Connection
we solve IT

LinkedIn Live: Ask the Experts

WINDOWS 11 PRO DEVICES AND ZERO-TRUST SECURITY WITH ROB MCGILVREY

TRANSCRIPT

Watch the full session recording:

Watch Now

My name is Rob McGilvrey. I'm the Americas Specialist with Microsoft, covering everything Windows Pro and modern endpoints. And so just looking forward to this discussion today around Windows 11 and the innovation that we're bringing into the platform around security. We'll touch a little bit on AI, because we do know that is always top of mind. And we had some great announcements last week around what we're bringing to Windows 11 around AI.

So, it is becoming more sophisticated, and it is becoming more costly. So how can Windows 11 truly help with that is what we really want to focus on today. I just kind of want to level set around zero trust. We talk a lot about zero trust, but we really just kind of want to level set here because zero trust is at the foundation of everything we're doing.

We want to bring technologies into the operating system, and we'll talk a little bit about some of those new enhancements we're making around verifying explicitly. We want to make sure that the person who's logging in is who they say that they are. We also want to know that the devices are in the right state to gain access to information within our organization.

You want to use least-permanent access. The better terminology I like here is the right amount of access, right? We don't want to give too much. We don't want to give too little so we can make sure that our end users are productive. And then if a security breach does happen, how can we maintain that blast radius? Do we have the right tools and solutions in place to contain that blast radius? And always operate in that manner of assuming breach. When we think about Windows 11 and what it can do for your business, we're going to focus in really heavily here on security. We will spend a little bit on AI because we made some fun, exciting announcements around AI last week.

But when we think about security, we are tracking a 58% reduction in security instances on Windows 11 devices versus Windows 10. And a lot of this was accomplished by raising that base hardware threshold and turning on certain features by default. We'll talk a little bit more about that here in a second. We also know that AI user experiences are on the rise and the importance of that is on the rise. So how are we continuing to innovate? And how are we going to leverage AI to really help improve security at the operating system as well.

We did a study with Forrester back in December of 2022. We're not going to look at that study today, but we do have a link here in the presentation. And we encourage customers to go visit this calculator where you can go in and input your own information and get a customized output of what it would be if you did migrate your environment to Windows 11 and leverage a lot of these features that we'll mention here today.

I really did just want to again focus in on that Windows 11 is the most secure version of Windows ever. As I mentioned, we are seeing a reduction in security instances between Windows 10 and 11 devices. A lot of this has to do with us raising that base hardware threshold and requiring TPM 2. 0 and newer silicon. We are able to turn on things like virtual base security and HVCI by default in Windows 11.

Full transparency. Those features were available in Windows 10. Okay, they weren't on by default. You could have enabled them, and you may have enabled them in your environment. And if you've done so, that's awesome. But they do require certain hardware components to be able to leverage those features. By raising that base hardware requirement and turning those features on by default, we are seeing an overall improvement of security instances on Windows 11 devices. We also want to stay ahead of these evolving threats, right? We know that threats are on the rise. We know that bad actors are becoming more creative.

So how can we take all the telemetry and all the signals that we're gaining? At Microsoft, we get signals from 1. 4 billion endpoints around the world. So how can we take all this information and bring it into the operating system to help our end users be more secure? As we know, end users are the number one vulnerability here and certain behaviors—and not being aware of what's going on around them—could potentially lead to a security breach within your organization.

So, we have a new feature within Windows 11 called Enhanced Phishing Protection with Microsoft Defender SmartScreen, where if a site or an application has been flagged with Microsoft as being malicious and harvesting credentials, and one of your end users goes and visits that site... Now this works across any browser application on the device because this is happening at the OS level, and we know that credentials were entered, and that site has been flagged with Microsoft... We will proactively generate a pop up for the end user that says, "Hey, we think something malicious may have happened, and we would encourage you to go through a process of notifying security and potentially resetting your username and password because it was potentially spooled."

We're trying to bring in that creativity and that AI into the operating system to really help improve end-user security, especially around credentials. We're also making a lot of investments with Windows Hello for Business. And we'll talk a little bit more about that here in a second. Also, your apps, right? Mission critical apps? Win32 apps run in isolation. So, if something happens to one of those apps, it's not going to affect the entire operating system. And then really that end-to-end production. You know, as we think about chip-to-cloud security, how are we going to continue to improve our chip-to-cloud security story with some new features? And we'll talk about one of those new features that we launched last week as well.

