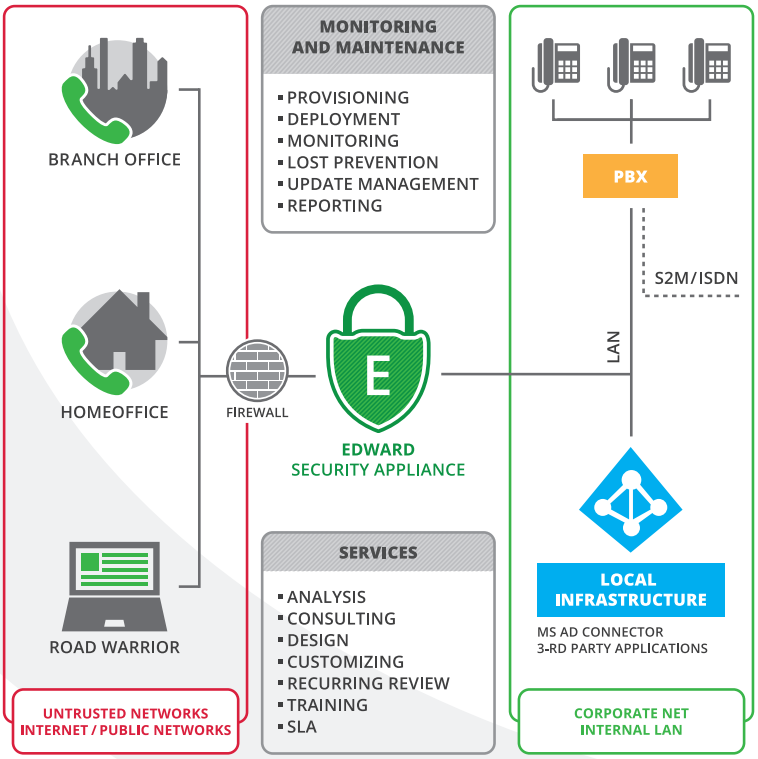
EDWARD SECURITY APPLIANCE

SICHERE TELEFONIE ÜBER IP NETZE



- Standalone, Hybrid oder Proxy Betrieb
- Volle Verschlüsselung von Steuer- und Sprachdaten
- Transport via SIPS / SRTP oder OpenVPN Tunnel
- Automatische Provisionierung
- Integration ins Microsoft Active Directory
- Integrierte SSL PKI
- Hardware oder virtuelle Appliance

Sichere Kommunikation ist in aller Munde. Mit der Edward Security Appliance bietet METASEC ein Produkt zur sicheren und verschlüsselten Audio- und Videokommunikation über IP Netze.

Die Edward Security Appliance deckt jedoch nicht nur Aspekte der reinen verschlüsselten Telefonie ab, sondern sieht auch Funktionen im Bereich der Verwaltung der Endgeräte als auch proaktives Reporting und Monitoring vor.

Grundsätzlich kann Edward in **drei unterschiedlichen Modi** betrieben werden:

Als **»Standalone System«** etabliert es einen zweiten, sicheren Kommunikationspfad parallel zur vorhandenen Telefonie.

Im **»Hybridmodus«** können entfernte Niederlassungen oder Homeoffices sicher an die bestehende Telefonie angebunden werden. Hierbei läuft Edward als Unteranlage des TK Hauptsystems.

Mit dem dritten Modus, dem so genannten **»Proxymodus«**, wird eine vollwertige gesicherte Übertragung zwischen Endgerät und dem TK System etabliert.

Hierbei wird Edward als Ver- und Entschlüsselungsinstanz zwischen TK System und IP Endgerät geschaltet. Die Verbindungen werden vom Edward entgegengenommen, entschlüsselt und an das vorhandene IP TK System übergeben. Die Vermittlung der Rufe erfolgt auf dem IP TK System.

Als Verschlüsselungsarten* unterstützt Edward sowohl die Standardübertragung via SIPS/SRTP als auch über OpenVPN Tunnel, die von vielen Endgeräten aufgebaut werden können. Beide Prinzipien setzen technologisch auf SSL und gelten als sicher.

Soweit vom Endgerät unterstützt, wird die Provisionierung, also die automatische Versorgung mit Konfigurationseinstellungen, ebenfalls angeboten. Damit ist ein Plug and Play beim Rollout ohne weiteres machbar.

Im Falle von Diebstahl oder anderer Art der Kompromittierung, können Geräte ebenfalls zentral deaktiviert werden.

Ein weiteres wichtiges infrastrukturelles Feature ist die Anbindung an das Microsoft Active Directory. Somit ist der Administrator in der Lage, auch diesen Teil des IT Prozesses zentral zu verwalten.

Sprechen Sie uns an und diskutieren Sie Ihre Idee mit uns. Eine Lösung ist häufig einfacher und näher als man glaubt...

* Die verfügbaren Verschlüsselungsoptionen sind vom Funktionsumfang des jeweils eingesetzten Endgerätes abhängig.

made in Germany

www.metasec.de