Microsoft Ignite 2021
Vasu Jakkal Keynote Transcript

VASU JAKKAL: We're getting closer. In many parts of the world, workplaces are reopening. And while some couldn't work from home, millions discovered they could do their jobs remotely with Microsoft technology.

Hybrid work is here to stay. Ensuring we can do it safely and securely is a challenge we will overcome together.

Hi, everyone. I'm so glad you've joined us for Microsoft Ignite. I'm coming to you from the brand new Microsoft Silicon Valley campus in Mountain View, California. We aren't fully back in the office yet. Like everyone else, we are embracing hybrid work, which brings new experiences, new opportunities and new security challenges.

Securing an organization has never been simple, but with hybrid work and the increased surface area for digital attacks, it's so much harder now for organizations in every sector and of every size.

The frequency and sophistication of cyber events has increased dramatically. We see headlines every day now of phishing schemes, of ransomware, and nation-state attacks. And as personal devices become an essential part of the corporate network, a powerful identity solution is critical.

Now, the wonderful thing is that we can leverage the Microsoft Cloud, the most comprehensive and trusted cloud, to build end-to-end, best-in-breed security solutions that are ubiquitous and composable, security for everyone and everything, protection across clouds and platforms and devices, so customers can stay in the flow.

The Microsoft security team builds solutions from the endpoint to the cloud across security, compliance, identity device management and privacy management. They work together and simplify the complex. And when you add industry-leading AI, automation and expertise, you can catch threats others miss from outside or inside your organization. And with the peace of mind that comes with that kind of comprehensive security, you are free to grow, to create and to innovate.

Daily, I hear examples of organizations across all industries using Microsoft solutions to be fearless in the face of growing threats. A perfect example is HCA Healthcare, one of the largest hospital and healthcare facility organizations in the United States.

Now what stands out to me about HCA is how the organization's commitment to patient care extends beyond the hospital room all the way to their cyber defense center. Take a look.

(Begin video segment.)

RIKI ANGELOV: I love my job. Ever since day one, I've had a huge passion for cybersecurity and protecting people. That's what it comes down to.

HCA Healthcare is a healthcare company that is committed to the improvement and care of human life.

When I walked in that morning, there was a little bit more chatter in the room, so I knew it was probably not going to be your business as usual morning. I learned that someone clicked on a link they probably shouldn't have clicked on.

As with any security event, first we want to find the root cause. Then we want to find the impact and isolate the device in order to make sure that whatever is on that machine is stopped and it cannot spread.

First thing that goes through our mind is the ability to take care of our employees and our patients. Whenever we have a patient out in our facility, the last thing that I want them to worry about is their information safety.

I was called on to lead the response team. Fortunately, we have a robust toolset and Microsoft Defender is one of them.

Defender was a great tool to use because it gave us immediate visibility into the endpoint and its timeline, which helped in the investigation process. It also allowed us to take action against the endpoint and then also isolated if we needed to. And all of that with great speed. Defender actually elevated our capabilities to investigate this machine.

Just like any other industry, the reality is we all have to deal with cybersecurity and we have to be prepared for it. By working together with Microsoft, we're able to acquire and share information between both parties that helps us deal with these events. Those relationships and collaborations make all the difference.

(End video segment.)

VASU JAKKAL: I love how our partnership is helping HCA live its mission.

In just a little bit, Microsoft's Chief Commercial Officer Judson Althoff will sit down with HCA's Chief Security Officer to talk more about how they rely on Microsoft Security Solutions.

Their proactive approach to security underscores the reality that cybersecurity is a risk for everyone, not just for large enterprise and government organizations. In fact, security remains

one of the top concerns and the most challenging responsibilities facing small and medium sized businesses today. According to recent reports, one-third of all cyberattacks targeted small businesses. And after being attacked, 61% of small organizations are left unable to operate.

The simple truth is, small and medium business customers have resource and budget constraints and often don't have the specialists to help them deal with attacks. Yet they need to be able to fortify their security just as much as large organizations like HCA.

That's why today I'm so pleased to announce Microsoft Defender for Business, an endpoint security solution that helps protect small and medium sized businesses with up to 300 employees against cybersecurity threats. That includes malware and ransomware across Windows, Mac OS, iOS and Android devices.

