accenture

# IRONNET

## VIDEO TRANSCRIPT

While as commander of US Cyber Command, we had the responsibility for defending the nation. One of the issues that I saw in trying to defend the nation was we couldn't see the attack in cyber against our nation. As a consequence, the government's response was always incident response which means after the attack. We wanted to come up with a way of helping see attacks and help companies stop the attacks before something bad happens not after. And so IronNet was created to help fill that void by identifying threats to our nation's critical infrastructure in a way that we could stop an attack beforehand. What that entailed was bringing together companies in terms of collective defense. Seeing events as they happen in real time and sharing that information with the government and private sector. A lot to take on but I think that is the right thing for our nation and other nations.

IronDome is the way we pull together our collective security. What makes it different is that IronDome isn't sharing legacy information or information about known threats. We companies need to share are the unknown threats. And the only way to share unknown threats is by creating a set of behavioral analytics that can pull out event data on threats that we don't know anything about and sharing those quickly. In that way we can combat those who would attack our nation's network in terms of reconnaissance, command and control, actions on the objective, and other forms of the kill-chain in a way that we have never been able to do in the past.

So what we talk about our IronDome is putting all that information into the Dome and now running analytics across those events across many companies to see who is being attacked, in what form, and showing them the multiple attacks that are going on.

When you look at the secret sauce that we have, it's in how we develop our analytics and our Expert Systems. Those two are the foundations for creating collective defense. And without those running right, everything else is worthless. Our ability to prove that with out testing framework, and with these cyber threat emulations is part of that secret sauce and when companies see that, they immediate get it and think "Oh my god, I see this gap. We got to fix that".

Building an international capability like this is the best way to defend individual companies and the collective. The data we get into the IronDome, the better we can defend. So in this way, data is the new oil for cyber security. And the more data we get, the better will defend and the faster this will go.