

Securing the Road to VoIP and IMS

As your organization makes the leap from traditional TDM communications to VoIP and Internet Multimedia Subsystem (IMS) Palindrome Technologies can be your trusted security advisor in architecting and deploying VoIP Solutions. Palindrome remains vendor neutral in order to provide unbiased and objective recommendations and solutions that match your business, operational and infrastructure requirements. Our experience with carrier grade networks allow us to assess and apply tailored solutions that are designed to enhance the security posture of your network while maintaining the benefits of new technologies, platforms, services or products. Palindrome can assist you in the following areas:

- ✦ Assess the security of the current VoIP/IMS architecture in order to identify weaknesses that can impact operations, perform fraud or gain unauthorized access to information or services.
- ✦ Develop requirements for secure operations to administer and manage your VoIP/IMS network. This focuses on securing the administrative and management tasks by specifying security services such as authentication, authorization, system and network integrity, confidentiality and auditing. It will also cover the security architecture aspects of protecting the management and control functionality and interactions.
- ✦ Develop requirements for network elements (NEs) that perform access, transport, switching and signalling functions. This will focus on both protecting the NEs and for supporting other security functions such as access screening and filtering.
- ✦ Develop requirements for the secure rollout of the VoIP/IMS network by specifying the security engineering activities to support the development, trialing, integrated testing and staged deployment of the VoIP/IMS network functionality and services.
- ✦ Develop requirements for the secure interconnection of the VoIP/IMS network with the PSTN and other internal and external VoIP/IMS networks to support boundary controls to manage the risks and support network resiliency.
- ✦ Perform vulnerability assessment your VoIP/IMS network in order to identify vulnerabilities that be used to gain unauthorized access to organizational assets, information or services.
- ✦ Perform product evaluations to verify that they demonstrated the proper functionality to support your architectural, operational, management and security requirements.



Experience

Palindrome team members have assisted telecommunication carriers, service providers and enterprise network owners in architecting and evaluating the security of VoIP implementations and are known for their research efforts and contributions to standards-setting bodies (e.g. IETF and ATIS) and industry forums.

Palindrome Technologies is a product-neutral organization with no inherent technology bias. For additional information you may contact us at info@palindrometech.com