U.S. Air Force Protects Voice Network and Call Activity with SecureLogix

Privacy & Information Theft

Robocalls & Spam

Spoofing & Impersonation

TDoS

Unauthorized Access

Challenge

The U.S. Air Force (USAF) needed an integrated solution to manage authorized access to its voice network resources and strengthen overall voice and data network protection for its entire defense installation infrastructure.

The USAF employs over 150,000 civilian personnel and more than 425,000 active-duty members, not including contractors, National Guard, and Air Force Reserve service members. One of the world's largest operators of military bases, the USAF has 59 bases in the U.S. and 23 bases in countries across three continents and 89 Air National Guard units.

Locations such as Elgin Air Force Base (AFB) received large numbers of spoofed calls in which the caller deliberately sends false Caller ID information to mislead recipients. Upon answering, the fraudster would either try to sell something or attempt to gain unauthorized information via social engineering attempts.

The volume of robocalls was impacting the USAF's operational effectiveness. For example, Wright Patterson AFB was receiving an overwhelming 80,000 spoofed robocalls a month. At Elmendorf AFB, a Telephone Denial of Service (TDoS) attack took down phone systems and services with high volumes of unauthorized / malicious inbound calls.

Another issue that has become a top priority for the Department of Defense (DoD) is the mitigation of the insider threat to DoD information systems via phone / call activity and access. The "insider" is anyone who is or has been authorized access to a DoD information system, whether a military member, a DoD civilian employee, or employee of another Federal agency or the private sector. The USAF has a Cyber Defense mission to monitor, collect and analyze phone calls traversing through their network for adversary collection and exploitation of sensitive information.

The USAF needed an integrated platform that would not only reduce the spoofing and robocalls but would guard against all other types of threats, including malicious activity from undetected insiders with access. The USAF had an urgent need to harden the voice / call portions of their digital communications perimeter, provide organizational-wide visibility and security control over all inbound and outbound call activity, and record encrypted phone calls for operational security.

Approach

The SecureLogix® Call Defense™ System provides a voice firewall, voice intrusion prevention, analytic reporting, and call recording solution. It secures enterprise voice networks from unauthorized access, malicious calls, TDoS attacks, toll fraud, call pumping and other threats.

SecureLogix is also effective at reducing robocalls, spoofed and harassing phone calls, and voice spam, blocking on average 20,000 spoofed calls coming into Elgin AFB every month.

The USAF also strengthened its security perimeter and risks associated with call related insider threats. With SecureLogix, the AF can monitor and record incoming and outgoing calls, on and off-base, and monitor for sensitive information being improperly disclosed.

Result

SecureLogix blocks over 2.1M fraudulent calls annually for the USAF and records encrypted and unencrypted calls for enterprise operational security. Having an efficient and secure information enterprise is part of the USAF's overall Digital Air Force strategy. SecureLogix voice security services continue to adapt to emerging, complex threats based on the most current intelligence to provide the USAF better security and the ability to mitigate external and insider threats.

Solution

CALL DEFENSE™
system

"SecureLogix empowers us to secure our mission critical voice network infrastructure and services.

Former Deputy Chief of Staff for Communications and Information, and Deputy Chief Information Officer, Headquarters U.S. Air Force, Washington, D.C.

SecureLogix®

https://securelogix.com