
# The 4 Phases of the Zero Trust Journey

*featuring Tim Morrow and Matthew Nicolai as Interviewed by Suzanne Miller*

---

*Welcome to the SEI Podcast Series, a production of the Carnegie Mellon University Software Engineering Institute. The SEI is a federally funded research and development center sponsored by the U.S. Department of Defense. A transcript of today's podcast is posted on the SEI website at sei.cmu.edu/podcasts.*

**Suzanne Miller:** Welcome to the SEI Podcast Series. My name is Suzanne Miller, and I am a principal investigator in the SEI Software Solutions Division. Today, I am joined by my colleagues, Tim Morrow and Matthew Nicolai. We are going to talk about the zero trust journey. Tim is a situational awareness manager in the SEI CERT Division, and Matthew is one of our interns working with Tim's team.

Welcome to you both.

**Matthew Nicolai:** Thank you.

**Tim Morrow:** Thank you.

**Suzanne:** When we get started, we like to know a little bit about the people that we are talking to, and, Tim, you have been at the SEI a long while. I'll start with you. Tell us what brought you here and what keeps you here. Matt, you are an intern. We don't often get a chance to interview interns, so talk a little bit more about how did you get this internship? How did you find out about it? And how exciting is it to be here? I am going to start with Tim.

**Tim:** OK, well, thanks so much. I have been here 19 years. I feel very blessed by that. The SEI has been great for me. I have had the opportunity to work in the acquisition area for DoD. I have worked in architecture, software architecture, and now I have moved over into our cybersecurity team. So it is a great place where it got to combine and put the whole package together now because cybersecurity is such a big emphasis. We really appreciate the opportunity to talk about zero trust today. So thank you so, Suz.

**Suzanne:** Sure. Matt, how did you get here?

**Matthew:** Well, I am currently a graduate student studying Information Security Policy and Management [Master of Science in Information Security Policy & Management, (MSISPM)] up here at Carnegie Mellon University. My professional background is in law and federal law enforcement, which kind of touched upon cybersecurity. Last year, I made the executive decision to focus on cybersecurity, like exclusively. So I made the decision to go to graduate school. When I was considering different graduate programs, I realized that cybersecurity moves at a breakneck pace, so I wanted to pick a school that has strong roots in both research and industry so you can kind of stay on top of things.

As a result of that, Carnegie Mellon was my number one choice from day one, and a big reason behind that is because of Carnegie Mellon's historic connection to CERT and the SEI. As we all probably know, CERT is pretty much the birthplace of modern cybersecurity as we know it, and it continues to play a huge role in the industry landscape until this day. It has been an awesome experience so far. I applied to this internship position at CERT about six months ago because I really want to take my classroom skills and kind of put them into action. I ended up joining the CERT Division's Monitoring and Response Directorate. I work under Tim Morrow on the Situational Awareness Team. Since joining CERT, I have learned a profound amount about cybersecurity and the current state of the industry. Our work as of now is heavily focused on zero trust architecture. We try to bridge the gap between government standards and implementation in the real world. It has been a novel and pretty challenging field that I think makes a positive impact across the board, and I am really just grateful to be here.

**Suzanne:** I think you are an example of something that we see a lot in the SEI, somebody who has worked outside— you worked in federal law enforcement—and got to see some aspects of the real world but came back for your graduate work and then these kinds of internships. That pattern is one that we see a lot. We don't see as many people come to the SEI straight out of undergrad school, because you kind of need a little bit of real-world involvement to understand why some of the things we do are important. So welcome, and we are glad you are here.

**Matthew:** Thank you.

**Suzanne:** So, talking about zero trust, no trust at all. We have done some podcasts on this in the past and why it is important, but I think there are audiences that are new to the topic. Could you just give us a little overview of what are we talking about when we are talking about zero trust? Tim, we'll start with you, I guess.

