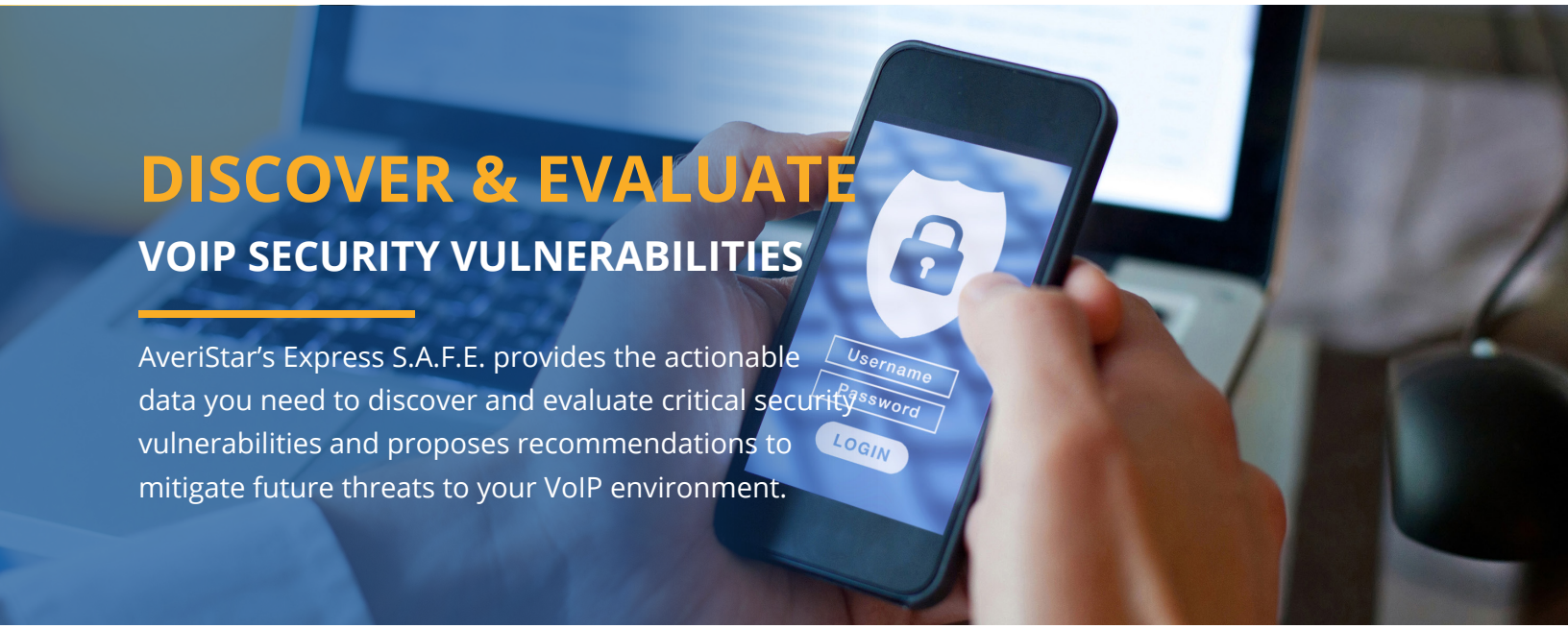
AveriStar

EXPRESS S.A.F.E.



DISCOVER & EVALUATE

VOIP SECURITY VULNERABILITIES

AveriStar's Express S.A.F.E. provides the actionable data you need to discover and evaluate critical security vulnerabilities and proposes recommendations to mitigate future threats to your VoIP environment.

KEY BENEFITS

- **Actionable Data & Reporting**
  Detailed security information allows organizations to make informed decisions based on the needs and requirements of the business.
- **Increased Security Posture**
  By evaluating the infrastructure of VoIP networks, corporations can strengthen their security posture and decrease the risk of a security breach.
- **Overall Reliablity & Piece of Mind**
  Security & Fraud Evaluation increases system uptime, greatly reducing costly downtime, loss of data, revenue, and productivity.

OVERVIEW

As with all network or web applications, cyber criminals will consistently attempt to exploit system weaknesses. Voice over IP (VoIP) is no exception. Because VoIP and data run over the same network, there are more ways for hackers to compromise a VoIP system than a PBX or traditional phone system.

The security level of VoIP is particularly essential, since malicious attacks can lead to the major disruption of your communications system and cause substantial financial loses. An attacker can ultilize features such as ID spoofing to bypass access control lists or firewalls, as well as obscure their real identity (caller ID) or location. Voice phishing is used to gain access to personal and financial information (credit card numbers or identity theft schemes) from the public for the purpose of financial reward. With VoIP Spam or "SPIT", unsolicited calls can be initiated in bulk. Spammers attempt to launch a voice session and then relay a pre-recorded message if the receiver answers (i.e., robocalls). Robocalls can be delivered automatically using telephony software such as Asterisk call files. And, DDOS attacks can shut down the phone system by generating thousands of incoming phone calls simultaneously. Primitive thinking, but effective.

What was once a minor threat has become a malicious tool for money-hungry hackers and a potentially catastrophic tool for state sponsored cyber terrorist organizations. In short, VoIP attacks are on the rise and with AveriStar's Express S.A.F.E. (Security & Fraud Evaluation) you can stop the attacks before they even begin.

Express S.A.F.E. Features

Security Audit & Threat Assessment

AveriStar will perform an evaluation to determine the susceptibility of your telephony infrastructure to an attack or exploit. Our engineers will scan for vulnerabilities, administer penetration testing, and review configuration settings.

Call Processing Limits Review

Having a proper call processing policy can help reduce the threat from Voice Phishing and SPIT. We'll analyze the call processing policy and ensure the number of concurrent calls and redirections are limited on a PER USER basis.

User Agent Spoofing Protection

Most SIP user agent spoofing is done by cloning the MAC address of the end point and using that to download phone provisioning files, or attempt a Register request. If the MAC address is cloned, the phone will not be able to pull down configuration files without having the correct username and password. Using device management file authentication, we will use encryption to determine that the user at a given phone is who they say they are. Consequently, preventing the hijacking of service in your hosted environment. We'll also check for unique username and password settings for each device provisioned.

DOS and DDOS Prevention

Our engineers will develop an advanced caller identification system for calls placed over the Internet. The number would be verified and authenticated through attached certificates or "secret" signatures. We will also enable software to identify the origin of these calls. If they are an Internet number created solely for a DDOS attack, the software will be able to block the call.

Application Server Security

Web application security is of particular concern because it's used to simultaneously let legitimate users in while keeping suspicious individuals out. We will take the necessary steps to make sure the recommended password and passcode settings are in place.

Communication Barring

Our engineering team can impose restrictions on call type, duration, and time of day, and apply specific actions (block, allow, transfer) to calls that meet certain criteria. Rules can be applied to incoming calls, outgoing calls, or redirects. These restrictions can be activated at the system level or the service provider / enterprise level.

Call Processing Policies

In addition to the system settings, we will review the call processing policies. They can be set to override the system settings at the Service Provider, Enterprise, group and user levels.

To learn more about Express S.A.F.E. and other solutions from AveriStar, speak with a Sales Representative at 704-992-7701 or visit www.averistar.com.