Lifting and Shifting Yesterday's Cybersecurity into the Cloud is Tomorrow's Adversary Attack Vector

Russ Smith
Technical Director, Strategic Response Group
ZScaler

This presentation includes an interactive demo to describe the core elements necessary to achieve a zero-trust architecture, and how those core composable elements protect joint and coalition military operations.

The Department of Defense is leveraging Cloud Service Providers (CSP) to embrace the "perimeterless" cybersecurity of a zero-trust architecture. Modern zero-trust architectures must be designed, deployed and operated in a manner that keeps pace with the ever-changing threat landscape. Security offerings face the perils of keeping pace with the threat or perishing as a viable solution. The composable architecture of the CSPs allows for flexibility and rapid innovation.

The stakes are even higher when lifting and shifting traditional perimeter-based security approaches into the cloud. Legacy security is typically tightly integrated and monolithic; therefore, a lift-and-shift approach is often the only option. Failing to adequately secure cloud-based infrastructure exposes organizations to data loss, denial of service, and potential mission failure.

A new approach that focuses on securely connecting any user, device, applications, or data to any cloud-based resource, and in contested environments is needed. The interactive portion of the presentation will include four use-case based scenarios:
1. A zero day will wreck your day: this demonstration shows how zero trust principles allow for continuing cyber operations while under attack in a contested environment.
2. Network security is easy when users and applications are not on the network: this demo demonstrates the value of moving from a network-centric security model to an operator-centric security model. This approach allows for the multiple coalition and joint networks to just provide transport but are not the foundation for cybersecurity.
3. Privilege Remote Access for Dummies: this demo demonstrates how elevated privileges can be granted and managed in a way that does not result in losing access to critical infrastructure.
4. The adversary will not wait for us to build a coalition network: the final demonstration shows the value in implementing zero trust principles to make access to coalition data by connecting coalition partners, not by building a coalition network.