When we think about security, I would encourage you—if you're sitting on your device right now, which hopefully you're sitting on your Windows device—if you go down to Windows security, you just do your search bar. If you're in Windows 11, you can search it if you're on the latest version. If you go Windows 10, you can just open up your start menu and search Windows security. And within that menu, you're going to see a section called device security. If you click it on there. Click on device security. You're going to see somewhere on that page, depending on what version of Windows you're in—maybe at the top, maybe in the middle, maybe at the bottom—but you're going to see a statement.

That statement is going to tell you what level of security your device needs from this perspective. It could say that your device does not even meet standard security. It could say your device meets all standard security settings, pan security settings, or potentially even secure core settings. I'd encourage you to do that on your device. There's a ton of links in

there that explains all these different features that are available from a Windows device security perspective. But really what we're doing is trying to build on the foundation to give you the most secure device—all the way down to the core—as possible.

As we mentioned, 83% of those organizations that we surveyed experienced some type of firmware level attack. So, are we making sure that we're buying the right devices with the right technology at the chip level? Intel vPro and AMD Pro enables a lot of these features. We can reach that secure core PC. Which is the highest level of security from a Windows device perspective. It builds on that. Things like modern device servicing, secure boot enabled. It has a TPM, and we've turned on that virtualization support. When you get into enhanced, we have memory integrity enabled. Are we using enhanced sign-in capabilities?

And then when we get into that secure core PC function, dynamic root of trust and system management mode protection really isolates the core of that device to make sure that nothing bad and malicious has happened to the firmware or the memory of the device before that device boots. Again, I encourage you to go visit this and really kind of understand where you're at in your current Windows security. And go learn more about these different levels of security within the Windows OS.

The other feature I really just kind of want to spend a few minutes on is around Windows Hello for Business. This is not a new feature and when we think about security, we know that bad actors for a long time have been going after a username and password. If a bad actor gets a username and password in their hands, that's what they need to potentially gain access into your organization. You're leveraging different MFA programs out there. That's great. You know, those MFA programs—like the Microsoft Authenticator app—can really help alleviate behavior that's maybe outside the norm with a username and password. And you could have rules and policies in place about when that multi-factor authentication needs to happen.

But when we think about logging in, biometrics is more secure than a username and password. Can biometrics stop every single identity theft within your organization? No, but we do know that it is a more resilient way to log into your device and potentially into third-party sites as well. So, when we think about biometrics with Windows Hello for Business, the biometrics—your face, a fingerprint reader, and PIN—are all stored locally onto the device. It's important to understand if you have devices that are capable of this feature. If your device has an IR camera, we've also now launched an external camera support for Windows Hello for Business. Also, if an external camera has IR, we are supporting that in the Windows Hello for Business platform as well.

Do you have devices the potentially have fingerprint readers? When you think of a bad actor needing to gain access with Windows Hello for Business, they're going to need your biometrics—which are stored or pinned locally on the device—to gain access to your device and gain information from the system. Windows Hello for Business can be used as a single sign on across all applications. It also can be deployed cloud only, hybrid, or even on prem.

We do know that MFA is a key pillar in helping protect security within an organization. With Windows 11, we're starting to build on Windows Hello for Business. We announced presence sensing when we launched Windows Hello. And now we've also launched adaptive dimming to save energy and refocus attention and dim screens in the right way. If you're no longer paying attention, that helps if somebody else is trying to look at your screen—and they can't see it. But I'm going to give a prime example of this when we think about presence sensing.

So, during COVID—prior to COVID—I was very...I was always Windows out. Anytime I walked away from my PC, I'd press the Windows button. And I'd press the L. And I'd lock my device and walk away. Over the past few years, working from home, I get up from my device and walk away—and I don't lock my PC. Yeah, that may not be a serious security risk inside my own house. But I found as I started getting back out there, and I've developed this bad behavior, and getting back out visiting customers and traveling a little bit more, then I took that bad behavior with me. I've been at coffee shops, and I've stood up and I've been like, "Oh, I forgot to lock my PC." Or I've been on a plane and get up to go to the bathroom and I forget to lock my PC.

