Wednesday, February 13, 2019
11:00 a.m. – 11:20 a.m.
Are You Protecting Machine Identities?

Steve Briley
Federal Solutions Architect
Venafi

Abstract: There are two kinds of actors on every network—people and machines—and both need to be secured. People rely on usernames, passwords, CAC cards, and biometrics; but machines use keys and certificates for machine-to-machine communication and authentication. Billions are spent each year securing identity and access management, but virtually all of it is spent securing human access, almost none on protecting keys and certificates. “Machine” definitions in the traditional sense have exponentially expanded in recent years to now include software that emulates physical devices, algorithms, and microservices such as containerization in addition to the more traditional machine types like servers, clients, mobile and IoT devices. The proliferation and ubiquity of machines is outpacing most agencies’ ability to identify and authenticate them. Nation states and other US adversaries know machine identities are often left unprotected and have become lucrative targets used to eavesdrop on private communications, make phishing sites or malicious code look valid, and hide their nefarious activity in encrypted traffic—getting malware in and sensitive data out. In this presentation, we’ll discuss the different types of machines identities and where they proliferate in your network. You’ll see the role and lifecycle of machine identities, and where we’re falling short in protecting them. We’ll then look at where there are current risks today as well as where new risks are emerging. We’ll conclude with steps you can take immediately to get these risks under control.