swish FORESCOUT

Case Study

Swish and ECS Federal Provide the United States Marine Corps with a Zero Trust Architecture for Comply-to-Connect Across Primary Classified and Unclassified Networks

Introduction

The United States Marine Corps (USMC) is the maritime land force branch of the U.S. armed forces, responsible for both land and amphibious operations worldwide. The Marines support three primary areas of responsibility: seizure or defense of naval bases and other land operations that support naval campaigns; development of tactics, techniques, and equipment used by amphibious landing forces in coordination with the Army and Air Force; and other duties as directed by the President or DoD.

Zero Trust is the concept of restricting access to resources by authorizing user-resource connection requests at the most granular level possible. "Comply to Connect" (C2C) is an extensive cybersecurity framework of solutions designed to address uncertainty as it pertains to cyber readiness to meet DoD mission challenges and secure DoD networks against adversarial attacks. DoD networks make up the core of the command-and-control infrastructure that provide our military access to mission-critical services and information needed to keep our nation safe. C2C leverages Zero Trust's least privilege principles to protect resources and assets by evaluating and possibly remediating the security posture of every endpoint before granting access to a network.

The Problem

USMC needed to comply with the Jan 28, 2021, DoD CIO Memorandum Section 1653 for Comply-to-Connect for all new and existing hardware and software deployed on the Marine Corps Enterprise Networks, Unclassified (MCEN-N) and Classified (MCEN-S); the Marine Corps Recruiting Command (MCRC) network; and the Marine Corps Community Services (MCCS) network. The objective was to instantiate a C2C model including both pre- and post-authentication checks on all internet protocol-enabled endpoints that are connected to or receive services through a USMC network. The Marines sought compliance with the highest security standards and the ability to achieve and maintain "Authority to Operate" (ATO) on all systems.

"Given what I know today about the contractor's (Swish's) ability to perform in accordance with the contract's most significant requirements, I would recommend them for similar requirements in the future."

Service Owner, Cyber Threat and Vulnerability Management, USMC

The Solution

Using CounterACT, Forescout's network access control (NAC) cybersecurity solution, Swish and ECS Federal designed a C2C standard reference architecture for the USMC networks and then implemented it as consistently as possible on the MCEN-N, MCEN-S, MCRC, and MCCS networks making slight adjustments to accommodate for differences across those networks. Swish's deep expertise in Zero Trust Architecture (ZTA) and experience in tool integration were key to USMC selecting them for the job. The contract scope also included full ISSO services to achieve and maintain ATOs on all systems. Swish was able to leverage USMC's existing tools on the MCEN providing automated compliance, control, and remediation of managed end-user devices.

Swish believes that customer collaboration is critical to solution sustainment and delivery. They engage with all key stakeholders at every stage of the process to enhance collaboration between the system end users, agency managers, and deployment teams. Their cross-functional deployment teams collaborate with the Program Officer during regularly scheduled meetings and align with MCEN, MCRC, MCCS, Enterprise Engineering & Verification Environment (EEVE), logistics, cybersecurity, lead engineers, test engineers, administrators, and configuration management teams throughout the system deployment life cycle. Swish completed and continues to maintain all training requirements for USMC's accounts on government-designated ticketing systems and repositories used in each C2C management domain.

Results

Swish achieved 802.1x implementation across MCEN, MCRC, and MCCS and executed 802.1x enforcement, becoming the most mature implementation of C2C across the DoD services. IEEE 802.1x is a network authentication protocol that opens ports for network access when an organization authorizes a user's identity and access privilege.

Summary

With hundreds of networks, each having thousands of connected devices and systems, C2C is a critical cybersecurity control for USMC. Engaging Swish and ECS Federal services with Forescout solutions, USMC was able to achieve the most mature implementation of C2C across the DoD. Swish provided support in all areas including system administrator support, cybersecurity support, engineering documentation, and engineering reviews and meetings.

About Swish

Swish is a provider of technology solutions and engineering services to the U.S. Federal Government with a focus on high-quality outcomes for customers. Since 2006, Swish has delivered high-performance solutions and services to the Federal Government market ensuring that customer's digital service capabilities, performance, and security exceed expectations and requirements. Swish is a Service-Disabled, Veteran-Owned and HUBZone certified Small Business.

To learn more, please visit:
www.swishdata.com

1420 Spring Hill Road Suite 320
McLean, VA 22102

P 888.460.0275 / E info@Swish.com

swish