With presence sensing, what that's going to enable is that if it doesn't sense your presence and you get up from your device, it's going to automatically lock it for you. It's also going to wake it back up when it senses presence. And then, if you're using Windows Hello for Business, you can log directly in with your face. And it just really improves that end-user experience, but also improves the security posture of the device—potentially protecting organizations against some of that end-user bad behavior that might be out there from when you get up and walk away and forget to lock your PC. We also are taking this a little bit a step further here with Windows 11.

So, we now have passkeys with Windows 11. The best way to really explain passkeys, if you don't know what they are, just think about your mobile phone. And you know, you can set up within an app to log into that phone, leveraging your biometrics that are stored locally on that device. We'll bring that feature into the Windows platform, Windows 11, as well.

This is a Windows 11 only feature as well where you can go in and you can download those passkeys from those sites and those third-party applications. And then you can log into those sites moving forward with the biometrics that are stored locally on the device. So, the focus here is just how can we continue to innovate around identity and bring in features that can really just continue to help organizations move away from passwords. Because we do know that is a step in the right direction from a security perspective. Again, it's not going to stop all security instances, but we do know that does help improve that overall security posture within an organization.

If you're leveraging Intune to manage, you have Intune managed devices and you have Windows 11 Enterprise. We have a new feature that just launched last week as well called Config Refresh. What this does is that this goes back, and it can revert all your security settings to IT's preferred state every 90 minutes, automatically refreshing them and reverting any changes that potentially have been made. So, you think about... this helps prevent against settings drift, or potential registry edits that may have happened, or malicious software that's trying to go in and change things on the system. This will come and revert those settings back to its IT preferred state, just making sure that device stays as secure as possible and is protecting against some of these evolving threats that we do see out there in the market today.

We talk a lot about security. We talk a lot about features. And we're going to talk a little bit about AI here in a minute as well. But when we think about the priorities of selecting a PC here in 2023, I think it's important to just truly understand and have some things to consider. It's no longer necessarily about i5 16256. It's more about outside of the design features and the form factor. Am I looking at what a secure core PC needs? Potentially, devices with Pluton security processors are becoming more popular. Also, Windows Hello: am I making sure that when I purchase a device I have those capabilities—from a fingerprint reader or a camera with IR—so I can enable those enhanced signing capabilities at the device level.

I looking at the latest silicon out there—Intel vPro, Ryzen Pro, Qualcomm? You know, get better all-day battery life. And in those platforms, we talked about secure core PC. Some of those features that I mentioned are tied to some of these different platforms—like vPro. And so, am I understanding what my options are when I look at the core security of a device? And then productivity features. I was at an event the other day with Intel, and they mentioned, "Hey, we did a survey and 80% of those surveyed said they would like a touchscreen on their laptop." And you think about bandwidth. Wi-Fi 6E is supported on Windows 11 where Wi-Fi 6E is not supported on Windows 10.

And we do know that there's a continuous innovation too as well coming with Wi-Fi signals. And as that innovation evolves, we'll continue adapting Windows 11 there as well. And so, this is just a good little kind of selection criteria and just things to consider as you look at purchasing new hardware that can really help your organization be more secure and set you up for a lot of these great new features that we're bringing into the Windows 11 ecosystem.

And so, to close this section out, just briefly want to talk about Copilot and then we'll turn it over to some Q& A here. But last week, if you saw our launch event, we did officially launch Microsoft Copilot. We did also announce that Microsoft 365 Copilot. Good luck trying to keep all of our Copilots straight. I think I have trouble with that as well, but that Microsoft 360 Copilot will be generally available November 1, 2023. But when we think about Copilot, it is your everyday AI companion. And what we are really excited about on the Windows side is bringing that Copilot UX into the operating system.

So, we announced last week Copilot in Windows started rolling out this week if you're on Windows 11 22H2. I have it on my device, and I used it over the weekend. I'll kind of share an example of that here in a minute. But again, we're very excited about your AI assistant at work and bringing in Copilot into the UX of Windows 11.

And just to be clear, Copilot in Windows is only available on the Windows 11 platform. I used this this weekend, and I had a customer meeting earlier this week and there was a slide and a feature that I really wanted to talk about, and I didn't have a slide that was ready. So, I went into one of our sites and highlighted some text and it showed up in the Copilot agent and said, "Hey, do you want to send your selection to Copilot?" I said yes, and I asked it to summarize it and it created a summary. Now, was I able to copy and paste that summary over into my PowerPoint presentation word for word? No, but you know, I did have to do a few edits. But I will say that it probably accelerated that task by about 50%.