**Tim:** Sure. I think zero trust is really interesting right now. It is a moniker or a name that people are really focused on and gravitated to lately. I think it is all about making sure you know who is

accessing what on your network in a way that you want them to be. I think that is not something novel to people, but I think that when you start as we go through the journey we are going to talk about here. You are going to see there are different aspects about it that people have not thought about in the past. I know Matt is going to elaborate on that a little bit more. So go ahead, Matt.

**Matthew:** Sure. At the core of the topic, the zero-trust architecture, it represents a shift away from the castle and moat style of cybersecurity that has become so prevalent. In a traditional castle and moat style network, your perimeter for the network is the moat that pretty much keeps untrusted bad guys out. When people are inside the castle, they are kind of trusted by default, and they can move around and kind of do their thing relatively freely. So, as the name suggests, in zero trust we are trying to remove that element of implicit trust from the castle model, and we want to constantly verify users' identities and privileges whether they are inside or outside the network. Something that is particularly unique with zero trust architecture is that we have a policy decision point that kind of drives all this decision making. I tried to explain this to my parents in very simple layman's terms, but the best way I can compare it is like a control tower at an airport or perhaps the control tower at a prison, where 24/7 you have a system kind of monitoring and granting access as needed. There are different feed-in points from external threat intelligence and things like that similar to radar or CCTV in a real-world tower that kind of helps to guide decision making about allowing access.

**Suzanne:** OK, so zero trust has lots of technology implications. So when you start talking about continuously verifying (I have talked to other people about this), and one of the things that makes zero trust even possible is the advances we have had in speed, processors, and lots of memory, and all the resources that we have. In the past, you really didn't have a choice to do that continuous monitoring. Now we have this choice, but there is also this big policy aspect of this. There is, as you said, a policy decision point. *How frequently, how often do we look at things?* How much of that is…Are we seeing people being challenged by zero trust because they are not keeping up with technology, and so they can't take advantage. They can't really perform at the speed that zero trust implies? Or is that sort of off the table, and everybody has got enough of everything that that we don't have to worry about that?

**Tim:** I will take the first pass at that. I think it is very challenging when you look at that. If you mention the logging aspect of things, there is so much information being accumulated and collected from whether it's a SIEM (Security Information and Event Management) tool, or trying to get different inputs into a sort of tool, to think about and be able to act on activities that are going on. We are seeing that a lot of times, especially in large organizations, the logging capabilities are stove piped, and so there is not that integrated view. That is one key aspect of zero trust that you need to do is have that integrated logging view. I think the other thing is a misconception about being able to, it's all about purchasing a product here. I think as we talk

about this during our podcast today, the zero-trust journey is not just about buying a product. There are a lot of things that you need to think about, and it is something that you are going to have to keep thinking about for quite a while in the future. So it is an ongoing thing. To me, those are some of the things that I find a little bit challenging. How about, Matt, what are some of the ones that we have talked about?

**Matthew:** Sure. One thing, as we mentioned, systems, technology has advanced an incredible amount over the last several years where processors and resources are now much more capable of constantly operating and making decisions. The flip side of the coin is that networks have become much more complex, and their threat surface is essentially larger. These kind of go hand-in-hand in terms of policy considerations and decision making on where to start and how difficult or costly it might be to migrate to zero trust.

**Suzanne:** OK. Now, in our federal space, we have federal executive orders that require federal agencies to move in this direction. That is one of the reasons that we are having this podcast is because the federal government is trying to figure out how to go about doing this. There is not quite as much pressure on the private sector, other than some sort of leaders that are seeing value in this approach. I think we want to talk about, because this is a relatively young concept—we weren't even talking about this five years ago—there is not as much guidance for either federal agencies or large organizations on enterprise implementation and transformation. So tell us a little bit about this journey, and especially we mentioned, Tim mentioned, you are going to have to buy some products. So we know there are lots of companies out there saying, *Buy this. If you use this, you know, you are going to get to zero trust*. Those of us that have been in the game a while, anything that sounds too easy, usually is too easy, right? It's there's no free lunch. So you two published a blog post recently. You outlined four steps, basically, in a PDCA or—Plan, Do, Check, Act—kind of cycle for the zero trust journey, so let's talk about those steps and how they can help organizations that are embarking on this journey because they've been told to, or they see value in it. So Matt, let's start with you this time.

