today. We're going from a world of task-based machine learning, good at phishing or ransomware, to generative AI based on foundation models, and a world with copilots that can simplify the complex, catch what others miss, and address the cybersecurity talent gap by bridging critical knowledge gaps. Copilots will upskill defenders everywhere. Those heroes defending organizations around the world finally have some reinforcements,

TI and AI combine to help defenders go faster than ever before. I'm excited to see what you're going to do with it. And I know that whatever it is, together we will better protect the planet.

**BRET ARSENAULT:** Welcome. This is an important time for our industry. We're all working to manage increased risk, while enabling our business amongst recessionary headwinds. In the last two years, the number of password attacks has risen from 579 to 1,287 per second. The median time for an attacker to begin working laterally within your network if a device is compromised, less than two hours. What's more, the average cost of a breach hit a record high in 2022 of 4.35 million U.S. dollars.

As a CISO at Microsoft, my team and I are focused on how we can accelerate and operate at the speed of the current security landscape, and constantly evolving threat environment. Three things that are top of mind to me – one, ransomware. Ransomware attacks represent one of the most significant factors organizations are facing today globally. Two, recessionary headwinds, security is not the elimination of risk, but driving down the total overall cost. And three, the regulatory environment. We're currently monitoring over 230 regulatory changes per day globally. When I couple all of this together, it's no wonder organizations on every size in every industry on every part of the planet are all struggling to keep pace.

So with this in mind, I'm really excited to be here today to share some about how we protect Microsoft and talk with my friend and peer, Emma Smith, the cybersecurity, technology, assurance and strategy director at Vodafone, who will share her insights on the road ahead and provide additional CISO perspective on what's top of mind in the climate today.

I hope you'll leave this session with three things. One, a valuable perspective on what's going on in the industry. Two, insights on what's top of mind for a CISO. And three, a clearer view of the Microsoft Security Strategy.

Emma, thank you for joining me today.

**EMMA SMITH:** Hi, Bret. Great to be here. Great to see you.

**BRET ARSENAULT:** And it's awesome to see you.

Hey, let's start off with a simple question. What's top of mind for you?

**EMMA SMITH:** Well, there are really challenging headwinds, as you say, Bret, and let me give a European perspective. We've got a war taking place between Russia and Ukraine, and none of us thought we'd experienced that in our lifetimes; energy prices that are growing exponentially. As you mentioned, the regulation is changing in all the countries that we operate in. We've got volatile supply chain prices, the cost of living increase, and the cyberthreat is really volatile. And on top of that, the cyber workforce is in really high demand. And so maintaining that workforce in a steady state is really challenging. And I think it's really important that we understand those headwinds, all those tensions to make sure that our strategy still remain focused in the right areas.

I also have a few other things top of mind. You mentioned ransomware, and that's a threat I think everybody's concerned about, who works in our industry. Also, the trend of increasing

compromised or compromising users in order to get to companies, whether that's suppliers or contractors, employees, or customer is a real target on trying to compromise their accounts.

And then we're really focused on supply chain security, and how do we help elevate security across the supply chain, and make sure we've got a really clear understanding of cyber-resilience. And I think there's more we can do to support our supply chains and our partners that we work with.

And then lastly, thinking about how we spend our money and invest in this time is really important. So we're focused on making sure that everything we spend balances threats, maintains the momentum inside the company, and that we really invest in controls that bring tangible risk reduction.

**BRET ARSENAULT:** No, those are great points. I think that everybody, as you said, even you said the people in our industry, and even people outside of our industry are worried about ransomware and all the things you talked about. So I think that's awesome.

When you think about this current economic climate, though, how do you prioritize? And where do you invest, right? Because I mean, I don't think you have an unlimited budget. I know I don't. And so, you have to prioritize where you invest, and you have a cutline. I'd just love to get your thoughts on how you prioritize.

**EMMA SMITH:** I've got a super limited budget, Bret. I think we all have. People and culture is really important. We focused on in-sourcing and building a capability in-house at Vodafone over the last seven years, and I plan to continue with that. So having the right depth of expertise inside the team, I think, is vital.

And then having the right culture in the whole company from top down is something that we need to keep investing in.

I'd say that continued focus on good cyber-essentials, patching, hardening, access control, vulnerability management, endpoint security, and so on, making sure we don't take our eye off the ball, those good solid foundations will always stand as in really good stead.

And then making the strategic shifts that we need to take, that take us to the next stage of security, so dynamic trust, or as many people call it, zero trust. Big data without the exponential cost; we really want to be able to access as much telemetry as possible. Continue to elevate automation and build on strategic partnership.