Now what Microsoft Defender for Business does is bring together preventive protection, post-breach detection, and automated investigation and response. How cool is that? Combine that with tools that help you manage software vulnerabilities and misconfigs, and you have a powerhouse protection solution at a cost effective price.

Microsoft Defender for Business is easy to deploy and manage, all while providing maximum security value. It delivers an integrated experience with existing Microsoft cloud solutions for productivity and security and helps small and medium sized businesses reduce cost and complexity.

It will be available to customers as a standalone solution and will also be included in Microsoft 365 Business Premium. Preview is coming soon, and this is going to be a real game-changer for so many small and mid-size organizations.

Now, of course, Microsoft Defender for Business is big news, but it's not the only security headline at Ignite today. We have some other really exciting developments with Microsoft's threat protection solutions. So let's head to the Microsoft Ignite Studios in Redmond where Jeff DuBois is standing by with more of these headlines. Jeff, take it away.

JEFF DUBOIS: Thanks, Vasu. So cool to hear about Defender for Business, and not just for smaller organizations, but for Microsoft partners too, because they'll be deploying the solution for many customers.

And as I understand it, Defender for Business also works with Microsoft 365 Lighthouse, so you'll be able to view security events across your customers from the Lighthouse portal.

OK, in other threat protection news you may remember last spring at Ignite, we shared how we were unifying two key components of Microsoft's threat protection solutions – our cloud-native Security Information and Event Management solution, or SIEM, Microsoft Sentinel, and Microsoft Defender, our extended detection and response tool.

This is really about bringing two incredible tools together to help customers fortify their defense against the growing attack surface. The integration gives organizations a bird's eye view of an incident with Sentinel's AI and automation capabilities, and then allows you to investigate and resolve incidents through Defender. And there's no other security vendor that can bring you better visibility and faster response times with SIEM and XDR integration like this. No one.

Today we're announcing the next step in that integration, bidirectional incident detection and response between Sentinel and Defender. It will now be easier for users to get the full context around an incident and even close that incident from either tool.

And on top of that, in Sentinel, there are a bunch of new updates to help security operations teams be more efficient, more effective across the full lifecycle of an incident.

Now I want to share a couple of the big updates with you. First, we've developed a new content hub with more than a hundred solutions that help organizations collect data from any source, like data connectors and workbooks, that help uncover security weaknesses or gaps.

And we've added new integration into Sentinel with Azure Synapse, so you can tap into the power of big data analytics and machine learning models for deeper insight into threats and attacks. Really exciting news across the board, unleashing the power of both there.

Now there are a couple other big headlines we'll cover in more detail coming up about Microsoft Defender for Cloud and Defender for IoT. Those two solutions really speak to how Microsoft Security is building protection across the clouds and edge. We're talking Microsoft security integration with AWS workloads and protection for enterprise IoT devices. All of those details in just a little bit. Vasu?

VASU JAKKAL: Thanks so much, Jeff. It's really exciting stuff.

Now I want to shift gears a little and follow up on something Satya shared earlier today about boundaryless collaboration and the security layer that is changing the way we work together.

With hybrid work, we need to always be thinking about ways to bring teams closer together with the people they work with inside and outside the organization. And to do that safely, we need to re-envision our identity and security solutions so they establish the right level of trust. This is critical work.

And to talk more about how we're thinking about identity solutions for today and tomorrow, I am thrilled to bring in Joy Chick, Corporate Vice President of Identity and Network Access.

Joy, thank you so much for being here today.

JOY CHICK: It is great to be here, Vasu.

VASU JAKKAL: So Joy, securing hybrid work is really challenging a familiar security paradigm, protecting the boundary between your organization and the outside world. That approach just doesn't work anymore, does it?

JOY CHICK: No, it doesn't, and hybrid work is making that really clear. Customers know the way we collaborate has changed. For example, the data has shown us 86% of business leaders collaborate externally, and 35% of them use at least one personal application. That is very scary, right? And many customers think to collaborate externally, I will just expand my security perimeter. But with so many partners, alliances and mergers, things get complicated really fast.

So we need to shift this mindset. It is not about perimeters. Instead, you have to start with Zero Trust principles and answer three questions about your users: Who are you, what do you need to do and how much do I trust you right now?

