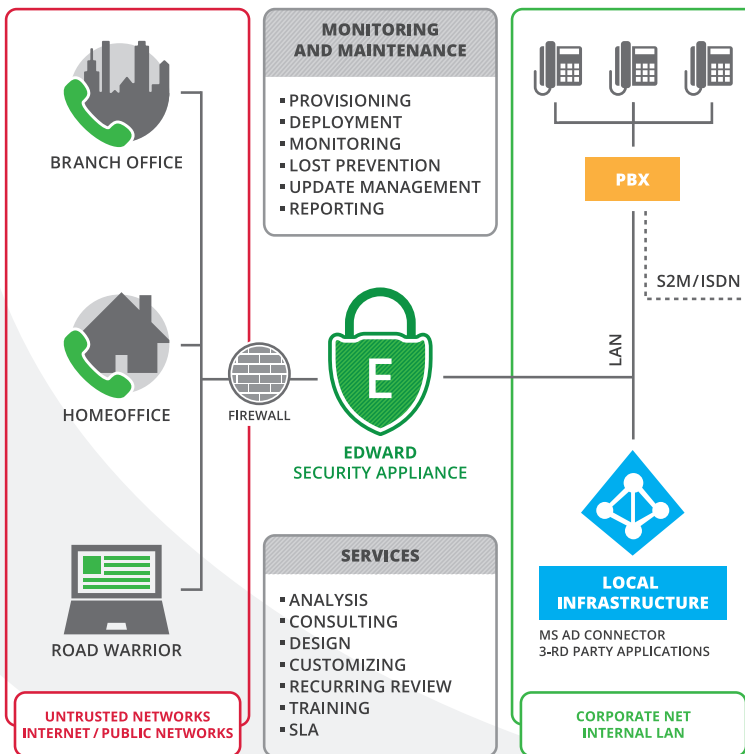


EDWARD SECURITY APPLIANCE

SECURE TELEPHONY OVER IP NETWORKS



- Standalone, hybrid or proxy solution
- Full encryption of control data and voice payload
- Transport via SIPS / SRTP or OpenVPN tunnel
- Automatic provisioning
- Integration to Microsoft Active Directory
- Built-In SSL PKI
- Hardware or virtual appliance

Secure communication is a trending topic. With the Edward Security Appliance METASEC delivers a solution for secure and encrypted audio and video communication over IP networks.

The Edward Security Appliance covers not only the common aspects of encrypted telephony but, also provides functions for device management, proactive reporting and monitoring.

Basically Edward supports three different operation modes:

As a »Standalone System«, it establishes a second secure communication path beside the regular telephony.

Running in »Hybrid Mode« remote branch offices or home office workers can be connected to the existing telephony. In this mode, Edward operates as a subsystem of the main corporate PBX system.

The third mode, the so called »Proxy Mode«, Edward handles only the secure connection to the telephone device.

In this mode, Edward operates as a de- and encryption instance between the corporate PBX system and telephone device. Connections coming from the telephones are received by Edward, decrypted and forwarded to the regular IP PBX system. The call handling itself stays on the main PBX.

Edward supports the industrial standard encrypted transport* via SIPS/SRTP. Also the very common tunneling via OpenVPN is implemented as well. Both principles rely on the SSL technology which are considered as secure.

As far as the device supports it, automatic provisioning with configuration settings is also implemented. This allows plug and play rollouts and saves lots of time.

In the case of theft or other kind of compromise, devices can be disabled remotely.

Another very important infrastructural feature is the connector for the Microsoft Active Directory. This enables the administrator of larger setups to handle this part of the IT process also from a known instance.

Ask us and discuss your ideas with us. A solution is often easier than you think...

*The available encryption options depend on the functionality of the terminal used in each case.

