



RUNAS RADIO



<http://www.runasradio.com>



RunAs Radio is a weekly Internet Audio Talk Show for IT Professionals working with Microsoft products. The full range of IT topics is covered from a Microsoft-centric viewpoint.



Text Transcript of Show #063
(Transcription services provided by [PWOP Productions](#))



Frank Simorjay and Dan Griffin bring NAP and Forefront Together!
June 25, 2008





[Music]

Brandon Wenn: From runasradio.com, you're listening to RunAs Radio, the Internet audio talk show for IT professionals with Richard Campbell and Greg Hughes. This is Brandon Wenn, announcing show #63, recorded live June 11th at TechEd Orlando with guests Frank Simorjay and Dan Griffin. RunAs Radio is produced each week by PWOP Productions, providing professional media and podcasting services online at pwop.com.

Richard Campbell: Hi, this is Richard Campbell, you're listening to RunAs Radio we're coming to you live from the TechEd Orlando IT Week, on the floor, in the noise, the vendor space is open, so it's a little crazy here and with me, as always, my co-host Greg Hughes.

Greg Hughes: Hey, how are you doing Richard?

Richard Campbell: I'm good sir. We've been knocking the shows out. Speaker Idol is about to start so we're racing to get one more done before it really gets crazy behind us at the IT stage.

Greg Hughes: Yeah, we are. We have some people with us today that have some really cool stuff to talk about. Now we've heard about Network Access Protection before, we've talked about that here. I think we've talked briefly about Forefront Security. What we're going to do today is we're going to talk to a couple of guys who are going to help us put those two things together.

Richard Campbell: Gentlemen, I'll get you to introduce yourselves, starting with Frank.

Frank Simorjay: Hi, my name is Frank Simorjay, I am a product manager for Solutions Accelerator for Microsoft.

Richard Campbell: Dan?

Dan Griffin: Hi, I'm Dan Griffin, I'm a software security consultant based on Seattle and a former Microsoft employee.

Richard Campbell: Ah, so you're recovering?

Dan Griffin: Recovering would be a good word for it, yes.

Richard Campbell: So we're talking about Forefront and NAP together somehow?

Frank Simorjay: Right, right so one of the integration elements that we we're approached from the Forefront Team was this whole idea of bringing

the Forefront client security, the client element associated to Forefront and integrating it with the NAP (Network Access Protection) capabilities to actually allow network access protection to, so called, monitor the health or health state of a client.

Richard Campbell: So, for me, NAP has always been that very cool technology that allowed laptops and stuff to plug in and they would, essentially be rated as to how much access that they have in the network by how secured they were. I know there's more to it than that but is that really the foundation we're talking here?

Frank Simorjay: Well, rated, I'd caution you though, the word rated, it really is a health state monitoring.

Richard Campbell: Okay.

Frank Simorjay: The idea is to allow for clients to be basically self-reliant on a network, I mean that's the whole premise behind Network Access Protection, it's not really a server based control, the client actually ends up owning the health, its own health, the idea is that it actually will remediate itself. Also, it's a relatively simple process to take a machine and knock it off your network, put it into quarantine, that's simplistic, what's much more complicated is to actually go in and restore or repair whatever was changed.

Greg Hughes: Fix the problem rather than quarantine.

Frank Simorjay: The fix, that's exactly it and what we wanted to do is to provide that capability for Forefront Client Security particularly and actually help it heal itself, to actually fix potential breakages to Forefront Client Security. Dan was actually my lead Dev on this project, he did all of the actual code work associated with those projects.

Richard Campbell: Okay and then I get the idea that it's not hard for NAP to say, "You don't have the Service Packs in or you're misbehaving in some way so I'm going to essentially protect the network from you by not giving you an IP that accesses anything."

Frank Simorjay: By quarantining you, sure, sure and I think that the enforcement methods kind of play a role in this. Network Access Protection like to look at 802.11 access, one of methods and IPsec is one other leading method for security

Richard Campbell: Okay.

Frank Simorjay: Keep in mind that this is a compliant solution not a security solution.