And then when I'm making investments, balancing those investments is really important. And so, we're working on a model to try and quantify risk and risk reduction, and understanding where we get the best benefit from the layers of control that we invest in, and also managing those supplier costs.

Bret, I'm really interested, how do you manage Microsoft in protecting Microsoft, and what are the elements that you're investing in?

**BRET ARSENAULT:** Yeah, it's a great question. I think many people have this confusion that like we run Microsoft, we only run Microsoft, right? We run 31 operating systems. I mean, my environment is very similar to yours.

And I think you raised really two good points. You talked about I think your second point around the core things. I think we called them the pedestrian part of the job is the, you know, patching and hardening, or I refer to them as the brilliant basics. You always have to be focused on the brilliant basics, and you can't – you can never let up on that. It's – it never goes away.

And I think, you know, when I think about that, and I think about what the threats we're facing, as you pointed out, what's happening in the threat landscape around attacking users, and how do you get at, whether it's your supplier, your vendor, your employees, your support people.

And so really, if I break it down, I think, number one, you know, we went to 100% multifactor authentication years ago, but we're seeing the attack patterns now go after multifactor authentication and taking advantage of users and, you know, 2FA fatigue and other things like that.

So you'll see us, you know, today, we're really moving to true fish-proof credential, so not just multifactor, but fish-proof. So Windows Hello is fish-proof, but all of our other platforms, we have to go make investments and enhancements in the ability to have fish-proof credentials, and especially with our high-risk population, some of the ones you mentioned.

Secondarily, I do agree that focus on the user is the most important thing, but we still worry about devices. With all the great technology that's helping us, if it happens, how do you limit the blast radius that may happen in that? And so, in our environment, getting everybody to run as a standard user, so that you can't run privilege programs and can't run privilege models is super, super important for us.

And then this comment about the workforce. This idea of a brilliant person once told me, you know, how do you get four times the productivity out of the same amount of dollar? And if I look at our Security Operations Center, for the last five years, they've been doubling the number of investigations and things that they have to look at, better telemetry, more and more events. And yet, we've reduced our meantime to remediate by 50 – by two times, right 2x, with doubling of the number of events, with less than 10% increase in actual human capital. And that's all done through good automation technology, machine learning.

And now it really as we advance into AI, when I think about the Security Operations Center, like, we don't have a lot of true polyglots that can speak like seven languages, but our attackers do. So how do you use Large Language Models and AI to actually do that work for you, which is not the thought of the process and the pattern, but actually just even the multilanguage issue?

So there's so many things we can do to make those people more productive. It's super important. And how do I take all this amazing signal intelligence as a company we have, all the threat

intelligence, which is very human operated, and turn that into really taking artificial intelligence and turning that to scalable intelligence that isn't for response, but actually to protect us?

And the last thing I'd say is, as you said about security is everyone's job, like really securing the developer pipeline, like how do you make sure that every piece of code that's written – most companies are in digital transformation – how do you make sure that we make it so that the developers fall into the pit of success? Automated code analysis, all the things that would give that and give me all the telemetry I need to understand where we have issues and really drive, you know, if you have cleaner and cleaner environments, whether it's from yourself or your vendors or otherwise, you need less response.

So when my teams are asking me for more response capability, I'm asking them how they're going to move to the left and shift it from ever happening in the first place. So that's really a big part of it.

And as you said, this vendor consolidation, how do I get from all my point-based, best of breed products to best of integration, because that's where I really get the most leverage for my people? And I think they find that to be the most useful. So those are probably the four big areas for us.

One of the things when I think about that's interesting is I mentioned, I run 31 operating systems, and I happen to run N+1. So I'm always running one version as we look at the next release of operating systems we're doing.

But, you know, if I think about Vodafone, you're like one of the most tenured companies I have ever worked with, and you have an amazing heritage that comes with that. But then how do you think about that with the legacy that comes with that, as well as how you think about innovations going forward, because that's a super interesting tension you have?

**EMMA SMITH:** And that heritage of the company is really important to us, because it was born on innovation in the telecommunications sector. So customer service and trust are really at the heart of the company, and we take our responsibilities to protect customers, particularly their communication data, really seriously. And how we maintain that privacy of our customers is very important.

And that's built a foundation of transparency. So we're very transparent when we talk about how we manage cyber-risk, how we manage privacy, and the disclosures that we do. And working on that foundation of transparency has been really important to build and maintain that trust with customers with stakeholders, investors, etcetera. We've even won awards for our annual report on cybersecurity, for the disclosures and the way we describe how we manage cyber-risk.

