**CSD 101 - Day 4 - Non Security Workflow, Packaging, Validation**

0:04  
All right.

0:04  
We are recording.

0:06  
Welcome.

0:07  
It is day four.

0:09  
Yeah, you guys have come back.

0:11  
So yay, awesome.

0:14  
We are happy to have you back.

0:16  
And before I dive into the material for today, hopefully you can see my screen and what I'm sharing.

0:23  
It's what we talked about yesterday or at least it's, it's the last thing we talked about yesterday, which is the workflow for security cases.

0:30  
And so I wanted to take a moment and in case anyone had any questions, we are happy to answer them before we move forward.

0:39  
Any questions or any comments?

0:44  
No.

0:45  
All right, we're going to keep moving then.

0:47  
And then, of course, as always, please feel free to ask questions as we go along.

0:50  
You're welcome to ask a question through the audio or put it in the chat and we'll do our best.

0:56  
And James, you're going to help me monitor the chat.

0:59  
Yes, that'd be great.

1:01  
Yep, I've got the chat.

1:02  
Thank you.

1:03  
So now let's talk about non security workflow 'cause you know, we talked about the security workflow yesterday and we talked about how MSRC right is our partner for that.

1:13  
We talked about how how there is a case ID and an SLA, how there's some negotiations with the finders and then also how we triage on our side, how the onus is on us to figure out if it's really a vulnerability and what OS as it applies to you and of important to SIM ship.

1:30  
So now let's look at non security workflow and see how is that similar and how is that different because they're not exactly the same, right?

1:39  
There's some similarities, but not exactly.

1:41  
So what is it?

1:42  
So non security bugs, let's start with why do they even matter, right?

1:46  
If our, if our mission is keeping customers protected, like why are we talking about this?

1:51  
And so they are important.

1:53  
Part of this is just quality and functional issues, right?

1:57  
This might be, we've just released an OS version and there's some quality issues that we knew about that we just need to get fixed up.

2:03  
Some of this might be a quality issues that get uncovered later.

2:06  
Some of this might be, oh, you know what, we issued a fix and then we regress something, right?

2:12  
You know, we broke something, we need to fix that.

2:14  
So non security bugs are important.

2:17  
There's a, another category of non security bugs that I specifically want to call out because you will hear about it and, and you'll see that people talk about it with a great deal of seriousness.

2:27  
And these are what we call adoption blockers.

2:30  
And you know, we always want customers to move forward.

2:32  
We talked about the, the windows as a service strategy and about keeping customers moving forward all the time.

2:37  
Well, we always want that.

2:38  
We want customers to move forward.

2:39  
It's in their best interest.

2:40  
It's in our best interest.

2:42  
But every so often you'll find that when a customer is trying to move forward, they run into something that blocks them.

2:49  
It might be that as they're moving forward, they're finding that some of their settings are no longer being honoured.

2:55  
Or they might find that as they're moving forward, some of their data isn't, you know, quite moving the way that they had thought and being migrated the way they thought.

3:03  
Or some of their very critical line of business applications no longer continue to work.

3:08  
And they've investigated on their side.

3:10  
And the issue isn't on their side, it's something on our side.

3:12  
So these are examples of adoption blockers and they're called that way because it's preventing them from adopting the new version from moving forward.

3:21  
And these are very important to us because if we customers please move forward, it's better for you.

3:26  
You're, you know, getting the latest and the greatest, you're, you're more secure.

3:32  
And then if they can't move forward and we don't address that, it's really a conflict, right?

3:37  
It's not in our best interest.

3:39  
And so adoption blockers is a category of non security bugs that you'll hear about quite a bit and you'll notice that they get treated with a fair amount of priority.

3:48  
And then, and then one more thing I want to say about non security bugs.

3:51  
I know we touched on this a little bit when we talk about life cycle.

3:53  
The bug bar does change over time, right?

3:57  
And so you'll find that the older and OS's, the, you know, the, the OR, or another way to put it is the closer it is to the end of life, the bug bar will go up.

4:06  
You'll notice that.

4:07  
And as it's going up, it's getting more and more focused on enterprises and enterprise scenarios, right?

4:12  
So something to know about.

4:13  
We do have a bug bar.

4:14  
I think James can put a link to that in our chat window.

4:18  
And it is a generic bug bar in that, you know, you won't find every single example in there because we do have different areas in different parts of our team.

4:29  
But that bug bar is to help us get the same understanding.

4:32  
And then you'll find that as you attend your local ship rooms, you'll see how is it being applied in the snap area or the server area, for example.

4:41  
So, so This is why non security bugs matter and why we care about them.

4:45  
And then crit set, we talked about this earlier, crit sets, right, about critical situations from enterprises.

4:51  
Those also fall under non security, non security issues.

4:54  
So how do non security issues come to our notice?

4:58  
You'll notice that they're all in ADO, just like security items.

5:01  
They're all in our bug database.

5:03  
But these don't come from MSRC, right?

5:05  
Some of these come from the feature teams, you know, whom we who is our sister team.

5:10  
And it might be, hey, we're shipping the next version.

5:12  
And we know up front that there's a couple of things that, you know, aren't quite 100% and we need to get these there.

5:19  
You know, with the first few surfacing updates, some of it might be the future teams actually discover them later.

5:26  
Oh my goodness, We found something as we're working on this new version that actually impacts maybe the last one or two versions, so they can tell us about those as well.

5:35  
Some of these come in from customers via CSS, right?

5:38  
It could be a crit set.

5:39  
It could just be customers informed their account team about a problem.

5:43  
There's social analysis in the SSD team that we talked about the that's having this world class service, they're building it.

5:51  
There's a team called the RAM team and the M in that stands for monitoring and they monitor a wide variety of things.

5:59  
But one of the things they monitor is when an update is going out or when a new OS version is going out.

6:05  
What are we hearing from customers, whether this is Twitter or whether this is Technet or whether it's patch management with IT, which is a place usually where IT professionals are giving feedback and discussing and troubleshooting issues.

6:22  
And, and so they mine all of these different avenues and they look for trends and they go, OK, we think we found something, we think we found a problem.

6:30  
So these are some examples of ways that we find non security issues.

6:35  
We all come into the same bug database, same place where the security bugs are coming in.

6:39  
But in this case, they don't get opened the same way you don't get this one task group and a bug for each OS and support just comes in as one item.

6:47  
And then the CFE teams are the ones who typically pick it up and they will triage it.

6:51  
And you'll notice that here they're going to do a business justification.

6:55  
So in a security case, you know, we're looking for, is this really a security vulnerability?

6:59  
How severe is it, things like that.

7:01  
Here we're looking for business justification.