And so very exciting about what AI comes into the platform and how we're continuing to innovate around AI. Another really cool feature from an AI perspective that we've launched is AI recommendations within File Explorer. So, I had a meeting Monday this week and when I went to go open my File Explorer, it offered up some files for that upcoming meeting that said, "Hey, these files might be relevant for your upcoming meeting." And one of the two files it offered up was something I was opening File Explorer to look for. So, you think about just how that, again, can just help improve that end-user experience across the platform as well.

And so, I just briefly want to say this—and we'll keep moving because I know we got some Q&A here and I want to leave time for that. But Copilot Windows is free. So, there's no cost associated with Copilot Windows. It's available on Windows Home. It's available on Windows Pro. And it comes enabled with Bing Chat. If you do have a Microsoft license that comes with Bing Chat Enterprise and you turn that on, then Bing Chat Enterprise is enabled within the Copilot agent. So that's Microsoft 365, Business Standard or higher. If you don't have one of those subscriptions, Bing Chat Enterprise is available a la carte for end-user SKU—as long as you have Azure Active Directory as well. But just wanted to say I am very excited that this feature coming into Windows is a free feature.

I'm very excited about Copilot and what it can help us do across the entire Windows platform. So, to close this out, and then we'll open up Q& A—and I know we got some questions that have come in here... But just really want to stress the importance of understanding where you're at in your Windows 10 journey as well.

We know that there are tons and millions of devices out there running Windows 10 today that are on the non-supported version of Windows 10. When we think about security, this is a very high risk for your organization. Editions that go end-of-support no longer receive security updates. And if you contact Microsoft, we're going to tell you that you need to update to the latest version of an operating system that's supported. We also know that the second most popular version of Windows 10 in use today is Windows 10 21H2, which goes end-of-support in June of next year. And so, it's really important to understand what impact the lifecycle moment on Windows 10 has on your organization.

We know that some people just think, "Oh, I'm on Windows 10. I'm good until October 14, 2025." But that may not be the case. So, we encourage you to make sure that you're going back, you're checking which version is your standard in your organization, and then looking how you can strategically start to migrate and move those eligible pieces of hardware up to Windows 11. So, you set yourself on the best trajectory to take advantage of a lot of this investment that we're bringing into the Windows 11 platform.

Q&A SESSION

Question 1

Crystal: What recommendations do you have for Windows Hello settings in an enterprise environment?

Answer

I think the biggest thing to understand is if your hardware is capable of supporting Windows Hello. You want to make sure that you're enabling the best end-user experience there. I've talked with customers who say, "Yeah, we've got Windows Hello on the roadmap, but we realize that we've been buying devices for years. And we weren't paying attention to the camera components or fingerprint readers being available on those devices."

Yes, with Windows Hello for Business, can you turn on convenience pin? You can. So, you can leverage that feature. But if we really want to maximize the end-user experience and security, leveraging the biometrics of face and finger really are important. So, my first recommendation is just understand what capabilities your current devices have—and (as you look at purchasing future devices, and it's something you want to leverage in your organization that you're paying attention to) those additional features and those hardware components that are required to light up those features in your environment.

Question 2

Michelle: What role does the CPU and its capabilities factor into the zero trust model? Intel versus AMD, for example.

Answer

This one's great. So, this goes back to secure core PC. I will say we probably don't do a great job at Microsoft explaining what a secure core PC is. A lot of those technologies—like Dynamic Root Trust and System Management Mode—are part of those silicon platforms. And so, we encourage you again, as I mentioned, to go to your current Windows device, type in Windows security, click in device security, and look at those categories. And then click on some of those links to understand what those features are and understand how moving potentially into a vPro platform can help you enable some of those additional features that can really help harden up the core of a device and make sure you're comfortable with what level of security you want in your organization from a hardware perspective.

I definitely encourage everyone on here to check. Sometimes in webinars, we ask people to go check it out and drop their screenshot in if they're comfortable. But we do encourage you to check out what level of security your device is from a Windows perspective.

Question 3

Kyle: Will my existing non-Microsoft security products work with Windows 11?