Tech telcos have always really pushed the boundary on innovation, and that continues. It requires really serious investment to maintain those networks across the world. And we're very focused on how do we keep expanding that coverage so that it gets to all of the parts of the countries that we operate in, and everybody has access to the services that we might take for granted in some cities or parts of the world.

We're focused on really pushing standalone 5G and all the benefits that come with that for our customers. We're working on open run technologies and hoping to start work on 6G and all that comes with 6G.

We've also just published a paper with GSM about post-quantum cryptography in telecommunications, and that really unpicked an approach to how to go about thinking about post-quantum safe crypto. So we looked at how to prepare now for something that we know is coming in the future.

We're a super heavily regulated sector, as you talked about, and the geopolitical tensions are rife. And so, we're very proactive in how we communicate and collaborate in the sector to the development of standards and regulations, to make sure that they are doing the right thing for customers but are also really practical to implement. And so, we really recognize the importance of being part of that discussion, dialogue and setting of those standards.

And then I'd also say that our operating model at Vodafone for cyber assumes that we'll never finish the job, and there will always be cyberattacks, and really focused on minimizing the impact of those attacks. But our model assumes that we're always learning, always improving. It's based on the NIST lifecycle.

Bret, I'm really interested; how are you preparing for the future, and what are the innovations that you're excited about?

**BRET ARSENAULT:** Yeah, it's interesting. I think, well, there's a lot of things that I'm excited about. You know, obviously, it's a fascinating industry, as you said, It's interesting; it's also tiresome. Like, there's never a finish line, which is, you know, it's – I think we've always said there's a – there's a lot of security jobs, just not a lot of job security. I love that line, because there's always going to be security things we have to go do.

But I think some of the things I think are exciting for me is, I see for the first time an asymmetry where the good – the good people have an advantage over bad people. Some of the things you're talking about, like preparing for post quantum I think is important. Post-quantum crypto will be super important.

But also when I think about how we use things like artificial intelligence and ChatGPT and the stuff we announced earlier today, really give me a leg up because it's really based on an amazing capability and learning model, but also based on broad telemetry.

Telcos have always had amazing network and, you know, telemetry at a – at a network level and at a low level, but when you add network telemetry with device telemetry with access telemetry with system use telemetry, and, you know, large scale cloud system use capabilities, you really can train these models to make, you know, our team super effective.

Imagine having a tier one SOC where all your tier one SOC people do tier two work instead of tier one work, right, which is just, I mean, they love it. So it's a win-win. They love the more

interesting work, and we automate a bunch of the work that we don't really need to do in human capital. I think that's an exciting, exciting thing for us, and in this war for talent, it will really help us. I'm excited about that.

I think this idea in regulation, I'm not sure I'm excited about it, because it's always an interesting conversation, but like we were mentioning, this ability to influence what the regulations become, so that they're practical, and – and purposeful, I think is super important.

And as you mentioned, like I don't need five privacy regulations in the five states of India or globally, whatever the, you know, not picking any particular area, but like, how can we harmonize those, so we can get the most consistency, the most cost-effective model that really, really protects both assistants and the constituents we're trying to serve? And I think there's great opportunity to do that, both with technology, but also with how we work, like, as you said, with many of the regulators around the world. And I think that will really help us in that perspective.

And I think those, to me, are some of the most exciting things we have coming, and I do believe this asymmetry of good people and bad people is happening, which is a turning point. It's a seminal turning point for all of us in the industry. And to be part of it is exciting. And I think it's super, it's a great time to be in the security space, which is like as we try to go get talent and I look at it, the other part for me is it's not about a bunch of tech people, right? Like one of my favorite security people and risk people I have is a PhD in Sociology and helps us with civil unrest and how we do cyber resilience. And I think about all the different roles and the bigger roles for data and this burgeoning set of population that's coming out of schools, and not traditional schools, that are really going to participate in this workforce, I think is an exciting time for us. So those are probably the three big things I'm most excited about in this space.

Emma, thank you so much for joining me today. Really, I always value – I always value the time we get together.

**EMMA SMITH:** My pleasure, Bret. It's been great joining you.

**BRET ARSENAULT:** So I hope you're taking away a better understanding of what CISOs think are top of mind and insights for practitioners in this ever-changing industry. Next you'll be joined by Vasu and Brad on further conversations on the role AI plays in the regulatory environment. I think you'll find it fascinating.

**BRAD SMITH:** We're living in a changed world. Advances in technology are dramatically reshaping how we live, work and learn. And while there is great potential for technology to help address society's biggest issues, the pace of this change is also raising new challenges and amplifying existing inequities in our communities.

Now more than ever, Microsoft recognizes its enormous responsibility and opportunity to ensure that the technology we create benefits everyone on the planet, as well as the planet itself.