7:03  
Is this a legitimate issue?

7:04  
And do we really need to fix it?

7:07  
What does it mean for us to fix this, right?

7:09  
Because with every fix that we put out, there's a chance of regression.

7:12  
So is it, is it worthwhile, right?

7:13  
Is it worth the risk?

7:16  
Which OSS do we need to fix this for?

7:18  
You might find for example that someone reports an issue and it's on RS3RS3 is going to hit end of life in just a few months and we might say no, we don't think that it's worthwhile fixing an RS3, but we are going to fix it in RS5 and above, right?

7:32  
RS5 has a long term servicing channel, so we should fix it there and then we should fix it in 1903 and 1909.

7:39  
There's the more current releases.

7:40  
So you'll find that some of these discussions happen.

7:43  
And then the other thing that happens here as well is that because we're going to address the issue, we need to make sure that wherever we fix it, we always fix it in all the future OSS.

7:54  
So if we said no, we're not going to fix an RS3, but we are going to fix an RS5, you can't just stop at RS5.

8:00  
You have to fix it all the way up to the active branch.

8:02  
Because when a customer, you know, let's say they're, they moved to RS5, yes, everything's great.

8:06  
And then they, you know, they move up to 1909 and then again they regressed.

8:11  
They're like, wait, what happened?

8:12  
My non security issue came back and you're like, oh, yeah, we didn't put that fix in.

8:15  
You don't want them to regress, right?

8:17  
It's not a good experience.

8:18  
So we must fix for all future OSS all the way up to the active branch.

8:22  
You will come into some situations where you find, oh, that scenario doesn't even apply anymore or it's completely been rewritten or it works completely differently.

8:30  
So there's some homework we need to do there.

8:32  
But in general, the IDs fix it in an OS and all the future OSS.

8:37  
And this is where the feature team triage comes in where we have to work with them and say, hey, we think this is something that's worth fixing.

8:44  
Here's the business justification that we've done for it.

8:47  
And because we think it's worth fixing, it needs to be fixed all the way forward from wherever we think that we need to put the fix in.

8:54  
And that includes the active branch and in here's our case.

8:57  
And what do you think?

8:59  
And of course, the feature team, if they don't agree and they don't put it in the active branch, now you're gonna be in this weird situation where a customer, when they move forward, will regress.

9:07  
And so we have to have that discussion and get alignment and couple more things that I'll say about this.

9:14  
Usually the way that non security fixes work goes in the active branch 1st and you'll notice it's different from security fixes and security fixes, we said they must SIM ship.

9:24  
We can't ship at different times with non security fixes.

9:28  
SIM ship is not mandatory because this is not a vulnerability, right?

9:33  
And so our principle here is if you're going to fix it, fix.

9:36  
And if you're not going to do it simultaneously, because sometimes we don't do it simultaneously, then you should fix it in the newer OSS 1st and the older OSS later.

9:44  
So if you said RS5 and above, then you're going to fix it in the active branch and in 2004 first before you fix it in RS5.

9:53  
And the reason for that is the latest is always the best, right?

9:56  
And so we always tell customers move forward.

9:58  
It's always the best.

9:59  
We want to adhere to that.

10:01  
And the other thing you'll see is that we typically will say we're going to put the fix on the active branch and then they're going to flight that fix, which means that there's this set of people that are they, they are early adopters.

10:16  
They know that this is not fully done.

10:19  
They know that it's not released yet.

10:20  
They know there's going to be bugs, but they like it.

10:23  
They want to know what's coming.

10:24  
They want to be on the cutting edge and so the flights will go out to them and we have a chance to actually get our fixes out to them and to get bug reports back and also get telemetry back that we can analyse.

10:37  
You know, for example, we put this fix in, it went out into the flight and suddenly we see a spike and crashes in a certain area, right?

10:46  
Well, what's going on?

10:47  
Did our fix 'cause that that's an example of how we can leverage the telemetry.

10:51  
And so you'll typically find that we put in the active branch first, do the flighting, look at the telemetry, look at the, you know, the bug feedback and the, and the customer feedback.

11:00  
And assuming that it's all OK, then bring it down to the other OSS that are in in market up to the point where we said we would bring it in.

11:08  
So I'll pause for a second because I know I said a lot of things and ask if there are any questions or maybe there's some in the chat that I can pull up as well.

11:18  
I think we've been covering chat the other as I was thinking because Namrata has explained it perfectly.

11:26  
The only other nuance around adoption blockers, because you will hear that a lot is adoption blockers.

11:32  
Typically we care the most about the latest operating systems.

11:37  
An example would be like if an enterprise called said, hey, I'm having an adoption blocker from getting off of Windows 7 to Windows 8.1, we would go how about 10?

11:50  
Can you?

11:51  
So a lot of times with the adoption blockers realize that they're really important in the latest OSS, you know, think like the the latest OSS that they could be for like server, client, embedded, those type of things.

12:04  
Yeah.

12:05  
And the only other thing that I would point out here is the LTSCS are important, right.

12:09  
So in case folks, there's so much terminology, in case folks don't remember LTC stands for long term servicing channel and not every OS version has an LTSC, right.

12:20  
We have those every few years, H1RS1RS5.

12:24  
So you know, that's an example where you know, typically we would say, hey, you know, you're having trouble moving forward, how about you move further forward, right, get as close as you can to the latest and we'll make sure we address it there.

12:36  
But LTSC puts a little bit of a wrench into it where we go.

12:39  
We probably need to also fix it in RS5 because it is in long term support.

12:44  
It's going to be in support till 2028, something like that.

12:48  
It's 10 years, right?

12:50  
And I think we released it in 2018.

12:52  
So I think 2028 sounds about right.

12:54  
And so it's going to be a long time.

12:56  
And then in those cases, you know, we might need to fix it for that.

13:00  
The the one that has the LTSC.

13:01  
So, you know, I think James put it well yesterday that there's all these nuances and so these discussions have to happen.

13:08  
Yeah, yeah.

13:09  
Also has a great, a great question which is what is the ratio of security to non security bugs that we fix?

13:17  
Yeah, I will tell you on average we we usually are around 6 to 700 bugs per month that we are shipping.

13:29  
I would estimate there are metrics that I could go look up, but so we do have metrics.

13:35  
Yeah, yeah I was gonna say, but we really focus heavily on security.

13:41  
But in terms of what we can fix and what we get out it, it feels that it's almost like a 6040.

13:48  
I'm, I'm being because this is over a long time like it's it, it varies each month, but it really is kind of 60% security, 40% non security.

13:57  
And I think we have a Power BI, don't we?

13:59  
James, with the metrics that maybe you can put in the chat window.