Richard Campbell: Right.

Frank Simorjay: There are ways to subvert NAP that's not its purpose. The purpose is to really keep the honest players honest.

Richard Campbell: Yeah.

Frank Simorjay: There are some mechanisms that are built in and in the future, you are going to see Network Access Protection move more into a true security solution but right now it's addressing health compliance.

Richard Campbell: It's not really aimed at the black hat, it's aimed at the Hatless, the non, somebody who's not knowledgeable, who may have, he's taken his machine home and something's bad has happened to it and now he's brought it back to the office and how does he get healthy again?

Frank Simorjay: Well, the scenario that I'll going to be talking about this Friday in my session is this whole idea of a travelling laptop that goes overseas, he picks up a virus, the virus, there are now viruses in the wild proliferating that disable any virus solution or replace DAT files, they deliberately move the protection to avert itself, right. I mean you've got a virus in the machine that wants to protect itself, so it disables any virus solution. With this mobile laptop, now as it comes back to the corporation, our Network Access Protection layer will actually assist in verifying that that Forefront is running, it's enabled, it can start on time and that all, it's actually in its current version and any malware signatures are up to date.

Greg Hughes: So it might be worthwhile, I think, to stop for a second and talk about what is a Solution Accelerator in Microsoft. You hear this term a lot.

Frank Simorjay: Sure.

Greg Hughes: Why don't you just explain that so people could...

Frank Simorjay: So Solution Accelerators from Microsoft, we're a team that addresses, we bridge the gap between products. Our teams focus is to really assist every single IT pro to be able to faster and quickly adopt our solutions. I think the best way to look at it is, maybe look at some of our other solutions that have come out in the past for a while, Security Guides, if you've heard of the Vista Security Guide, if you've heard 2008 Security Guide, the XP Security Guide, those are all Solution Accelerators.

Richard Campbell: Sure.

Frank Simorjay: MOF is a Solution Accelerator, Microsoft Operations Framework, in fact we just came out with version 4. MAP, which is the Microsoft Assessment and Planning guide, planning tool that actually is also a solution accelerator and we also have a lot of content virtualization, for instance.

Greg Hughes: So some solution accelerators are documents?

Frank Simorjay: Some are documents and some are tools. What we try to do is try to address that immediate need associated with a particular gap missing in one of our solutions, in one of our products.

Greg Hughes: So it's the glue that you might stick between two solutions or that you might use to add on to an existing solution to help solve a common problem.

Frank Simorjay: Correct, right. We are always trying to make it so, the best way to look at it, I always thought the closest analogy is we are a free solution that you can download, anybody can download that would be the equivalent of having to hire a consultant to actually bridge these solution problem spaces. What we do is we provide this for free. We work with our customers very closely, we always solicit feedback to understand what some of the pains are and then we take those pains and try to realize them in either guidance or in a toolkit.

Greg Hughes: So let's talk about this particular solution accelerator, what makes it up and what kind of work went into and what does it exactly do.

Frank Simorjay: Certainly. So I'll let Dan actually take this part.

Dan Griffin: Just to segue in here, I think the Forefront NAP solution is an excellent example of the value that the Solution Accelerator Team can deliver because those components that make up the Forefront NAP solution would require a developer; they would require an organization to have a technical developer or a consultant to implement those things. Relatively complex, even though the solution itself doesn't really do anything very complex. Just kind of that you're talking about, writing some C, writing some C++, that's the kind of thing that your average customer probably doesn't really want to spend a lot of money on, right?

Greg Hughes: Right.

Dan Griffin: It's something that Microsoft is very good at delivering but its features, that cohesion didn't exist in those products as it was.



Frank Simorjay: And it's logical to make those two things operate with each other, right?

Dan Griffin: Completely, completely. There are two components in the Forefront NAP solution; the client is called a System Health Agent.

Greg Hughes: Okay.

Dan Griffin: And the server is called a System Health Validator, those are basically two COMs, two COM components written in C++.

Greg Hughes: So those plug in to the existing products and allow them to interoperate and communicate with each other?

