Paul Morris
Chief Information Security Officer (CISO)
Centers for Disease Control (CDC)

The CDC Rolls Up Its Sleeves

The CDC needs to get data to whoever needs it, where they need it. Moving into a multi-cloud environment where identity and access are monitored through Zero Trust principles, the CDC is moving towards an era where data can move securely between clouds.

Progress: Bringing Identity Access Controls Into Next Generation Firewalls

The CISO Council (Chief Information Security Officer) has been working hard. But to get where we're going takes good policy and takes a lot of people rolling up their sleeves.

There's a lot of existing projects in different places in the enterprise under different teams. So, how do you bring them together so that we can start to think about establishing trust in any user, on any device, when accessing data. And bring those together so that a decision can be made at that point in time whether this is an approved connection.

We're taking advantage of Tech 3.0 opportunities that are available to us with a solution that brings cloud access directly down to the user. That's really an opportunity to use SASE technology and really also provide that tech security monitoring capability that is so important.

The upside to our users is we don't have to back all that data back to our data center up through a single TIC from the department which reduces that latency as we're finding ourselves all in multi-cloud environments. Bringing all those things together is a big plus.

Mr. Morris comments are from the Federal Executive Forum on Zero Trust Architecture broadcast on Federal News Network.

We're also working hard right now on bringing identity access controls into our next generation firewalls. We know – based on the attacks, breaches and ransomware attacks – adversaries are coming in at the application and user level.

So we are thinking about how to use name spaces instead of IP addresses for specific users or groups. That's part of the decision policy point of saying "do they really need access to this data?" Along with network segmentation, we're starting to build that architecture and that framework where I think you are going to see results long term of keeping adversaries out of our networks.

Success: People Only Have Privilege For The Job They Are Doing

I would really have to point to our Privileged Access Management (PAM) efforts. These things work when you have people who understand the complexities of what that means. It brings the elements of separation of duties and privilege which are so are so critical in defending against an adversary. Our program has really advanced past just managing an active directory by installing technology so that when we grant access there is a lot of administrative and technical checks along the way. These make sure

that you are granted access to a use case or that you need to have elevated privileges.

So we go through those checks before we grant that. We cycle your credentials – your user name, your password – every time that you use them. We throw them in the trash and then we watch them and make sure those people who are using those elevated privileges are staying where they should be. Are they in the same building that they should be; are they working during the times that they should be; or are they trying to give themselves more privileges?

Those things set off alarm bells that make us all go running and we're constantly looking at Office 365 and Exchange.

So we continue to evolve those capabilities and we're going to continue moving that out to all programs, out to a mobile device and into the cloud. That is so critical for making sure that people only have the privilege they need for the job that they are doing; and then we make sure that doesn't change unless we actually make that change.

Priority: Leverage Zero Trust In A Multi-Cloud Environment

Our number one priority is to support our mission. We are still knee-deep in a response to the pandemic. We've deployed multiple national level critical systems that support the ordering and tracking of vaccines, tracking of testing and then bringing that data from across the nation, whether it's a small public health department at the state level all the way to our data stores. So. how do we quickly make sense of the data?

We're talking about data analytics; we're talking about accessibility and getting that to the people who need it quickly; and making decisions at the national level that go down to the state and local level. So it is a Big Data challenge and an opportunity to add that to what we've also received funds for our specific public health data modernization initiatives, which are allowing us to upgrade legacy systems of data collection supporting all the mission areas of CDC.

We're bringing those to the cloud, we're bringing that data into a data lake and into multiple areas. It gives us an opportunity as we're doing these changes to apply the Zero Trust architectures to the things that we learn. I think the opportunity and priority for us is to make sure that we are leveraging Zero Trust and looking at users as to who has access and then making it easier for our user.

Again we need to get the data to whoever needs it, where they need it. I would say that one of the big things is as we move into these multi-clouds that we can monitor securely and provide access; and we are moving towards an era where we can move data back and forth between clouds, between the premise and the cloud and do that quickly and securely leveraging the technologies that we've talked about by people and applications that are trusted in this framework.

We are moving towards an era where we can move data back and forth between clouds, between the premise and the cloud and do that quickly and securely.

There's a lot of work on policies, but again we need to embrace the future to really take hold of the modernization and innovation that we're undertaking. ■