Executive Viewpoint
A conversation with
JOHN HALE

JOHN HALE
Chief of Cloud Services, Defense Information Systems Agency

This conversation is adapted from a presentation at an FCW event.

From baked-in security to defense in depth

I used to make the statement that I'm not a security expert, but I play one on TV. But I don't do that anymore because in the world of cloud, everybody has to be a security expert.

The Department of Defense has been involved in cloud from the very beginning. We actually kind of created the cloud. We started a project about 55 years ago called ARPANET, which was all about connecting research labs and universities together so they could share compute power and research. ARPANET ultimately became what we call the internet today. And then DOD created our own networks for warfighting purposes.

So cloud computing is in our DNA. When we started sharing compute power early on, security really wasn't a major concern because the networks were closed. They were limited to the academic institutions and the research labs that were connected. And you had to go through a human in order to get jobs run on computers. So security was baked into the system from the very beginning.

As we moved away from that kind of model to client/server and then ultimately springing back into the cloud world, security has gone into what we call the onion layers. You build security in a series of layers to ultimately get to the center of the onion. But once they're in the center, there's really nothing in there to protect you. People are allowed to move around in there as they see fit.

Defense in depth is the model we use for cloud security today. We start with firewalls at the edge and add intrusion-prevention capabilities, intrusion-detection devices, reporting, aggregation of log data, humans who actually review that data and machines that do AI analytics to try to find people who are doing things they shouldn't be doing in the cloud and then take action to stop that from happening.

The rise of zero trust

That defense-in-depth process really has not changed in the last 15 years. And while it was probably good when it started, we're now seeing the problems with that model.

> **The data in the cloud is what's valuable,** and with zero trust, access to that data is not guaranteed at any time.

> **We need to move to a model where security is baked in** from the very beginning and it's ubiquitous.

Once you're inside, that lateral movement from one system to the other all the way down the chain is the scary part. It's almost impossible to catch because the tools we use are designed to protect the onion.

Where we're going and where I see the industry going is zero trust. The data in the cloud is what's valuable, and with zero trust, access to that data is not guaranteed at any time. Many pieces of information have to come together for you to gain access to that data and process it. And that information could be who you are, where you are, what kind of device you're on or what network you're on.

As part of the zero trust model within DOD, we're looking at everything possible to create that authentication signature. Mobile devices are becoming not just a nice-to-have capability for leadership. They're basically becoming a core way of doing business for the warfighter, and everything a mobile device goes through can help generate an authentication decision toward your ability to access, process and manage data in the cloud.

The role of weather data in mission success

When we talk about DOD, everybody thinks about the warfighting mission — the soldier on the field, the sailor on the ship or the airman in the plane. But in reality, the department has a lot of structure behind it in order to make that mission happen, and it used to be that something like the weather was not even listed as a critical system. Well, you can't fight a war if you don't know what the weather's going to be.

The Air Force's weather organization processes and distributes more data in a day than the entire Department of Defense did in a year 10 years ago. And anybody who's a history buff knows the weather people actually decided when D-Day was going to occur, not the senior leadership. D-Day was supposed to occur two days before it actually did, but the weather team said, "It's going to be horrible. It's going to be a disaster." And they convinced leadership to push D-Day back to a point where the weather would be in the right place for the mission to be successful.

Now the weather system processes petabytes and petabytes of information every day from a myriad of commercial and DOD providers that feed information into that system, process it and then distribute the information to their mission partners so they can make tactical decisions about the warfighting mission. And that's all done in the cloud because of the need for compute and storage at a scale that's growing astronomically.

But security has been baked in from the very beginning. And so how particular users of the system gain access, how they process that information and how they ultimately distribute that information toward the decision-making process have all been driven by access-based control capabilities.

The platform of choice for new capabilities

My point is that the missions are pushing toward a zero trust model, and we're really hoping that commercial products catch up and lead us in that direction so that we can continue to push cloud capabilities to enable warfighters to complete their mission. Cloud is not the right fit for every capability, but as we modernize all our warfighting capabilities, ultimately the cloud will become the first platform of choice for every new capability.

Right now we run a couple of thousand applications in a commercial cloud environment, and in a given week, we block about 190,000 benign probes into our capabilities. Those are script kiddies, college kids who are just poking around to see what they can find. Out of that 190,000, there are about 10,000 that we list as serious attacks, where somebody is actually trying to do something malicious in the system. And then out of those 10,000, about 250 attacks a week can be directly attributed to nation-state actors. And that's only with the portion of the workload that DOD has moved to the cloud, which is not the largest portion.

We're using defense-in-depth capabilities the way we would in a traditional data center. For the most part, we have looked at the cloud as just another data center, and we've treated the applications and capabilities that go in there as if they're just going into another data center. That's wrong, but that's the way we've done it to date because that's the mindset and the tool set we have available to us.

We need to move to a model where security is baked in from the very beginning and it's ubiquitous throughout the entire system — and away from this model where once you're inside, you're inside.