**Matthew:** Sure, yes. In our zero trust journey, we have four main steps. The first step in our journey is prepare, which is pretty much an organization trying to set the foundation up for their zero-trust transformation. Some common elements of this step would be developing your strategy for migrating to zero trust, identifying your existing infrastructure and resources, working out any budgetary concerns that you might have, as well as creating your roadmap over the short and long-term for actually executing that strategy. Once you meet these responsibilities as an organization, you can move on towards the next step, which we refer to as the plan phase. The plan phase is heavily focused on taking inventories, making sure that you are referencing cybersecurity engineering standards and developing your implementation as well as monitoring subsequent changes you are going to be making to your enterprise. The inventories that we are

going to be doing during this phase should cover your physical and non-physical assets, data flows, as well as any enterprise workflows that you might have within your network.

**Suzanne:** Can I stop you there because what I am hearing and from what I have read, prepare and plan together are really one way to talk about it is understanding what is your risk profile? Because you are going to have to spend some money to do this. Most people aren't going to spend money unless they see some reason, big benefit, or big mitigation of risk. Is that a good read of sort of what those two steps are all about?

**Tim:** Yes, I was going to say that I will pick that one up. Yes, that is. I think that is a big part of the prepare pillar we are talking about is getting that executive endorsement. Doing that, understanding of what you have, where you want to go to that strategy and developing a roadmap that supports the budget you have, I think that is very key, especially for the commercial side of things. Like you mentioned, Suzie, for federal agencies, they have directives, and they don't have a choice. For commercial, it is all about we think that prepare pillar is to be able to put that package together so you can go talk to your chief technology officer, your CISO, your CEO, and convince them that this is something we need to do is to make this change.

**Suzanne:** OK. When we say prepare and plan, it is easy to just think about prepare and plan, right? But the real goal here is to get that executive sponsorship, get everybody to understand. Even in federal agencies, just because I have to do it doesn't mean I have the money to do it. Often what it means is I have got to take something else off the table, and understanding how this risk fits in with my prioritization of my agency's mission is really important if I am going to actually have people actually do the work that is required for this journey. So all right, I interrupted you, Matt. Go ahead and tell us about steps three and four, because it is four steps.

**Matthew:** Yes. The third step, we refer to it as the assess phase. In the assess phase, we look at your maturity of your zero trust transformation as well as identifying any gaps that you might have within your architecture. Kind of building on top of the risk discussion that we just had, in the assess phase, you also want to calculate and mitigate any risks that might impact your transformation effort. Finally, you kind of move towards conducting some small-scale inventory pilots, covering both the assets and various flows that will be moving within your zero trust network. Once this phase is complete, then we can move into the final step, which we focus on implementation. In the implement phase, we are focused on developing policies for zero trust transformation as well as fostering communication between all kinds of stakeholders within your organization. We also focus on deploying the systems actually and operating them as you can probably imagine. On top of that, you want to monitor and measure your network's zero trust behavior to make sure it's functioning properly. Based on what you discover in that element, then you can make changes as they might be necessary.

**Tim:** I think I would like to add on to that is a couple of the things that we stress being important in this journey is those inventories. I think when you listen to commercial products talk about zero trust, they have typically focused on an aspect like identity and access management or the login capability or data or the segmenting of your network. I think the thing that we felt really important in this process is developing these inventories over time, so that you have that very good contextual information concerning who is using what on your network basically. You need to have a better understanding so that you can then assess what you want to move to zero trust, and then do it through a set of pilots. Those are the things that we try to stress. It's a little bit different than what we typically see in the zero trust documentation.