Dan Griffin: Yes and so the way these things tie together, that's exactly right. The way these things tie together is that on the client, your System Health Agent is a plug in to the NAP agent which runs in Vista and also runs in XP SP3 and actually now, also runs on Server 2008.

Frank Simorjay: That's important to point out, that's 2008 Server 2008 as a client. Up until now, most people tend to address 2008 as a server but if you actually were to look at 2008 as a client which some of our IT pros use Server products on their own devices, RSHA is one of the first, actually it is the only SHA available on the market right now that actually addresses antivirus, antimalware solution protection because the Windows SHA, in fact, actually can't do the capabilities that we introduced.

Richard Campbell: Okay. So the client fires up, the NAP client is really the host, so pretty much, as soon as start up NAP fires up, it starts the DHCP doesn't it?

Frank Simorjay: The enforcement mecha -- so let's focus. Let's say for instance at 802.1x, the switch base, it's much more intelligent, it has much more capability because now we're dealing with port level security.

Richard Campbell: Right.

Frank Simorjay: So what you actually see is a NAP agent will actually, on start, as it's trying to acquire an IP address, because it's still going to reach out across the network, it's trying to establish a connection.

Richard Campbell: Yes.

Frank Simorjay: So now we're going to see an 802.1x connection negotiation, at that point, you're actually going to see a request for a statement of health from the client, that statement of health gets

generated by the Network Access Protection Agent. It then calls out our agent to request for Forefront's health which is...

Richard Campbell: So the health of Forefront is part of the overall system health, then exactly?

Dan Griffin: That's right, so you could have multiple, in fact, generally, you would have multiple system health agents running on your client. So the overall client statement of health consists of reports from each one of those client plug-ins, each one of those SHA's pulling whatever that is that they pull on the client. In case of Windows SHA, it's that information that you get from Security Center like is your firewall turned on or off, is your patching, you overall system patching is up to date? In the Forefront case, the Forefront SHA, it's questions like, "Okay, are the Forefront Core Services fully operational and running and set to auto start? Are the Forefront antimalware signatures up to date?"

Greg Hughes: Up to date sure.

Richard Campbell: Do they actually check if they're up to date or not or they just collect what the currently are and then hand them to the server and say, "Are these right?"

Dan Griffin: Ah, great question, there's some technical details in terms of how that is actually implemented and evaluated. Let me try to describe, what's happening there is the Forefront SHA is taking a look at the system registry to determine the last time when Forefront product updates and signature updates were applied.

Greg Hughes: Okay.

Dan Griffin: It's then going to the onsite Windows Update Server, in other words not the update server on the Microsoft Cloud but the onsite Windows update server...

Greg Hughes: The WSUS Server.

Dan Griffin: Thank you, thank you. And determining if newer updates are available. Finally, by policy, you can define how wide that gap can be, in other words, between the time when the last update was applied and when the current updates or when the now update become available, if you exceed that duration, then the response to the server is, "Hey, I'm outside of the duration that you've defined."

Richard Campbell: Yeah, your compliance rules.

Dan Griffin: Yes.



Richard Campbell: So we're just talking about days here that, say, you've got to be within 30 days of up to date or is it a version number?

Dan Griffin: Yeah, hours, Frank was just talking about it, it's actually defined in hours in the policy.

Richard Campbell: Yeah, okay, in hours.

Frank Simorjay: So in fact we can scope it from as little as an hour to several days and it's really entirely up to, again, the architecture of your environment. So if you have a Forefront server already in place, you're going to rely on it managing its updates. NAP will provide, so called, you could say a backup for that update. You do want to rely on that Forefront environment to provide you with everything that it requires, the client requires.

Richard Campbell: But I could also see that if your policy in your system is that your clients must update from your WSUS server and you have guys who are retailing in the field, they are routinely going to be out of compliance.

Frank Simorjay: Right.

Richard Campbell: Which I think is a valuable thing. If out of compliance state is a rarity, it doesn't get tested enough, if it is absolutely normal for a guy who spends a month on the road to come back and is effectively having done nothing wrong and not been attacked in any way, he's already out of compliance and so recovery to compliance is a routine procedure, it happens every time this guy comes back to the office.