14:02  
I will add one more comment to this.

14:04  
It's a it's a great question.

14:05  
Yeah, Sir, thank you.

14:07  
I will add one more comment.

14:08  
But this ratio is not static and I don't just mean month to month, but I mean for the time of that OS.

14:18  
So you will find that when an OS version first goes out the door, like 2004 is just going out the door, you'll find that the the number of non SEC fixes and therefore the ratio will be quite high, right?

14:29  
You'll have, you know, quite a few 100 right, non security fixes in in the first few months, as the OS gets more into its life cycle, you'll find that the non security, the bugs or the fixes are dropping in number, right?

14:46  
And you'll find that because of that, the ratio is changing.

14:49  
Now security, we still have to keep them secure.

14:51  
We're still doing security fixes, but the non security numbers will come down.

14:55  
And that is intentional, right?

14:57  
And part of it is by design, right?

14:59  
When we first release, there's all these problems we need to address.

15:01  
And part of it is also remember, the bug bar is going up.

15:04  
So you'll see that that changes over the life cycle of an OS.

15:07  
I think that's something to keep in mind, yeah.

15:11  
Any other questions we can answer so clear.

15:19  
All right, so we've talked about security fixes and non security fixes, right?

15:24  
And so I, I want to just call that one small thing, which is that, you know, the time that a team works on a security fixer, non security fix is variable.

15:33  
It depends on how complex the issue is.

15:36  
It also depends on the triage, right?

15:39  
It might be a very complex issue and it takes a long time to work on.

15:43  
It might not be a complex issue and doesn't take that long, but really there's other things that are more important.

15:49  
Now, if it was completely unimportant, of course we would just reject it.

15:53  
This is still important, but there might be some other things that are ahead of it.

15:56  
So you might find that an item comes in may not even be that complex to fix, but we don't fix it immediately.

16:03  
In the case of security issues, of course, I'll remind you that there's an SLA with the non security issues.

16:10  
It's less about the SLA, though.

16:12  
Of course we can't.

16:12  
You know, if a customer is waiting for a fix, you also don't want to be dragging them out indefinitely.

16:18  
But then this is where you know, you'll notice that that how long a security or a non security items, it's on a team's plate and how long it takes to fix is variable.

16:27  
And so if I remind you of this release timeline, you'll see that over here, it's a little bit open-ended, might be a week, a month, it might be multiple months here.

16:39  
So once you've done this, you've done the workflow and you've decided it's going to go in 8B or it's going to go in 9B or whatever, you know what check and deadline you have to work towards, right?

16:48  
And you get everything checked in.

16:49  
And then we have bills and packaging.

16:51  
And so let's talk a little bit about that.

16:54  
We have, I'll briefly mention about the build system.

16:58  
We in CSD partner very strongly with the Engineering Systems team.

17:04  
It is a sister team of ours.

17:05  
They do not sit within CST.

17:08  
It is, I kind of think of them as a shared resource, right?

17:11  
Multiple teams actually work with the Engineering Systems team.

17:15  
Of course, we are one of their large partners.

17:19  
And you'll notice that in our organization, we care about builds and all the associated things, right?

17:26  
Build machines, build tools, everything for all of this range of OSS, the latest Windows 10 all the way down to Windows 7, SP One and Windows Embedded OSS.

17:37  
If you talk to someone who's working on the active branch or the feature teams or sister teams, for example, under Henry Sanders, you know, they're, they usually are only thinking about the latest Windows 10 release, the next one and and the one, the last one that's in market, right?

17:51  
So just those last two.

17:53  
And so our bill systems are really quite complex and we have people that have to figure out, you know, the tools and the systems for all this variety of OSS and they don't all work the same way.

18:05  
So that's something quite interesting for our team to have to deal with.

18:08  
The bill team sits in SSD and I think they're called Boom build.

18:15  
Oh my.

18:15  
Do you know what it stands for James build optimization and operations and I forget what the M is.

18:23  
I will be honest managers.

18:25  
We'll we'll it is yes, it is I I will go look it up.

18:32  
Yes, James will save us, Yeah.

18:35  
But it's it's really quite complex to keep our bills running.

18:38  
It's not as easy as it sounds.

18:39  
I just wanted to call that out.

18:41  
So then once you've got bills out, you need to package all your fixes up.

18:44  
And I want to share a little bit about Windows 10 packaging versus 81 and earlier.

18:49  
You might remember that when we talked about the different OSS and there was that dark line and I said so many things changed when we went into Windows 10.

18:58  
And so I want, you know, packaging is one of those.

19:00  
And so I want to take a moment to talk about that.

19:02  
So the way packaging used to work for eight one and earlier, and you've noticed it's called out here, in the early days for every fix there was a KB.

19:11  
KB stands for knowledge base and so there is a KB, right?

19:16  
And so for example, I might have a fix for Windows 7SP1 coming up in the next month and James might have one and our colleagues might have others and there might be a whole set of maybe 30 fixes, right.

19:28  
And so there would be 30 KBS.

19:29  
You would have, you know, 30 individual little packages that get generated.

19:35  
And then, you know, we would go through all of the validations, etcetera.

19:38  
And then when we would release them, you would see 30 little KBS getting released.

19:42  
And as a customer, you would, you know, like my mom, for example, who she would just go scan, write, scan for updates.

19:49  
She would see these 30 little KBS pop into her UI.

19:52  
Or if you're an IT admin or an enterprise, you would see them all pop into your console, your centre console or whatever software you're using to manage updates.

20:02  
And so the system worked for a long time.

20:06  
It was successful, but it also had some issues with it.

20:09  
It basically we ended up with a fragmented ecosystem, right?

20:13  
And, and the reason for that would be that as a customer, right?

20:17  
You could look at these 30 KBS and go, I want that, that, that, but I don't want that and that, and so you can make those choices, right?

20:25  
What it then means is that you know.

20:28  
Everyone out there has a machine that looks slightly different, right?

20:32  
My machine has all the updates because I took all my updates.

20:36  
And James's machine has only about half of them because he was picking and choosing, and somebody else might have like a tenth of them, right?

20:43  
And you can imagine now when something goes wrong, how hard it is to troubleshoot because you don't quite know where you're starting from.

20:50  
So it caused some concerns from that perspective.

20:55  
Of course, also internally, it was a lot to manage.

20:57  
You can imagine that every single team within, within CSD was having to manage, you know, their individual KBS and doing all of the legwork and the paperwork for it.

21:08  
And then in our pipeline team, right, processing all of these many, many 10s and 10s of KBS, which you then multiply by the number of OSS and now hundreds and hundreds of KBS that are going out every month.