**Suzanne:** So you are not promoting a, *Let's go from 0 to 60 right away*. You are promoting, *Learn about it.* It's an iterative process, right? Learn about it. Make iterative changes and get to a policy that is acceptable and to products that are acceptable for your organization, but realize that through your pilots, you may not have picked the right one the first time. So you are going to have to evolve the approach over time. Especially, I think aren't we in a place right now where the market for the products and processes for this are still kind of in flux? You are not really in a market where there is a clear, O*h, you know, this is the best way for us to implement*, which means we need to be able to have more guidance for people to make selections and understand how their inventories connect to the kinds of products that are available in the marketplace. We are kind of talking about some differences between federal and industry. For our industry listeners, what are some specific issues they are going to have that we might not see in government because the government is told, *You are going to do this, like it or not*? So industry has got some choices, and then sometimes those choices lead us into some different challenges. Why don't you talk about some of those industry-specific challenges you have seen?

**Tim:** Well, I think one is, we have touched on it a bit, is just there is less guidance out there. I can't go to a bookstore and find a book that tells me how do I implement zero trust. They are looking for resources to be able to help them guide what they should be doing, how they should be doing it. I think that is the purpose of our zero trust journey is to provide that guidance because I can go look at SANS or I can go look at Cloud Security Alliance or all these other different organizations, but I'm not going to find a process out there. I think that is a real issue for commercial companies. The other thing we touched on too is that executive endorsement and buy-in. I think that is a challenge, because especially now we are seeing the cost inflation and things. *Can I reuse parts of my existing infrastructure in my network? Is that capability there?* That is where you have to have that good understanding of what your missions are, what you are trying to do with what people, and figure out, *Well, can I just maybe do this functionality in a reduced way or a way that makes sense for us? Look at the risk associated with that, and see, does it make sense for me?* Matt, do you have anything you would like to add in that area?

**Matthew:** Sure. One thing I want to add is that, you know, Tim and I discussed yesterday some of the challenges that we see. One commonality that unfortunately is across the board is money. Whether it is a massive government agency with a billion-dollar budget or, you know, big or small energy company, for example, everyone struggles with money here. Depending on the organization that wants to implement zero trust, it may be easily funded or may be an absolute challenge. I think that when you venture towards private industry and public/private partnerships, such as energy companies or something, these budgetary concerns are a little bit more real, a little bit more severe. There may be more groundwork to make up on their end to get ready for transformation versus the agency. It depends on the agencies. They all have different budgets and levels of preparation, but it might be a little bit more difficult depending on who you are trying to walk through the transformation.

**Suzanne:** Now moving to common aspects and challenges, we have talked about executive-level support. That is one that money and just even will, the organizational will to do things comes from the executive level. What are some other challenges that regardless of your government or industry position, you are likely to run into if you are trying to move people towards a zero trust strategy?

**Tim:** I think one thing is communicating that message to your organization. I think sometimes we get a fear that, *Oh, we are going to put big brother into our system because there is going to be all this monitoring*. *There is going to be automated responses to things*. It's not that idea. I think the thing is to be able to, *From our point of view, I need to be able to have the forensics information to know if an incident happened, what happened? What led up to that? What were the actions?* I think we need to be able to think about what are those inputs that go into this, our policy decision point, that people need to start thinking about. Because a lot of times a real simple example in this area is if a system administrator's logging in from a different country at 2:00 in the morning, that is probably not something you want to do, but that is real simple. I think each organization, they are going to see that they have different instances like that, that are relevant. Maybe it's insider threat considerations, but those are the things that I think every organization as they think about moving to zero trust. What is applicable to them? I think that kind of goes back again to having a very good understanding of what your mission is in the context of what your system is.

**Suzanne:** Yes, and the context of the world, right? I remember, Tim— I don't know if you were here—but I was at the SEI in the time before we had badges. Security was very concerned that it wasn't zero trust, but it was, *There is too much trust*. Anybody can walk in here at any time, and we do have sensitive information of various types. There were several years where there were attempts to sort of get people to adopt badges. The thing that actually was the tipping point was when we had 9/11. Everyone realized badges is not just about keeping the wrong people out. It is

about knowing where everybody is. One of the things people said is if the SEI building had been attacked, we wouldn't know who was in the building to know who we had to go rescue. A lot of these kinds of mechanisms that are used to add security are also very safety related. So understanding if there is somebody that is in another country at 2 a.m., and they are logging in, that is fine if that is where they are and that is where they need to be. But it is also about understanding that we have people all over the place, and we need to understand how to keep them safe as much as it is about how to keep them secure. I see zero trust kind of in that light. It's a different way of trying to make sure that we are staying safe within the boundaries, within the ecosystem that we are trying to operate in. Is that a fair characterization?

