For the past two, three decades, companies have relied on their network security as one of their primary means of protecting their IT environment. Really, the networks themselves are just avenues of access, or for a hacker, an avenue of attack. The network security situation has changed dramatically over the past decade, with the implementation of wireless networks and mobile devices, and everyone wanting to access data systems applications from wherever they are. It's really increased the complexity of how we can manage the control, the network access control, that we used to take for granted. We are seeing companies continue to increase their adoption of VPN technologies. Again, with the proliferation of mobile devices and mobile users, they need a way to securely connect back into an IT environment. And that really increases the importance of securing those end points, be it an end of mobile device, end-user work station, or a server that may be where they're connecting. It used to be so simple. We could put a firewall in place, we could allow access to the applications our users we wanted to come in through, and deny all. We still can do that, but now we have so many more devices that we have to consider, a wireless access point, you know, we have to make sure that's locked down, because that sits directly inside the environment. And if someone gains access to the wireless network, they may have access to your entire environment, if it's not segmented properly. Today, organizations have to look at how they protect their perimeter, but they also have to look inside their networks.
and consider things like network segmentation or other network controls, firewalls, intrusion detection, intrusion prevention, web filtering, the list goes on of types of different network security controls we can implement. But you cannot just implement a control, you also need to manage that control and monitor it on a 24 by seven basis. IBM Managed Security Services does that today for several thousand clients around the world. We look at over 20,000 devices and nearly 20 billion events a day that we see go across these networks. So, we see all too well that it's not just the network we're protecting, it's all the users, systems, and application that reside on it. Our Intrusion Prevention platform also integrates with our IBM security QRadar platform, to help with intelligent detection and monitoring of those threads as they occur in the environment. When you couple those technologies with our industry-leading Managed Security Services, clients really have a winning approach to trying to get ahead of the hackers and be able to respond quickly to threats as they occur in their environment.