21:21  
And so we said, wow, you know, can we change this?

21:24  
And so when Windows 10 came along and that was where that dark line was, and I said things changed.

21:30  
So when Windows 10 came along, we said, OK, we are going to go with a different model.

21:34  
We're going to go with a cumulative update model.

21:37  
And you will often hear people talk about, oh, have you installed the LCU or have you looked at the 7B LCU?

21:43  
What they're really saying is the latest cumulative update.

21:46  
That's what LCU stands for, L being latest.

21:50  
And the idea here is that when when we send updates out, they're cumulative.

21:56  
And so when you send an update out on, let's say the OS has just just released in May and the 1st update is in 6B, all the updates are in there.

22:08  
When you come to 7B, the next month, 7B has the new fixes for 7B and all the previous updates from 6B and so on and so forth.

22:16  
And so at the end of the year, like A12B for example, it'll have all the new fixes for 12B, but it'll also have all the fixes from 11B10B9B8B7B and 6B, right?

22:26  
It is truly cumulative.

22:29  
Now it's again, you know, good and bad.

22:32  
As always, change is hard and this was a hard change and the real reason we did it was we didn't want to have this fragmentation anymore.

22:42  
Customers did struggle with it.

22:44  
Change is always difficult and they struggled with a few things.

22:48  
They struggled with the fact that they don't have choice anymore.

22:51  
They felt earlier that they could make an they can make a make a choice about what they wanted to install and what they didn't want to install.

22:57  
And here it's all or nothing.

22:58  
Either take the LCU or don't, but you don't get to pick and choose.

23:03  
I would assert that I think people felt like they had a choice, but in reality they weren't really informed well enough to make the right choices.

23:12  
So I actually think the cumulative model is great because you're getting all the security fixes and everything that you need to truly be protected and productive.

23:20  
But of course for customers, they felt like, wow, you took away my choices.

23:23  
I I can't choose anymore.

23:25  
That was really hard.

23:26  
I think one of the other things that was hard as well was customer said, wow, this is a lot larger, you know, this one package obviously a lot larger than me taking the smaller packages that were a lot smaller.

23:37  
We did some work to address the size issue.

23:41  
And and so without going into all the details that if anyone's interested, we can certainly connect you to the right people.

23:47  
We are, you know, we, we did work so that we can send down just the fixes that you need.

23:55  
You're not necessarily getting the whole payload.

23:57  
So if you were, if you had turned on your machine in May, taken the new OS version twenty O 4 and taken 6B and then turned off your machine and went in a cruise and came back in 12 B and you were trying to install the 12B update because it's cumulative.

24:12  
If you don't need to install everything in between, you just get 12B.

24:16  
You know, you wouldn't be reinstalling all the 6B updates, right?

24:20  
You're just going to be installing the difference, the delta.

24:22  
But yeah, it was, it was a bit of a hard shift in the beginning, right?

24:26  
Took a while for customers to adjust.

24:29  
But over time, with some of it was education on our part, Some of it was us listening and reacting, you know, giving, for example, you know, solutions for the size concerns or for example, understanding, Wow, we really need to be more transparent in our communications.

24:42  
So our release notes need to have more details about what's in the fixes, right?

24:46  
Because customers not felt like you didn't give me any choice.

24:48  
I'm forced to take everything.

24:49  
Well, OK, look, let's tell you what's in here, right?

24:51  
Let's ease some of the anxiety.

24:52  
So over time, I think we then found and we were able to prove that the cumulative model was successful.

25:01  
I was gonna say though, the, the, the definitely because change is hard.

25:07  
It took a a mental shift, but over time they really did land on Oh my God, this is so much easier.

25:15  
I only have to approve one package for my whole environment and and just start deploying.

25:22  
Whereas they used to have to go and evaluate each one by 1 by 1 by 1 by 1.

25:25  
And so yes, they had choice and they had and if one didn't work, they could pull that one out.

25:32  
And there was all these little buttons and lovers, but they would end up where they had not even their it would know.

25:37  
Do we have everything installed?

25:38  
And they'd be like, I don't know, too complex, way too complex.

25:42  
Yeah.

25:42  
And now when somebody asks us, hey, am I secure?

25:46  
We're like, install the latest.

25:48  
And yes, it's that simple now.

25:51  
And I think because James, you and I of course know this because we deal with this all the time in, in the areas that we are in, but something that's not obvious right at the beginning that I started realizing I was talking to customers.

26:04  
And I've learned over time, they have these huge mixed environments too.

26:09  
So it's, you know, when we're talking about lots and lots of updates, it's not just for one OS.

26:12  
So I remember this time when I was talking to a customer and they had such a wide variety of OSS in their environment.

26:20  
They had Windows 7, SP one, they had Server 2008, Server 2012, Server 2016, Rs one, RS3RS5 and probably Apple 7.

26:33  
Chromebook probably like, oh, not even thinking about those.

26:36  
Like I think just our stuff.

26:38  
7:00 And then of course, don't forget Office and everything else, but just even Windows, I think I counted 7 right in my hand.

26:44  
And now imagine like having 30 updates per per each of those OS's.

26:48  
It's, you know, 7 \* 30.

26:50  
It's a lot.

26:51  
Yeah.

26:52  
Yeah.

26:52  
I remember being.

26:53  
It just blew my mind the first time I heard about that, I thought, oh, my God, it really is complex, you know, to have to manage it that way.

26:59  
Yeah.

26:59  
I, I think the real worry was the job security of these system administrators because now you just have to click yes and go, oh, man, I don't know.

27:13  
So that was, you know, the big change, that dark line made a big change.

27:16  
And so once we proved out this, you know, we proved out that the LCU model does work, then we said, OK, should we be bringing this down?

27:26  
Should we bring it down to 8 one and earlier what should we be doing?

27:29  
So we had a side of people get together and really work on this and investigate and we made some decisions around one.

27:38  
How far down will we bring it?

27:40  
You know, should we take it to Windows XP?

27:42  
Should we take it to Windows Vista?

27:43  
Right.

27:44  
And we decided to take it down to Windows 7 SP one, right?

27:47  
Some of the other OSS were already in CSA, for example, the custom support agreements, you know, those end of life had been reached and we had, you know, 1015 customers on them or they were very close to being end of life and we just didn't feel it was worth the investment.

28:02  
So we said, OK, we're going to bring it down as far as Windows 7 SP one.

28:06  
And then we said, OK, the second part of the investigation was how do we really make it cumulative and do we truly make it cumulative or not?

28:15  
And so you'll notice here I use the word roll ups.

28:18  
It doesn't say cumulative update, it says roll ups.