Frank Simorjay: And really, the advantage of the solution, and again NAP as a whole, is the fact that the transaction of going back into compliance is seamless, it's a silent process. The only time the user would realize that something has happening is if there's something that's non-repairable, it's a state where you just cannot get out of but all of those normal states of updating that system, all that stuff is all done behind the scenes so the users experience, and again we're dealing with a lot of people that are consuming this are not going to be tech savvy. They just want to be able to plug in and have access to their network.

Richard Campbell: All right, let's keep running with our scenario then, so our fellow has arrived back in the office, he's fired up his machine, NAP's engaged, was requested for a state of health, has walked through all the SHA's, one of them saved Forefront, for example, has come back, he's out of date on his patches for the antivirus signatures. So then what happens?

Dan Griffin: So then what happens is that statement of health is provided by the NAP agent, goes back on to the wire, is received by your switch and is going to be evaluated by the Network Policy Server, oaky? And the Network Policy Server basically is going to take, is going to break down that statement of health data that it's received from the client and in the example that we're using right now, there are two SHA's running on the client, that means you're going to have two SHV's the server component, running on the NPS, the policy server. Each SHV, evaluates the data generated by its corresponding plug in on the client.

Richard Campbell: Right.

Dan Griffin: So the Forefront SHV knows how to peel apart the data sent by the Forefront SHA, it's going to look, in the example, you just gave, it's going to look in that data and see that the updates are out of policy.

Richard Campbell: Right.

Dan Griffin: And as a result of that it's going to respond to the client and simply say, "Hey, sorry your updates are out of policy, fix it."

Richard Campbell: So let me just point here that the client knew it was out of compliance before it told the server, right? It has gone off and said, "Look, what are the current versions that I need and so forth?"

Frank Simorjay: Well, actually the policy is, so the policy configuration is actually done by the health validator. It actually is where the value was set. So let's say, we're saying that the policy is set for 8 hours and then his client comes back, it's clearly outside the bounds of 8 hours, at that point the message is actually sent back to that client, the client then, now at this point, the client realizes that it's out of compliance.

Richard Campbell: Okay, so the client never, the main thing is the set of rules is never set.

Frank Simorjay: No, no, no, no.

Richard Campbell: It didn't know if it was set to 10 minutes or 1 hour or 20 hours, it's just told, you're out of compliance.

Frank Simorjay: Right, right. So when the statement of health was sent up, it's just a package, it's just sends up, "Here's how I am." It's when it gets validated is where the policy criteria is checked and the response is now sent back to the client and says, "Hey, you know what, you didn't meet the policy."



Greg Hughes: So what I'm hearing so far is at the time that I do a 802.1x authentication, I'm getting an IP at that authentication point, what happens if somebody switches, goes in and manually tries to switch off software after they've already gone through the 802.1x authentication, etc. etc., is there a real time component to this?

Frank Simorjay: Right, so a couple of things is this coming back is, it doesn't prevent black hats from bypassing. I mean, there are things like, for instance, if you know how to do it, you could probably craft your statement of health, totally bypass the system. It still won't give you an authentication package, I mean that's one of the key things here is that you can actually use a combination of 802.1x and IPsec and RSHA has actually a, you could say, a state where we call it, I believe, basically, a panic security state where what it does, on boot it absolutely has to have a valid statement of health.

Greg Hughes: Right.

Frank Simorjay: So for client experience purposes, that statement of health is actually cached on the client. So let's say you disable the whole system right after you've been validated, well hey, you're healthy.

Greg Hughes: Right.

Frank Simorjay: The point is, is that you've met the primary criteria, you are healthy. You can then, at that point, do some mucking with the system, for instance, but in reality if you do have security mindedness in play, the goal is you're going to have any 802.1x switch now your port is secure, IPsec which gives you the server side security, the minute that anything is changed, NAP is disabled or the NAP agent is disabled, all of a sudden you become a blank state on the network, it's up to the IPsec certificate to expire, the minute it expires...