Now is the time for urgent action. Those of us that can do more, should do more.

But the challenges we face are complex, and no one company, industry or country can solve them alone. Together, we can reimagine a better future.

**VASU JAKKAL:** The message of reimagining a better future together is such an important one, and especially important in the context of security, because safeguarding our future is very much a team effort. It requires the cooperation of our global community, and a commitment to helping one another advance the mission of cybersecurity.

So to help us, give us a global perspective, I'm thrilled to welcome Microsoft Vice Chair and President, Brad Smith. Welcome, Brad. It's so great to have you here.

**BRAD SMITH:** Great to be here with you. Vasu. Great to be part of this event.

**VASU JAKKAL:** Thank you.

So Brad, one of the unique aspects of your role is that you work with organizations, agencies, governments around the world, across public and private sector. And an important aspect of that is security. What are you hearing from the leaders that you speak with?

**BRAD SMITH:** I think right now, I'm hearing two principal themes. One is people in government really appreciate, I'll say, the diverse and textured nature of the cybersecurity threat landscape. They've got to worry about nation-state malicious attacks. They have to worry about even more so if you're in a government, basically hacks that are all about gathering intelligence, or in some cases using and weaponizing that intelligence. They're very worried about ransomware, not just against governments and schools, but especially critical infrastructure and businesses more broadly.

And I think they're increasingly focused on what we call cyber-influence operations. Sometimes that hack is used to obtain information, and then it's released to try to influence, say, domestic politics in another country. So there's this huge appreciation of how important all of this is to the protection of countries.

The second thing they really focus on is just an extraordinary realization, in my view, that unlike every other traditional national security or defense issue, cybersecurity is a team sport that brings together the public sector and the private sector. It cannot be done by one or the other alone, or even really separated. It requires this intense level of collaboration. And that's where we really seek to play a leading role in the most multifaceted way we can to support that team activity.

**VASU JAKKAL:** I love those points. Brad. It is truly a team sport that it takes in cybersecurity, and I love the cooperation between the public and the private sector, and we've come a long way in that.

And when I look at the threat landscape, and specially ransomware, every single business, actually even the consumers are being challenged with what that means.

**BRAD SMITH:** That's so true.

**VASU JAKKAL:** So if we think about that, and we think about where we are going, what is Microsoft's role in achieving a safer world and a safer internet for all?

**BRAD SMITH:** Well, cybersecurity is one key piece of this. We also focus on privacy. We focus on digital safety, which I think, increasingly, is about the protection of children. And we think about ethical or responsible AI. And so, we bring all of these areas of expertise together. We work to ensure that they all complement and reinforce each other.

I would say there's this common theme around using technology at the core. Of course, that's what we do. We're a technology company. But we look beyond the technology we create to the relationships, to the collaboration, to the public policy, and we ensure that it all fits together to the best of our ability.

**VASU JAKKAL:** I love that we think of privacy and security together, Brad, when we think of trust, and that Microsoft is so anchored in trust. Especially your comment on creating a safer world for our children is so important, resonates deeply with me as a mom.

And I know that AI is going to play a big role in this. We've heard a lot of AI and the role of AI and the future of security. And with that comes a lot of responsibility. So how should we, as an industry and as a company, think of a AI, and how do we ensure that we are developing AI and using AI responsibly?

**BRAD SMITH:** It really is, I think, a critical question that's almost a general public conversation now in 2023, as ChatGPT and generative AI and everything we're doing at Microsoft with AI has sort of burst into the center of public consciousness. And it's just driving innovation across every area of technology.

The good news from my vantage point is that we've been working on this for six years. It's part of our enterprise risk management framework. We really have very similar approaches to cybersecurity, privacy, safety, and AI.

But I will say if there's one thing above all else that we're learning in 2023, it's that you can only learn so much when you have technology in the lab, so to speak. You've got to get it into people's hands.

And when it comes to AI, we release it with guardrails. We release something like Bing, and we'll do this with other products, in a gated way. We won't turn it on for the whole world on the same day. We do it in a methodical way, get more usage, and then we learn and fix things fast.

And to me, the most interesting conversation I find myself having with government officials and the like is on this latter part: How do you release something and really do it in a measured way and fix things fast.

And we've got a lot of discipline. The thing I love about the issues that we encounter is that the way software works, especially in this kind of service, you can often fix things in four or 12 or 24 hours.

But I do think it's just essential that we continue to do this the way we are. The analogy that I have often used, and a lot of times people find analogies easier to think about, is that when Henry Ford released the Model T automobile in 1908, it changed the use of automobiles across the country. Everybody embraced it. But it was only ready in 1908 because he'd released the Model A, his first car, in 1903.