28:22  
And so the reason for that was when the investigation was being done, we said, OK, can we go back to right when the OS first released and truly make a cumulative update.

28:32  
And what we found was that it, yes, of course you can, everything is possible in code.

28:37  
But we found that really doing that was incredibly complex.

28:41  
And some of that was because, you know, our branch structures, remember these products are very old.

28:46  
Some of these branch structures were quite complex.

28:48  
There were these, you know, the LDR branches and the GDR branches and all the fixes were, you know, in slightly different places.

28:55  
And So what, and there was quite a few technical complexities.

28:58  
And So what we decided was no, we're not really going to go back and make a truly cumulative update.

29:03  
What we're going to do is we're going to pick a point in time and from then onwards it's going to be cumulative.

29:09  
And so one way that people would talk about is they would say it's partially cumulative because if you started from here, from here onwards, it's cumulative, but not, you know, it's not cumulative from the time the OS released.

29:19  
And so now how to communicate that?

29:21  
Because you know, if you have LC us and then you have partially, you know, partial LC us, like it's kind of hard to say.

29:27  
So we said, OK, we're going to roll ups, we're going to talk about them as roll ups.

29:30  
It's a little bit distinguished between the LC us and what this is because they're really not the same.

29:35  
And so you'll hear people talk about these and you'll notice that I have some some two letter acronyms here, SOMR and PR.

29:45  
These are the types of roll ups that we have.

29:48  
So, SO stands for security only Mr.

29:52  
stands for monthly, monthly roll up and PR stands for preview roll up.

29:58  
And if you, if you were to look at the public names, I think they're called security update, monthly quality update and preview update, right?

30:07  
Yeah, I think that's how we the technic, the official approved name that goes out to customers.

30:14  
And So what are these?

30:15  
So, and if you were to think about a customer who was in Windows 8.1, right, on the B release, they got a slew of security KBS.

30:23  
And on the C release, they got a slew of non security KBS, right?

30:27  
And they had all this autonomy of what they could install.

30:29  
And so we wanted to bring change, but also recognize that, you know, maybe too much change might be a little too crazy.

30:35  
And So what we said was OK, for the B release, instead of getting 30 security KBS, you're going to get one.

30:41  
SO one roll up, it's going to have all the security fixes for that month.

30:45  
If you do nothing else, just take the.

30:47  
SO just be secure, right?

30:50  
So now what about all the non security fixes that go out on the C?

30:53  
Well, we have to still put those out there and we didn't want to send out all these individual packages.

30:57  
And so we said, OK, we're going to make a preview roll up.

31:00  
Great.

31:01  
The preview roll up has the security fixes for that month and it has the non security fixes for that month.

31:07  
Fantastic.

31:08  
So if you want to take both, you can take both.

31:11  
And then what's the monthly quality?

31:12  
Well, the monthly quality is it has it goes out on the B release, right?

31:19  
The SO and the and the Mr.

31:20  
go out on the B release.

31:21  
The PR goes in the C release because it has a non security.

31:24  
The monthly quality has the security fixes for that month.

31:27  
It also has the non security fixes from the previous month, right?

31:31  
And So what Why?

31:33  
Because we when we put out the non security fixes, right, it's had some time to get baked to get customer feedback for us to react to it, right.

31:41  
And so by the time it comes to the next B, it can be put into the Mr.

31:45  
and we can feel pretty confident about it.

31:46  
So ideally we want customers to take the Mr., we want them to take the monthly quality update.

31:51  
It comes out on the B release.

31:53  
Please take it.

31:54  
It has the security fixes for this month, so you are protected.

31:57  
And then it has the non security fixes up to the previous month.

32:00  
So you can feel pretty confident that they're baked and they're good and you can be productive, right?

32:04  
So ideally everyone wants to be or ever, we want everyone to be on the Mr.

32:08  
train, right?

32:09  
Like Choo Choo Mr.

32:10  
train.

32:11  
Some customers don't want that.

32:13  
And so you'll find that there are customers that are on the SO only train.

32:16  
They're like, listen, I just want my security fixes.

32:19  
They're on the SO train only.

32:21  
And then some customers will take the SOS and then and maybe a small subset of their devices, they'll even take the PRS.

32:27  
They just want to check out what's coming the next month.

32:30  
So, so we have these three roll ups that's gonna set with with the.

32:33  
SO you'll find that most enterprises use them for their server scenarios because they need them to be very solid.

32:42  
They care mostly about security.

32:44  
They're usually older servers through 2008, 2008, R2, 2012.

32:49  
So they're good, they're functioning.

32:51  
They don't want to mess with them.

32:52  
And so that security only really came from a push from enterprises to say I need something I only care about being protected.

33:01  
It was minimum change.

33:02  
Yeah, minimum change.

33:03  
And it was us being customer obsessed.

33:05  
We're like, OK, get it.

33:06  
We will create a security only it's not a roll up by the way, every single SO is its own entity.

33:14  
So you for that month for that month.

33:16  
And so SO is different that it is not a A roll up partially Kimmel it up.

33:22  
Yeah, exactly.

33:23  
That's right.

33:23  
So you can't go and install April and think that you've got in January, February, March.

33:28  
So it is, let's do that with the Mr.

33:30  
though, with the Mr.

33:32  
That's right, it does which which of course we want everyone to be on the Mr.

33:35  
train.

33:36  
And so you could turn off your machine and come back and four months later you could just take, you know, the latest Mr.

33:41  
and you're good.

33:42  
It'll have all those security fixes that you missed.

33:44  
It'll have all the non SEC fixes that you missed.

33:46  
That's right, absolutely.

33:47  
And so, so, so the security on it was a compromise that we made with enterprises who were like, hey, I have a specific server, like an ATM or something.

33:58  
I don't want anything but security.

34:00  
I know I've gotta have it.

34:01  
And so that's, that was us being listening to customers and coming up with a solution for it.

34:06  
Yeah, yeah.

34:07  
Because we we do recognize, right.

34:08  
Again, change is hard.

34:10  
These customers have been on these OSS for years and years and years.

34:13  
We wanna be respectful, but we also wanna move them forward and we wanna move them forward in a way that's feasible and you know, kind of push them a little bit a little bit discomfort, but also, you know, have be respectful and listen to them.

34:25  
We would like the concept of healthy friction.

34:28  
Healthy friction.

34:29  
I like that too yes yes, we we hear that in ship room sometimes.

34:34  
So I want to talk about couple more things and we spent a bit of time on this slide, haven't we?

34:38  
Doesn't look like a lot of words in the slide, but there's certainly a lot of things to say.

34:42  
I want to talk a little bit about these specialty packages.

34:45  
I've, I've kind of skipped over them so far.