Greg Hughes: Gotcha.

Frank Simorjay: All of a sudden you're off the network.

Greg Hughes: Right.

Richard Campbell: Yeah and no way to get back on until you go back into compliance?

Frank Simorjay: And no way until you go back into compliance.

Richard Campbell: So the tricky part to me now is this point of, I have now been notified I'm out of compliance and now I have to figure out how to I get

into compliance. Obviously, we're sort of wandered towards this, "I need to go get an update for Forefront."

Frank Simorjay: Right.

Richard Campbell: But how does the client know that that's what it's supposed to do when it's out of compliance state.

Frank Simorjay: So all of that stuff, our agent, all of that stuff already is predetermined and built it.

Richard Campbell: Right.

Frank Simorjay: What we do is we call out for the Windows Update server and again, if the patch is there we'll install it. So it's a transparent process.

Richard Campbell: But this installation is occurring after the whole SHV process. So it's not like you're just going to go patch up and then go ask?

Frank Simorjay: No, you're right, you're right, the key here is that it's going to go reach out, once it knows what the policy set is.

Richard Campbell: Right.

Frank Simorjay: So it needs to know if you allow for maybe three days worth of software updates to be out of date.

Richard Campbell: Right.

Frank Simorjay: Especially, for instance, when you look at Forefront client security and if there was major upgrade or a .release to the product, that upgrade the download of of WSUS server could be a time consuming process.

Richard Campbell: Sure.

Frank Simorjay: Especially in a large network. So you may actually be a little bit more relaxed. Allow maybe one or two days before...

Richard Campbell: And this comes back to our sales guy who just got back into the office, he's got to do his email and we're going to tie up his machine for X many minutes while he updates a bunch of stuff. The ability to be flexible on those policies so that he has a choice of when that happens is interesting, I don't know how easy is that going to be though.

Frank Simorjay: Well, it's a fine line between creating an available system and a secure system and/or a compliant system and that's the key here, to really and our guidance is associated on how to set



this up, really focuses on that fine line is that what you should consider during this configuration.

Richard Campbell: Right. I mean it's also a management of expectations here, this sales guy is going to get used to the fact that, "When I get back to the office, I plug my machine in, power it up and go get a coffee." There are some things that have to happen and I've been out for a month and probably the longer I've been out the longer it's going to take to get into compliance.

Frank Simorjay: Right, that's no different from getting your updates to your system.

Richard Campbell: Absolutely.

Frank Simorjay: Most people now are very cognizant that if you were off the network for an extended period of time, you're probably going to be getting, receiving updates to your system.

Richard Campbell: An extended period of updates.

Frank Simorjay: Not only that, you may actually have to reboot, we don't even require a reboot for any of our updates.

Richard Campbell: For Forefront updates?

Frank Simorjay: Forefront or the signature updates.

Richard Campbell: Right.

Frank Simorjay: So we can upgrade the product, we can upgrade the signatures and we can also make sure that the product is running entirely without having to require a reboot.

Richard Campbell: But the bottom line here maybe is that you have policies in place that require another product that's on the box to be up to date as well and that's part of the agent process to check in and now you do require a reboot.

Frank Simorjay: That's correct. Maybe entirely true, that's not something that our agent addresses.

Richard Campbell: You don't actually have control of that either.

Dan Griffin: Just one comment, NAP is not a software deployment solution.

Richard Campbell: Right.

Dan Griffin: And we've had some other questions about that over the course of the project and I think it's important to note that that is a good

edge case that you're bringing up where the IT Administrator just needs to be aware if a NAP solution is in place where there is the option for bringing down WSUS updates. It's important to be aware about the status of your travelling workstations, let's say.

Richard Campbell: Yes.

Dan Griffin: You know, is there an opportunity where someone needs to go to the Windows Update Microsoft Cloud to download an update but they'll get slammed when NAP tries to pull something down. Is there a local WSUS server available on the perimeter?

Richard Campbell: Right.

Dan Griffin: In other words, that's in front of NAP that we can hit? Rather than bottlenecking the Network Policy Server.