And that car had performed beautifully around a racetrack in Detroit, but as soon as it was released, and people were driving it over every country road in the country, they found that it wasn't up to the task. So he had to take five years to change the materials, to perfect the design.

But it is a great reminder to me that whenever you have a fundamentally new technology that is such a transformative technology, you need to have an approach where you do rely on real feedback from the market and an ability to keep improving. And so, that is actually an indispensable part of what we're doing.

**VASU JAKKAL:** I love that. I love that story. I love the example and that continuous learning. And we're going to need the entire community to participate and to help us make AI better, going back to your team sport.

And that brings me to a topic I know it's close to your heart, and that's talent. And we have such a talent shortage today in cybersecurity. And I know that the AI innovations we do are going to help augment that talent and bring the best of humanity forward. Would love for you to touch on the work that you have been really leading the way on in cybersecurity talent.

**BRAD SMITH:** It is extraordinary because there's a cybersecurity talent shortage on a global basis. And, you know, here in the United States, for every two cybersecurity jobs that are filled, a third one is open. And that's an extraordinary number in and of itself.

Certainly, we have embarked on a global effort. We have a program now running in 28 countries. Our goal is to train 250,000 additional cybersecurity professionals by 2025, and we're progressing well.

In the United States, we're now working with more than 280 community colleges. And in other places, we're partnering with NGOs. You know, in India, I had the chance to visit one of the programs and talk to people last August.

And it's extraordinary because it's the same formula everywhere in the world, I find. It sort of has three elements. First, get digital curriculum out. We're good at that. We're not alone, but we're good at it. And the great thing about digital curriculum is you get global distribution for free immediately, and we've done that.

The second thing that is just a real challenge is you have to train the trainer's. It means training faculty in community colleges. It means training people who are teachers with NGOs.

And then the third thing you need to do is really attract people and give them in some cases financial assistance.

One of the more actually inspiring things for me was in India because I met young women. They had had to move to another town or city in order to participate in this. But it is transformative, not just for addressing cybersecurity, but for their future.

**VASU JAKKAL:** Totally.

**BRAD SMITH:** And so, that to me is a great cause for, I think, maybe everybody who is part of this today, because I think we're all part of a cybersecurity discipline and profession, and we should recognize that as we grow this profession, we're not just strengthening cybersecurity for the world, we are creating opportunity for people around the world.

**VASU JAKKAL:** And we're creating – creating a better world. That is very inspiring.

And I was in Australia two weeks back, and I met a refugee from Syria who was working in a SOC at one of our customers. Isn't that inspiring, using Microsoft products? So, gosh, that makes my heart full.

And talking about hope and inspiration, what are you most inspired by or hopeful for, optimistic about cybersecurity, its future?

**BRAD SMITH:** Well, what I would say is, I feel that the trend of technology development and capability is favoring defensive protection over offensive weaponry. And I think that is good for the protection of the world.

And in particular, I see three trends coming together. One is threat detection. Obviously, everything turns on the ability to detect threats broadly and immediately. And this is where I feel we've so honed our capability at Microsoft, and AI is augmenting that even further.

The second is, frankly, then the architecture of cybersecurity from a technological perspective, and including a lot of endpoint protection. This ability to identify a threat, in effect code an anecdote, a vaccine, whatever one wants to use as the analogy, and dispatch it immediately to every device, that has been a game-changer in defense of protection.

And then the third is looking to the future of AI. AI as a copilot for a cybersecurity professional, AI as a productivity enhancer for a cybersecurity professional, will give you the third great, I think, contributor of AI.

What I see every day is there's a communications gap between people who are deep in cybersecurity, like any discipline, and people who are CEOs or government officials or boards of directors. And I just think there is a use of AI in the future for cybersecurity professionals. It's

called write a report and then ask, translate this into the kinds of vocabulary that my CEO uses at the office and do that instantly. It just underscores, I think, how the technology itself really will augment the human ability of the great professionals that make up the cybersecurity profession.

**VASU JAKKAL:** I love that, and I love all examples, and I can relate to the last one.

**BRAD SMITH:** You and I have done it together with the Microsoft board of directors.

**VASU JAKKAL:** We're smiling. That is amazing.

Brad, thank you so much for being here and really leading the way for us. I am so grateful that I get to work with you every single day, and I look forward to building a safer world.

**BRAD SMITH:** Well, same to you Vasu. And there's a lot of work ahead of us. It's really exciting for us to have the opportunity, all of us at Microsoft, really in partnership with everybody who's watching this today, to look at what we can do for the future.

**VASU JAKKAL:** Thank you Brad.