34:48  
So the LCU and the roll ups are really the big thing, right?

34:52  
For the most part, that's what you're going to hear about.

34:54  
It's what people are going to be talking about.

34:56  
But we do have some other update types.

34:58  
There's actually a whole slew of package types.

35:01  
Our wiki is fantastic and has them all on there.

35:04  
There's some package types that I don't think I've ever even seen us use in 3-4 years, but we certainly have the capability.

35:10  
But I want to talk about just a couple of them, actually three of them.

35:14  
So because those are the most common and so that when someone talks to you about them, you have some context.

35:20  
The first one is an SSU.

35:22  
It's it stands for servicing stack update.

35:25  
And this is the idea that, you know, we talked about earlier, there's the update client, right?

35:31  
And it, and then that's, it's, it's calling up to the service, right?

35:35  
It's asking, you know, it's saying, here's my attributes.

35:37  
It's asking what updates are available for me.

35:39  
There's an evaluation that happens, right?

35:42  
And then when the update comes down, right, it goes in and it looks at the components and it, so it does a whole bunch of logical evaluation.

35:50  
Sometimes something will go wrong in the servicing stack.

35:53  
Either it's the security vulnerability that we've found or there's a bug.

35:57  
You know, there could be a variety of things now.

36:01  
So we don't often make change the SSU, you won't see that every month there's an SSU update, but but every, every now and then we have something we need to fix there and we need to issue an SSU to fix it.

36:13  
Fixes that go in the SSU for the servicing stack do not go into the roll ups and into the LC US.

36:19  
They completely live separately in this entity.

36:22  
And this is this is the only way, this is the only package type where you can deliver those fixes.

36:27  
Then there's set up DU and GDRDU.

36:29  
So set up DU is when you go through the set up experience, or you might, if you've worked in other teams at Microsoft, hear about as the Ubi experience or the out of box experience.

36:38  
It's very important that your out of box experience is a good one.

36:41  
And so most teams spent a ton of time making it a really solid experience.

36:45  
But every so often there's something we need to fix.

36:47  
There might be a vulnerability or might be there's a problem.

36:51  
Not very common.

36:52  
I think it's been a long time since we've done a set up to you because again, team spent a lot of time making it rock solid.

37:00  
But if we needed to fix something during that set up time, we would issue a set up to you.

37:05  
And during the set up experience it will go out and call and ask is there an update for me?

37:10  
Yes, there is.

37:11  
OK, bring it down and, you know, incorporate it.

37:13  
And then GDRDUGDRDU is this concept that when a customer is moving from an older version to a newer version, which yay, we want them to, we want to give them the best possible experience.

37:26  
So if a customer is on RS3 and it's about to hit end of life in a few months and they're moving forward to 1903 or 1909 or you know, any, any version, when they move forward, what we, what we need to do is we, well, they could move forward and they could jump to the, the version that at the release time, the RTM version.

37:48  
And then once they move there, they would need to take the latest cumulative update.

37:52  
And then now they're secure.

37:54  
We don't want them to have these two hops.

37:56  
And So what we do is we have a GDRDU that says you move forward and where you land will be that new version plus all the latest updates for it, the latest security updates for it, right, the LCU.

38:08  
And that means you have one hop.

38:10  
So if I'm on RS3 and I jump to RS5 or 1909 today, I would basically be jumping to 1909 with the 5B update because that was the last update that went out, right?

38:22  
6B has not yet gone out.

38:24  
So it's one hop, it's a better experience.

38:26  
So that's what GDRDU is.

38:27  
And I will pause in case and explain and number of the explain the concept of a hop because that might be a strange term for most people.

38:36  
Oh, like you mean moving forward?

38:38  
Yeah, the hop because we will use this term hop and and it it typically means that I install something and I and it looks like I'm gonna come into the Windows experience and then all of a sudden I get a you've got an update.

38:51  
And so that is a hop is usually when I move from a major or minor version of the operating system is considered a hop.

39:03  
Very true.

39:03  
Yeah, you're right.

39:04  
I think we use a terminology all the time not realizing it might be, Yep, unusual.

39:08  
And if you want to look on your computer and say, hey, what version, you type Winver in your search bar and Winver will pop up the and, and that is how you will know what the major and minor version, which includes the OS and then the Lcus.

39:26  
Yeah, which again, PLC is your friend.

39:28  
Because if someone reaches out to you, especially in the feature team, and they go, I've got this machine and it's, you know, blah, blah, blah, build number.

39:35  
And you're like, is that Rs 345-1903?

39:37  
Like what is it?

39:39  
You can go into PLCAK dot MS/PLC, which James had put in the chat yesterday.

39:44  
And when you go and you click on any of the lines and the details page opens up, it shows you the build number, at least the major build number that we start with.

39:53  
Yeah, any questions?

39:56  
There's a one, one more concept I want to talk about on this page before, before we move forward, but I'll pause for any questions because I know it's a lot.

40:08  
No questions.

40:09  
Well, I want to talk very quickly about the idea of supersedence.

40:15  
Right.

40:16  
So especially because we're talking about cumulative updates, I think it might be a worthwhile, worthwhile thing to talk about.

40:22  
So when we have a Windows 10 update going out, right, it's an LCU and it goes out.

40:28  
And let's say with Windows 10/20/04, the first LCULCU that goes out is going to be 6B and they'll be 7B8B9B, right?

40:37  
And they're cumulative.

40:38  
So if I were to set up a Windows 10/20/04 machine, take 6B, and then shut down my machine and open up in December, I should really be able to just take the 12 B, right?

40:47  
I shouldn't have to take 7B8B9B10B11B in between.

40:51  
12B has it all.

40:52  
It's, it's a cumulative update.

40:55  
Now imagine if as a customer, I opened up my machine and I was offered all of them, 789-1011 and 12.

41:01  
It's a bit of an odd experience, especially when they really don't need to take each one of them.

41:06  
They can just take 12B, right?

41:08  
And so you have this concept of supersedence, right?

41:10  
Or a supersedence chain where we say, hey, every one of these are superseding the ones before 7B supersede 6B8B supersede 7B, right?

41:20  
That chain keeps building.

41:21  
And So what you'll notice is a customer is that is that when you went, when I opened that machine up in December, I'm only going to be offered the 12B update.

41:33  
I'm not going to get offered 1110987 because on our back end, right, we have said, hey, this update supersedes the previous ones.

41:41  
And so we intelligently only offer you the latest, right, because we know what that supersedence chain is.

41:46  
And I bring that up because as you're working, especially with CFE folks, working with SSD folks, this terminology will come up and then, you know, Yeah.

41:56  
Any questions on that?

42:02  
Nope.

