ZTA's Not A Thing, Not A Widget, ZTA Is A Framework…

Use NIST SP 800-207 as your guiding North Star to implement your own Zero Trust Architecture (ZTA) capability within your own environment.

By **Luke McCormack**
CIO (Retired)
Department of Homeland Security (DHS)

The most important element of Zero Trust is architecture. It's important to say Zero Trust Architecture – it's not a thing, it's not a widget, it's a framework.

ZTA is an architecture that allows you to trust nothing and assume that somewhere inside your network apparatus you have been compromised. You always have to assume that there is no implicit trust granted to anyone under any circumstances; and you need to continue validate that and re-validate that.

In layman's terms: While I am granting you authority to come into my environment and get access to X, Y or Z, the next time you come in I don't just say "hey there you are" and let you in and again give you access to various pieces of information. I am validating you are the "approved person", but I am also validating that the approved person still has the authority to the information and I am doing that in real time, all the time.

ZTA – Where To Start?

I think that is very important to put together a structure, an architecture that allows for that capability. That's not a simple thing to do. You don't buy a box, a piece of software and implement it into your environment and all of a sudden you have this capability. There's a lot of pieces and parts that have to come together to adhere to this architecture to allow those types of things to happen, do it in a real time basis and do it with a level of maturity that you are looking for.

I think a lot of the CIOs struggle with "where do I start"? First you have to baseline your environment and based on that you can understand where you are at, what pieces of technology do you have available to begin to have this capability. And you may have to buy some new software and hardware to enable some of this and then you go through a multi-step process to harden the environment and keep it there.

Google has implemented this capability and it took them 7 to 8 years to fully implement this. So even though they had endless engineering and financial resources to make this happen, it took time. But it gives the community a chance to take the lessons learned from them including some of the products to engineer, design, implement and harden and simply reuse that.

So if you look at Google as a company, they went through this Zero Trust Architecture journey over a long period of time. It took them several years to get there but now the community at large can benefit from that capability.

It's a bit of an arms race; you need a constant flow of funds because you need to change the culture; you have to train people; you have to implement and reconfigure constantly pulling out old technology and putting in new technology.

Funding Critical

To guide the community, OMB has given some directions in the May 2021 Executive Order on Cybersecurity that states agencies will put a plan together and then execute on those plans. I also think this will get the funding.

Nine cabinet level agencies were compromised in the Solar Winds attack and all of them are going to get increased funding for cyber to build out their capabilities and harden their environment that is going to be based on this ZTA.

This is a lifestyle culture change. You need upper level management buy-in along with addtional annual funding. This is a down payment and it's not just to buy products and services; this is a plus up to not only start you on this journey but to keep you on the journey in the years ahead.

That way you don't run into technology that will become outdated and you are able to keep up with current technology; there are a lot of bad actors and you are going to need to refresh and update your architecture to stay ahead of and counter them.

End Users Benefit

The end user gets affected in a positive way. No longer will they have to use a VPN. As ZTA gets more mature and implemented, the whole login process becomes a cleaner and more secure experience because it becomes more embedded and fused into this architecture. Users get to enjoy the seamless capabilities that come along with this – less burden and a better experience.

The same thing goes for machine to machine communications. For example, a bank when it doesn't recognize the computer you are on asks for more proof of identity. They can validate the characteristics, elements of the device and if OK, you can go into the environment. Validation of both the person and the device they are using happens at the same time. ■

About The Author

Mr. McCormack is National Director of ACT-IAC. He also serves as the National Director for the U.S. Cyber Challenge.

Mr. McCormack retired as the Chief Information Officer (CIO) at the Department of Homeland Security (DHS), where he provided strategic direction, cyber security services, oversight to cross-component information technology efforts and IT Cloud/infrastructure services. He also served as the Vice Chairman of the Federal CIO Council. Prior to this appointment, he served as the Department of Justice Deputy Assistant Attorney General for Information Resources Management/Chief Information. .