And this is where identity comes into play. It is becoming your organization's trust fabric for all relationships, employees, partners, customers, or even workloads and the services.

VASU JAKKAL: I so love that, Joy. And I know that your team has been working side by side with Microsoft Teams engineering. Identity plays a really key role with Teams Connect, doesn't it?

JOY CHICK: Yes, identity is so central to Microsoft Teams Connect experience. Azure AD underpins shared channels in Teams. You can collaborate using your work identity from any organization, or admins can establish a trust relationship between two companies, so that all employees on both sides can collaborate seamlessly.

Just imagine, IT never has to create another account for an external partner. And partners can use their own identities so that they can stay in their workflow without having to switch between accounts.

Security leaders also get a peace of mind. Azure AD has the granular access controls that can apply the right security policies in real time for anyone, both internally and externally.

VASU JAKKAL: And that level of collaboration is available with Teams Connect today, correct?

JOY CHICK: Yes, it is. Very exciting for us.

VASU JAKKAL: Gosh, it's so exciting to push the boundaries of collaboration outside of an organization's perimeter.

So, Joy, what's the next big thing for identity?

JOY CHICK: We are building identity to be the trust fabric, not only for organizations, but also for the entire digital ecosystem.

First, we are making big investments in platform resilience and security. I have lots of news to share on that front in my session later today.

Next, as you know, one of the things that people trust least is their password. In September, we announced that Microsoft account users can now delete their passwords altogether, and we're helping commercial customers go password-less as well.

Plus we're going big on multi-cloud. Of course, Azure AD today already connects all apps, supports multi-platforms and devices, but we're going even further. For example, in my session, we will show how CloudKnox, our recent acquisition, can manage permissions for human and non-human identities across all clouds, including AWS, GCP and VMware.

And finally, we have groundbreaking solutions like verifiable credentials. It provides a new and a verified form of identity for digital transactions. You can already try this today, actually. And there is just so much more coming soon.

VASU JAKKAL: Simply wow. Amazing. Exciting. What a time for identity. I know that you and your amazing team will keep pushing that envelope and bring incredible ideas to life. Joy, thank you so much for being here, for being my partner in crime, for sharing your perspectives. It's truly such an honor. Thank you.

JOY CHICK: Likewise. Thank you so much, Vasu, for having me today. It's great to be here.

VASU JAKKAL: Now, it's exciting to imagine a world where boundaryless collaboration is the standard, where data, information flow freely, but securely, and with privacy prioritized.

So let's talk about privacy. Privacy is critical. Safeguarding sensitive personal data builds trust with customers and with employees. Plus, it helps organizations be confidentially compliant with regulations, laws and their own policies.

That's why we recently announced Privacy Management for Microsoft 365, which will help organizations build a privacy resilient workplace. Now, not only does the solution build trust, it helps you identify critical privacy risks, automate privacy operations and empower employees to be smart when they're handling sensitive data.

Data protection, privacy, trust, they're all interconnected, and they lead to stronger collaboration and productivity. I'm so incredibly proud to say, the Microsoft security team is

continuously innovating to enable industry-leading protection from the inside out, for example, new enhancements within Microsoft Information Protection that bring more security to your Microsoft 365 data, so you can share, coauthor and edit encrypted files without worrying about unintentionally exposing information.

You can also support a positive work culture in Microsoft Teams with new communication compliance features that detect sensitive or offensive content being shared from inside or outside your organization.

And they can help you reach the highest level of privacy for your most sensitive workloads by encrypting data in use with Azure Confidential Computing. In partnership with Intel and AMD, you can now move existing workloads to Azure and make them confidential.

So these are all examples of how we've integrated data security across the entire Microsoft Cloud, where you can set a sensitivity label once and have it remain with the data, whether it's shared in emails, stored in a database or used by an app you built with the Power Platform.

Now, of course, we believe modern security should be cloud-native and AI-based, so it works for you everywhere at scale. And it should be extensible to a broad ecosystem of clouds and platforms and devices because customers want and need to have choice.

That's why they're so excited to share today enhanced security capabilities for multi-cloud environments. Microsoft Defender for Cloud now supports AWS environments with the same native experience for cloud security management and workload protection they get with Azure.