Richard Campbell: Yeah, we're trying to minimize the slam when the guy gets back to the office.

Frank Simorjay: And Configuration Management Team is actually coming out with an agent that I think they'll be announcing shortly I believe that it's available on a beta state at this point. So software distribution is something that can actually be addressed and NAP will assist you in that process.

Richard Campbell: Yeah but NAP's job is not to do the distribution, NAP's purely to notify the here's where you're out.

Frank Simorjay: No, no. It's all about compliance.

Richard Campbell: But I'm also interested in degrees of compliance, too. To me what appeals in NAP is that, at the minimum it lets you get an IP to get you out on the internet but it won't let you into my servers.

Frank Simorjay: That's correct, that's correct.

Richard Campbell: But I also like the fact that I might have an intermediary stage that, "Okay, you're in good enough state now that I'll give you access to your file shares but you still can't get into the primary apps."

Frank Simorjay: By default, Network Access Solution doesn't quite do that but it has the capability through utilizing different technologies, combining the technologies.

Richard Campbell: To be able to do some tuning...



Frank Simorjay: Right, right, the key here is you can actually have several deployments of Network Access Protection based on the gradations that you're talking about and that'll provide you with different levels of access to different segments of your network, for instance, based on your certificate again.

Richard Campbell: Well, now I'm thinking in terms of at enterprise coping with these new generations of stealthy viruses that are breaking our antivirus protection in such a way that they just report positives, clean all the time and it's a lie. It's not that I expect you all to recover from that I'm just happy you detected it effectively.

Frank Simorjay: Right and it's worth noting too that Sterling will actually be addressing Network Access Protection much more extensive process in addressing a lot of those concerns that you were talking about, is actually capture and identify stealthy viruses and utilizing NAP to again use compliance to protect those clients from...

Richard Campbell: Find a way to fight back.

Frank Simorjay: Precisely.

Richard Campbell: Sterling is the code name for?

Frank Simorjay: Sterling is the next version of Forefront, the Forefront environment.

Richard Campbell: Okay.

Frank Simorjay: It is also one of those big things that's coming down the pipe I believe in the next, you know I'm not too sure, I think it's second half of next year, I believe.

Richard Campbell: Okay.

Frank Simorjay: I think is the general announcement.

Richard Campbell: But it is, so now our poor sales guy has picked up one of these nasty viruses, he's going to go into NAP and NAP's not going to be able to recover for him but now he knows, it's time to call in the IT folks, we've got ourselves a badly broken machine.

Frank Simorjay: That's correct. That's precisely it, what our integration will provide you is at least to be able to identify that and you'll see in the future as Sterling evolves and comes out, it'll actually be able to also remediate that behavior.

Richard Campbell: Awesome.

Frank Simorjay: One thing too is planning, so one of the other things that our team Solutions Accelerator, is coming out in the next month or so is a planning guide, and IPB Guide for Network Access Protection. So it'll actually provide you with high level understanding of how to plan and design a good Network Access Protection environment enforcement solution.

Richard Campbell: It's a whole other angle to go in here I thought about it, a typical Microsoft office where we often have guests in and we want to, I mean right now, today, if I go into a Microsoft office or something, their network is totally locked down. As a non-Microsoft employee visiting or we have the MVP's are in for a meeting or something, there's no ability to access the network at all, that's the norm, and it's tightly protected.

Frank Simorjay: Well, so let me give you an example of one of our alliance partners is a university and the way they're using our integration toolkit is in the following manner, is that they basically can take their labs and ensure that any equipment inside their labs has Forefront Client Security running and operational. Anybody can bring in devices that are non-Forefront, don't have Forefront Client Security installed or NAP Security installed, they'll still get access to the internet but not to local resources. So they've actually managed their resource allocation based on the compliance.

Greg Hughes: So assign them to a VLAN that has internet access but not LAN access.

Frank Simorjay: That's correct, that's correct. In this way they can actually, so if a student requires access to lab resources, they have to go through the compliance process of making sure that NAP's installed and Forefront Client Security is installed.