**Matthew:** I would say so.

**Tim:** Yes.

**Matthew:** Go ahead, Tim.

**Tim:** No, I was going to refer to you because that is why I have you on the team. I think this is the policy aspect of things. I hope you were going to talk about that a little bit.

**Matthew:** Sure. As we saw, with for example, like with the 9/11 example, you had stuff like HSPD 12 [Homeland Security Presidential Directive 12], coming out requiring PIV [personal identity verification] cards and CAC cards and standardizing it across the federal government and across branches. The big challenge though is getting private organizations to pick up on that as well. They might be lagging behind. They don't have the same level of force pushing them to adopt badging access standards in that same exact way.

**Suzanne:** Well, and badging is…It's an authentication, right? It's an authentication mechanism. With zero trust, we are using different authentication mechanisms that involve a lot of automation and that actually are less intrusive in some ways than some of these external physical kinds of security controls, like the badging. Is that a fair statement?

**Matthew:** I would say so. Then something else is like post-9/11 intelligence sharing became much more of a thing across various federal agencies, so they can make better decisions. The same thing needs to happen here where your policy decision point, it needs all kinds of intelligence feeds to come into it. The more you can provide to it, the better decisions it can make regarding network security as well as enterprise decision making that might result from network security.

**Suzanne:** This area is one that is ripe for machine learning and AI techniques when you talk about essentially data fusion of all these different sources. But I also like to point out that anytime we talk about machine learning, it is machine learning to enable human decision

making. We are not talking about automating the decision process to the point where we eliminate the human factor in decision making, because that is ultimately…We have decisions that are going to enable or disable people from interacting with our systems, and those need to be made by humans that understand our ecosystem, not just by the machines that are giving us a recommendation. Are you connecting yet with the ML community in terms of some of the ways that machine learning can help the zero trust journey? Is that an area of research I have to look forward to from you?

**Tim:** Yes, we are working on that. That is for sure. I think what we are trying to do is get that environment understood, because I think that is the thing that is going to be challenging for us. You are exactly right that yes, all this has to do with AI and ML, and doing that dynamic policy decision point is going to offer a lot of opportunities to people. I know our own AI Division, they are looking forward to providing that content to let them think about how to do some of these things better. I think another thing that we are hoping to do real soon is have a zero trust industry day where we kind of pose questions out there for people. We are going to develop a scenario and we want people to come back with some ideas of, *well, how would they do zero trust*?, and have some areas where they think about, they want to do some research, so we are looking to try to build this. So right now, we are just kind of getting the word out, focusing on the implementation side that things or how to implement and what you need to think about. That is the next big step for us, I think.

**Suzanne:** OK. Well, that means I get to have another podcast opportunity with you, so I will look forward to that.

**Tim:** I am looking forward. Yes, me too. It's always a blast.

**Suzanne:** So, research, we have got this process that is ready to be used within industry and government to help people. We have got some research ideas for the future. Talk for a few minutes about transitions, because that is the real meat of our work is how do we make sure that these good ideas are usable within both industry and government. What are some of the resources? You just mentioned an industry day that is going to be coming up, but what are some other things that people can look at to help them if they decide they want to embark on this journey that we can provide?