Connecting AWS is now seamless, so security teams can make sure their configuration follows industry best practices and regulatory standards. And we're also extending our protection capabilities to Amazon's Kubernetes service for improved workload coverage.

So with these new enhancements, you now have a holistic view of your security state across clouds. That is true multicloud security.

Certainly big news there, but there are so many other ways we are bringing security solutions to life across clouds and platforms. So for more announcements, I want to toss it back over to Jeff DuBois in the Microsoft Ignite Studio in Redmond. Jeff?

JEFF DUBOIS: Thanks, Vasu. Really cool news there about Defender for Cloud. And let's not forget about securing our SaaS apps across different clouds and platforms. Microsoft Defender for Cloud Apps now has a new application governance capability that helps you identify, alert and protect against risky behavior across data users and applications. Plus, Defender for Cloud Apps helps you secure more than 26,000 cloud applications, covering all major cloud app use cases.

OK, as you know, recent ransomware attacks like the ones this year that shut down production for the Colonial Pipeline operator and a global food processor highlight the challenge of securing IoT devices and operational technology, or OT, devices.

Defender for IoT already protects OT devices in critical industries like manufacturing, energy and water utilities, and oil and gas. But today, we're extending that solution to monitor enterprise IoT devices like VoIP phones, conferencing systems and building automation. And this is a big deal because those channels can often be attractive access points for bad actors. They are often unpatched, misconfigured and unmonitored.

And here's another critical piece of integration that we've been working on. To bring IoT protection into the same workflow as the rest of your extended detection and response, we're making every Defender for Endpoint instance a sensor for discovering IoT devices, alerting on IoT security events, and bringing those events into the Microsoft 365 Defender console. This is all about strengthening your ability to manage the attack surface area across every device. Deep integration there.

Now switching over to some multi-platform news around our Unified Data Loss Prevention offering, up until now, Microsoft Endpoint Data Loss Prevention was only available for Windows endpoints. But we're now extending the solution to millions of additional users by adding support for Mac OS.

In other words, customers on multiple platforms can now identify and protect sensitive content like credit cards, medical documents, IP, virtually anything they categorize as sensitive. They can set the policy one time in the compliance center and know that the content can't be copied, printed, shared or saved, without defined permissions.

And thinking more broadly about managing endpoints, we're expanding the breadth of Microsoft Endpoint Manager. Users will now be able to manage Linux desktops. And with that expansion, organizations can now apply and manage security policies and configure conditional access from Azure Active Directory across devices on any platform – Windows, iOS, Mac OS and now Linux. A lot of great new enhancements and capabilities there.

And for more details on these new features and many more, be sure to check out the security breakout sessions today and on-demand, even after Microsoft Ignite.

Vasu, back to you.

VASU JAKKAL: Thank you so much, Jeff. It's great to hear all the updates and new capabilities that bring tighter security across clouds and platforms and devices. I so love all our expansions from the Edge, OT, IoT, to the cloud, end-to-end.

Now, you've heard a lot today about Microsoft's comprehensive approach to security, but I thought I'd bring this back to some fundamentals.

Everything we've just shared is based on a Zero Trust philosophy, a proactive mindset that assumes all activity, even by known users, could be an attempt to breach systems. Given the multitude of business risk today, inside and out, Zero Trust is no longer an option, it's a business imperative.

The principles of Zero Trust – verify explicitly, provide least privileged access and always assume breach – are the cornerstone of effective protection and the foundation for comprehensive security. They help organizations develop a critical component of success today, resilience.

Organizations must be resilient to thrive in today's complex and competitive world, and security is key to your resilience. It's not just about protecting yourself from outside security breaches. We're reminded every day that business risk comes in many forms, and at the end of the day, protecting yourself from one, while leaving yourself vulnerable to another, is not really effective security.

That's why Microsoft is helping organizations take a comprehensive approach – security, compliance, identity management and privacy, all part of an interconnected whole, working together beautifully, extending protection to all data and all devices, all identities, all platforms and clouds.

This comprehensive end-to-end approach and the work of the defenders at Microsoft, and within your own organization, empower people and organizations to do more, to be safe and to be fearless.

END