Answer

So, this is a great question. I think this leads into our commitment on Windows 11 and app compatibility. Currently we have a 99.7% app compatibility rate between Windows 10 and 11. Windows 11 is a feature-update-in-place-upgrade to an eligible piece. If you want to get really technical, and you want to start looking at the OS version, I mean, the Windows 11 OS version still starts with 10. Windows 11 is built on the foundation of Windows 10. And so that's how we're able to have such a high app compatibility rate. But I'm not going to leave that there. What I'm also going to say is... Hey, look, you've got solutions in play today in your organization. You're leveraging these solutions on Windows 10 devices. We guarantee that if you're using something on a Windows 10 device today, it will work on Windows 11.

If it doesn't, we have what's called our Microsoft App Assure Program. It's available free of charge for organizations—one employee and more—where we will get our engineers involved to help remediate why that application that you're using today in your environment that's running on Windows 10 won't run on Windows 11.

Also, potentially, if you have a third-party provider who hasn't publicly stated that they will support their applications on Windows 11, please let us know because that App Assure Team wants to talk with that provider to understand why they're hesitant—and what roadblocks they're facing—so we can work with them to make sure that they're comfortable and can publicly state and support their applications (that are running on 10 today) on Windows 11.

Question 4

Jay: Is there anything in the new Copilot that's contributing to more security? Still waiting for it to be rolled out to me.

Answer

Make sure you check—if I remember correctly—I believe with the 22H2 rollout, it's off by default with that cumulative update. So, you definitely want to check to make sure that's being turned on. You know, I think the biggest thing on security with Copilot is Bing Chat Enterprise.

We do know that there's organizations out there that are telling employees, "Hey, don't use these chats that use these large language models out on the Web because you could be potentially putting company sensitive data into these chats that don't have those commercial protection policies in place."

So, on Copilot, the biggest thing around security is really you want to enable Bing Chat Enterprise with that information, so you get those commercial protections that are rolled into our overall responsible AI policies here at Microsoft. And if you need to have deeper conversations around that, around Bing Chat Enterprise, we have resources that are able to help with that as well.

My instance of Copilot, when I pull it up, it says Bing Chat Enterprise at the top and that my information is protected by our commercial policies—which means that no one at Microsoft can see your data you put in Bing Chat Enterprise. Your data is your data. It's not used to train any of the language models.

And so, we have put those commercial privacy data things in place. That's probably the biggest element with Copilot in Windows today, which is around Bing Chat Enterprise versus Bing Chat—which is the basic enabled feature within Copilot.

Question 5

Antenive: What advantages does Windows 11 have when it comes to zero trust spearhead or switchover versus staying on Windows 10 for a bit longer with end of support?

Answer

I think we talked a little bit about that. You know we have publicly stated that Windows 10 22H2 is the last version of Windows 10. We will not be bringing any new features into the Windows 10 platform. So, things we talked about around the enhancements of Windows Hello for Business with presence sensing passkeys. You know, things we mentioned about enhanced phishing protection with Microsoft Defender SmartScreen. Those are Windows 11-only features.

And so, we're going to continue to bring in new security features, and we're going to continue to innovate in the Windows 11 operating system over the next few years, helping it to become more secure. So, I think that's the question you have to ask is...one, you first need to make sure you're on a supported version of Windows 10 and know that "Hey, if I stay on Windows 10, I'm not going to get any new features. The only thing I'm going to get is security updates between now and end of support. And so, if I want to start leveraging these new features and leverage those in my environment to help it be

end of support. And so, if I want to start leveraging these new features and leverage those in my environment to help it be more secure, then Windows 11 is the platform for that."

And we're going to continue to innovate. We've made a commitment around continuous innovation in the Windows 11 platform, and we've also made a commitment around controls for that continuous innovation as well. So, like for instance, on Copilot, there's controls around Copilot so you can turn that feature off at the IT level. And so, we are continuing to make investments both from security and AI, and how we can leverage all the telemetry that we're tracking on a daily basis—I think it's 65 trillion signals on a daily basis that we're tracking—and how can we bring that into the operating system in Windows 11 to help it be more secure.

CLOSING REMARKS

And so, we're right at time here. Again, I just kind of want to say thank you to everyone. If we didn't get to your questions in the chat, I'll log in later this evening to grab your questions. If I can't answer a question, please reach out to your Connection Account Team. Again, just want to say thanks for tuning in to Ask the Experts—around Windows 11 security with a little bit of AI mixed in. So again, just thank you for your time today and thank you for tuning in.