**Tim:** Right. Well, I will, and then I will let Matt add on to that. One thing Matt touched on is across this transition, we think it is very important to do assessments, because it is about maturity. I have seen these four different zero trust maturity models, and it is like, *That is fine people tell you the levels, but how do you make that assessment?* So when we talk about a zero trust journey, we talk about how to be able to provide the right artifacts to be able to make that assessment. I think that is something that we need to stress here is to think about, as you do these

things, you need to have that information to provide that evidence to show that you are doing things. To me that is one thing moving forward is putting the information out there of what should be in an assessment. How do you perform that assessment? We have public documents out now [here and here] that talk about the different assessment methods that we recommend, and we are going to be developing new ones that are more tailored to zero trust.

**Suzanne:** OK, so is it fair to say that right now, the assessment industry—I don't know if it is an industry—but assessment has zero trust as an element of typical security assessments, but a zero trust-centric assessment is not really globally available yet? Is that a fair statement?

**Tim:** That is right. Like in the federal space, they have the high-value asset assessment is one that I know we work on and do, and people have an idea in that. But I have not found— maybe you have, Matt—that I don't think we have anybody that says, *I can assess you to be at a certain level*. It is not like the CMMC or CMMI like that at this point yet.

**Suzanne:** Matt, do you have anything you would like to add?

**Matthew:** Sure, absolutely. As Tim mentioned, this is very novel space, and there is a lot of work to be done. This can take years, especially depending on the size of the enterprise. This is not an overnight process by any stretch of imagination, and it is sort of like the Wild West still where there are some government standards coming out. There is stuff from NIST, for example, like 800-207, that can be referenced by organizations as a standard as well as in the academic community if you are doing research. You can build off of that, grab certain elements of it and really focus on it, and hopefully, that translates into a product offering that can make everyone's life easier. On top of things like that, CISA [Cybersecurity and Infrastructure Security Agency] has their Zero Trust Maturity Model, where, again, it is not this perfect rubric for assessing every single organization. There are still significant amounts of leeway and internal decision making that has to go into seeing where an organization stands. We are going to see, I think, a lot more emphasis within this field over the next coming years. It is going to require government action, private sector efforts, and collaboration with academia to make it all happen smoothly and quickly.

**Suzanne:** Smoothly and quickly are good goals. Having worked in some other maturity model arenas, I know that smoothly and quickly are good aspirations. I will put it that way. But you guys are working on things that are foundational to that. What I am appreciating is you are looking beyond the maturity model construct to what does it take for us to actually improve an organization's position in terms of this kind of strategy. At the end of the day, that is the action you need. It doesn't matter what your number is or what your risk factors are. It's what are you doing about it and giving us this kind of guidance. I thank you both, and I know you have got other members on your team that work this too, for taking that. The implementation step is never

easy on any of these things. You have got all these grand ideas, and when the rubber meets the road is when you really find out where all the challenges are that are going to make it not as smooth and not as fast. I want to thank both of you for talking with us today. As I said, as we said throughout the podcast, there are many resources for this. We will include links to the ones we have talked about, as well as some others in the transcript that we build for the podcast. I want to remind our audience that our podcasts are available almost everywhere: SoundCloud, Stitcher, Apple Podcasts, Google Podcasts, and of course, my favorite the SEI YouTube channel.

If you like what you hear and see today, feel free to give us a thumbs up just like you do all the other videos that you like. I want to thank everyone for joining us. Thank you, Matt, especially for coming in and being an intern with us. I know it is challenging to disrupt your life when you are in grad school with this job kind of thing and everything, but we do appreciate your work, and of course, Tim, always a pleasure. I look forward to the next time we get to talk.

**Matthew:** Thank you for having me.

**Tim:** Thank you, Suzie.

*Thanks for joining us. This episode is available where you download podcasts, including SoundCloud, Stitcher, TuneIn Radio, Google Podcasts, and Apple Podcasts. It is also available on the SEI website at sei.cmu.edu/podcasts and the SEI's YouTube channel. This copyrighted work is made available through the Software Engineering Institute, a federally-funded research and development center sponsored by the U.S. Department of Defense. For more information about the SEI and this work, please visit www.sei.cmu.edu. As always, if you have any questions, please don't hesitate to email us at info@sei.cmu.edu. Thank you.*