42:03  
All right, let's move forward.

42:07  
We have validation and I am going to share some information.

42:12  
I'll try to be as quick as possible.

42:15  
And then if we have Louise on the call, please feel free to jump in at any time.

42:20  
He knows a great deal about validation and we would be absolutely honored to have you speak.

42:27  
So you know, I talked about DTP, the depth test pass and this is where the usually the sweeze they want to test their specific fixes, right?

42:37  
They might do some unit testing on their machines, but then they submit ADTP request to have it run on the lab machines and they might say I want to run these specific 10 or 15 cases, right.

42:47  
They can do that.

42:48  
But then we get into MTP monthly test pass and we have two weeks of that week one and week two.

42:53  
And I mentioned week two is generally thought of as a rerun week.

42:57  
We certainly make full use of those two weeks, right?

42:59  
There's a whole lot of test collateral to go through and you'll notice that there's different types of validation that's happening during these two weeks.

43:06  
So the first one is automated test and Luis actually talked about that a little bit yesterday about the number of jobs that get run right.

43:12  
These are the automated tests that are happening so the lab gets set up right all the machines get set up all the different versions of the OS that are in support right are are are part of this.

43:23  
So machines are getting set up for Windows 7, SP one for Server 2008, for Windows 8.1, all the way to the latest version that we support.

43:31  
And then then the tests are getting deployed, The latest updates are getting deployed, and then the tests are getting deployed and being run.

43:38  
And then the results are getting reported back.

43:40  
And there's a central report where you can see your consolidated test results.

43:44  
So you can then figure out what's going on is if there's a failure, there's access to logs, etcetera.

43:50  
It's the automated test.

43:51  
We do have a whole slew of manual tests actually that get run too.

43:55  
And we have a vendor team, I believe they sit in India and they are running these manual tests and again they do the same.

44:02  
They set up the machines, they run the test and then they report the results back and people will be validating those.

44:07  
We partner heavily with the engineering systems team again for this.

44:10  
A lot of our infrastructure is either owned or managed by them and so you'll find that people that work in TNT and CFE who who work on MTP work with them very, very closely.

44:20  
We also have an app compat testing and this is stands for application compatibility and the we have a team run by Ramesh Gude, so you might be seeing mails from him come into your inbox and his team basically goes through and runs a whole slew of tests against all the OSS and support making sure that we're not breaking application compatibility.

44:43  
They do a lot of analysis on what test they should be running.

44:47  
For example, you know, for browser, what are the top sites we should be looking at or what are the top applications?

44:54  
So, you know, antivirus, we often have issues with those.

44:57  
OK, what about financial apps?

44:59  
What about, you know, so they go through and they do a lot of analysis.

45:02  
What are what are the top kind of industries within those?

45:06  
What are the top applications?

45:07  
What are the ones that seem to consistently have problems?

45:10  
So they they get a bunch of information, they slice and dice it in multiple ways and come up with this list of, you know, this matrix of what we should be testing.

45:20  
This app compat's very important to us.

45:21  
Many times we've caught very important issues here where we find out that, hey, a fix that we're doing is causing a problem in another another company software.

45:32  
And you know, it's really a lose, lose when that happens.

45:35  
There's no, I mean, we, we could say, oh, it's not our fault.

45:37  
It's on their end.

45:38  
It's not a win for us.

45:39  
It's a lose lose.

45:40  
Right.

45:41  
I'm going to do, I have time for small story.

45:43  
I'm going to try it really quickly to tell a small story.

45:46  
Do you remember this?

45:47  
Yeah, quickly.

45:48  
Yeah, quickly.

45:48  
I'll be quick.

45:49  
Do you remember the Citrix issue, James?

45:50  
We had this vulnerability and we were fixing it, which was the right thing to do.

45:56  
And in fixing it, one of the things that we did was shut down this undocumented API which customers are not supposed to be using.

46:04  
Citrix have been using it for many, many years and quite possibly with no I'll intention, right?

46:10  
It was out there, they used it and was undocumented and maybe the developer in there and didn't know, right?

46:15  
That's fine.

46:15  
But now that we've tightened it, they can no longer actually use it.

46:20  
And what ended up happening was that if you were running that particular piece of Citrix software on your machines, if you're one of their many, many customers and they have many, you could actually no longer log into your machine.

46:31  
Imagine coming in and to your work and not being able to log into your machine.

46:36  
I mean, this is a bad day for everyone, right?

46:39  
Because it's a bad day for that person.

46:41  
And it really, really is a horrible thing to happen to you as a customer.

46:45  
It's a bad day for Microsoft.

46:46  
Because what are they going to say?

46:47  
I took a Microsoft update and this stuff just stopped working.

46:50  
What is wrong with Microsoft?

46:51  
I'm just not going to take security updates anymore.

46:54  
It's so painful.

46:56  
This is the narrative.

46:57  
Oh my gosh, please take your security updates.

46:59  
Yes, but nobody wants to hear that, right?

47:00  
OK, so then we can say, oh, well, it's not really us, it's Citrix.

47:05  
Go talk to those guys.

47:08  
It doesn't really work that way, right?

47:09  
People still have that association.

47:10  
If I took a Microsoft update and it messed my system up, and imagine Citrix is not a good day for them either.

47:17  
It's an awful day for them.

47:18  
They have thousands and thousands of customers, millions of customers potentially, and then now have machines they can't use and they're having to react to this.

47:26  
So, you know, this is an example of where application compatibility is really important.

47:32  
We need to be able to find these things and fix them.

47:35  
In that particular case, we did find it during our validations.

47:38  
Yay.

47:39  
And so we contacted Citrix.

47:41  
We're like, what up?

47:42  
Because of course, we first triage and we investigated, then we realized what was happening and we're like, what up?

47:47  
And so Citrix said, Oh my goodness, OK, we need to fix this.

47:49  
Can you please not release the security fix because we need time to to be able to fix it on our end.

47:56  
And if you remember the timeline by the time you're in MTP week, there's only about like, you know, maybe depending on where you are in MTPS, maybe about two or three weeks before we're going to ship.

48:05  
And that wasn't enough time for them to fix their issue on their side and deploy it and make sure all their customers get it right.

48:12  
Because you need saturation because just because you put an update out there doesn't mean customers are taking it on day one, right?

48:17  
And so they needed saturation too.

48:19  
And so we said OK, and we didn't ship that security fix.

48:23  
I would like to take this moment.

48:25  
Yes, I would like to take this moment to remind you that we SIM ship our security fixes, which meant that we went back and we removed it from every single OS that it was applicable to.

48:34  
And I think it was applicable to all of them.