Greg Hughes: It's a great way to do it. It sure beats the heck of putting red LAN cables and blue LAN cables in your conference room and using duct tape to put labels on them.

Frank Simorjay: Don't use the red one because that one would give you corporate access.

Greg Hughes: Yeah and etc., etc. Now in order to take advantage of this, you have to have switches that support 802.1x, right?

Frank Simorjay: Well, most switches today, on the market, 802.1x switches, switches have 802.1x capability. There are two features that are required. Those ones can actually be identified in the NAP guidance. They're relatively and again I don't want to be general that all switches do but most major manufacturers of switches today have that capability already built in or have an ability to download those



feature sets into the switch. I know that again that list is comprehensive on the NAP blog site, for instance, having all the details as to who is in that partnership.

Richard Campbell: Right. So and what's interesting about this is that even at the lowest level of access on NAP, we could make a server available that starts the remediation process to give you higher levels of access. The usual thing about the two network thing or wherein a lock down environment like that where the only way to promote yourself is to engage tech support IT, it actually is a means of automated remediation so our university can have that student come in with the totally unsecured machine and then be able to access a server that is the one that says, "Here's what you've got to do next to work your way through and then make this phone call and get this account." I mean that's very compelling to me.

Frank Simorjay: Right, right. Actually so part of setting up NAP is to actually setup a remediation server which could be just a simple, here's the five steps of what you need to do.

Richard Campbell: Right.

Frank Simorjay: And make sure you're running Vista or XP SP3, if you're running XP, install the XP patch and then your step two is install Forefront and provide all the shares, by the end of the process most basic users will be able to go through this process and actually ensure that they're in place.

Richard Campbell: It gets us out of that zero state.

Frank Simorjay: That's correct, that's correct.

Richard Campbell: Where the first steps aren't so arduous for us that you can't even get started.

Frank Simorjay: It's basically the same behavior you'd expect in hotel type experiences where you plug in and you get the, "Pay \$9.99 to get access to your network."

Richard Campbell: Right.

Frank Simorjay: It's the same behavior you can actually experience with NAP is that it basically points you to the site that says, "You want access to these network, do these stuffs."

Richard Campbell: Right.

Dan Griffin: Just to characterize this conversation as well as the feedback we've been getting about NAP, is generally that it's been raising the bar.

Richard Campbell: Right.

Dan Griffin: So a lot of the customers are coming back and saying, "You know, we're not ready to deploy." And of course, the recommendation is not right out of the gate to deploy enforced quarantine.

Richard Campbell: No.

Dan Griffin: But rather to do the data gathering, do the reporting mode.

Richard Campbell: Let's start seeing how bad our situation is actually out here.

Dan Griffin: And what you learn, not only is how bad your situation is but you start delivering this feedback to the Administrators and the feedback to the users about, "Okay, we're not going to enforce but by the way here are the aspects of compliance."

Richard Campbell: Here's your compliance...

Dan Griffin: The compliance bar gets raised because people respond to that and say, "Oh, I didn't mean to not mean to be compliant, I didn't even know."

Richard Campbell: Yeah, exactly, they're in hat less mode. There's no intent here, they just didn't know.

Dan Griffin: Right.

Richard Campbell: So now we have a notification method to let them know what the state of their machines are.

Dan Griffin: So there's a positive impact on network "health" simply by deploying the system in a non-enforcement mode.

Richard Campbell: Awesome. Gentlemen; any final words before we wrap up?

Frank Simorjay: Well, no, if anybody's interested in any solution accelerators, best way to find us is www.microsoft.com/solutionaccelerators, all in one word.

Greg Hughes: What about finding out information about NAP, specifically?

Frank Simorjay: For NAP, the best place to point you would be to Microsoft.com/NAP.

Dan Griffin: I can be reached at jwsecure.com, that's J-W-S-E-C-U-R-E.



Frank Simorjay and Dan Griffin bring NAP and Forefront Together!
June 25, 2008

Richard Campbell: Excellent, gentlemen, thank you very much for coming on the show and we'll talk to you next week on RunAs Radio.