48:37  
So we removed it from from all the OSS, which of course meant we were churning packages and builds and packages for every single OS that that we were going to ship AB update for.

48:48  
So yeah, that was, you know, exciting.

48:51  
But that's an example where like, you know, application compatibility is really important.

48:56  
And this brings me to some of the other validations that we do partner testing.

49:01  
There's the thing about 33 or 35 partners, I forget.

49:05  
These are all internal partners.

49:07  
Great examples are officeand.net and Sequel, right?

49:11  
They are also doing security fixes, right?

49:13  
Everyone ships security fixes on the B week together, yes.

49:16  
And so they want to make sure that our fixes are not doing anything to mess up their systems and their fixes are not doing anything to mess up our systems.

49:24  
Everything's working well together.

49:26  
Again, remember, our customers are Microsoft customers.

49:29  
They're not just a Windows 10 customer and especially enterprises, they might be running, you know, Windows 10 particular version plus office plus sequel plus exchange plus SCCM plus.

49:40  
I don't know so many, many, many things, right.

49:43  
Everything needs to work well together.

49:44  
So this partner has things really important and then we have these pre release validation programs and these programs actually there's three of them together the the pre release.

49:54  
So this is where and we now get into the Serve team under CFE.

49:59  
They actually run the pre release validation programs.

50:02  
The previous programs are all managed by our MTP team and there's the self host which is you and me and everybody in our team.

50:09  
We are self hosting.

50:11  
If you are not sure if you're self hosting, you can find out.

50:15  
If you are for some reason unable to do it, contact NAV Cameron and he will get you hooked up.

50:20  
Please self host, it's very important and if you find issues please report them.

50:24  
That's very important too.

50:26  
CSCO, this is the organization that manages all of our Microsoft infrastructure network devices.

50:35  
We know, we often talk about, oh, the IT admins and another enterprise.

50:38  
These are ours.

50:39  
They're ours, and so they are very interested in getting their hands on the bits before we release them.

50:45  
It's a win win.

50:47  
It really is, because if they find a problem, we want to know about it before we ship it.

50:51  
And if they want to, it's a win for them too, because they want to know that come patch Tuesday, when they start deploying these fixes out, everything's going to work.

50:59  
Imagine deploying fixes out to a company as large as ours and having systems being taken down.

51:04  
This is a terrible, terrible outcome.

51:07  
So they want that, you know, it's a win, win.

51:09  
Good for them, good for us.

51:10  
They have actually helped us in the past to find issues.

51:13  
When they've done their testing and gone, you know, this doesn't work anymore and we go, OK, great, and we fix it.

51:19  
You know, Wi-Fi doesn't work anymore, for example.

51:22  
I think that was one of the examples of things that they found.

51:25  
I want to take 10 seconds to also call out that our own CSCO team, as well As for most other enterprises, especially large ones, they have goals around deployment of security fixes.

51:38  
Typically, it looks something like this.

51:40  
Two weeks from when a security fix is released, we should have 95% saturation.

51:46  
It looks something like that might change a little bit from enterprise to enterprise, which means that from any time we release a security fix within two weeks, 95% of all devices need to have it.

51:55  
You can this brings me to when we do an out of band release for a SERP, how disruptive that is because now they still have two weeks to get that out and they might already be, you know, they might be on day 10 of, you know, deploying the patch Tuesday staff and now we've come out with a SERP Bing and now they've got to get that out too, right?

52:14  
Very disruptive.

52:16  
And then SUVP, this stands for Security update validation program, which doesn't tell you much of what it is, what it really is.

52:23  
It's a program run by CSS, our support organization and we partner with them and this is a really great program.

52:30  
This does testing with our enterprises, our customers.

52:35  
These customers are under NDA, under a non disclosure agreement because we give them the security fixes ahead of time.

52:42  
It's very important that of course they don't leak them because we don't want to surf ourselves and put our customers in a bad spot.

52:48  
So they get these security updates under NDA and then they test them again.

52:52  
We're going for a win win.

52:54  
If there's a problem, we certainly don't want to release something that's bad.

52:57  
So we would love to hear about it and it's great for them.

53:00  
They want to know if their software is going to break.

53:02  
Citrix would love to know, right myself is going to break.

53:06  
I don't want to be in that position where I'm having to like react to it and fix it later.

53:09  
I'd rather know now.

53:10  
And so they actually want two things they want to know like CSCO.

53:14  
When the update comes out and I deployed in my organization, is everything going to be OK for my org?

53:19  
Are my line of business apps going to work?

53:20  
Can I still do payroll?

53:21  
Can I still do inventory?

53:22  
Can my factory still work?

53:24  
You know, and my printer is going to work.

53:26  
Is my Wi-Fi going to work right?

53:27  
All that's great.

53:29  
They also want to make sure that if they're like an ISVA vendor who's putting out software like Citrix, is that still going to work?

53:35  
Are my customers still going to be OK?

53:37  
So we're really going for a win, win, win for US, win for them.

53:40  
And then I will take 30 seconds to touch on update staging lab or test base, right?

53:44  
That's the new name.

53:47  
And this is really, you know, future thinking, right?

53:50  
Which I think it's the now, it's the now we have this SUVP program.

53:55  
We still do.

53:56  
We work with enterprises and we thought, you know, can we do, can we do even better?

54:01  
And so the idea of update staging lab or test space came up where we said, hey, we're going to take and build sort of the space in Azure where we bring our latest security updates, customers bring their their workloads and we help test them there.

54:17  
We get some information, some telemetry, they don't have to manage all of this churn.

54:23  
And it's a win win, right?

54:26  
And I know we're right at 3:00.

54:29  
I will stop, but if there are questions, I'm happy to stay for a few minutes and answer.

54:37  
That was a lot.

54:38  
We covered a lot.

54:39  
Yeah, this was a lot today.

54:41  
And, and, and there's a lot of complexity and depth to all of this.

54:45  
So don't be afraid to go dive into the wiki and, and, and dive into each of these areas.

54:50  
There's a whole page on test base.

54:52  
They're an incredible team that has just, they just launched I believe like last October at Inspire or ready or one of those events.

55:01  
So they're very fascinating team to go dive into how they're trying to solve the problem of quality and enterprise interaction.

55:09  
Yeah.

55:10  
And I want to shout, give a shout out that the, the this is one of the teams where we built out our, our office in Lagos.

55:20  
And so a lot of our colleagues that work on update staging lab are in Lagos.

55:24  
Yeah, right.

55:25  
Yeah.

55:27  
Any questions we can answer all crystal clear.

55:35  
Great.

55:36  
Thank you, everybody.

55:38  
Thank you.

55:38  
We'll see you tomorrow.