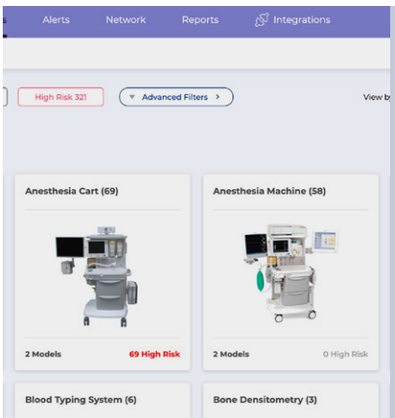

Vernetzte medizinische Geräte erkennen und schützen

Oft haben Healthcare-Organisationen keine vollständige Übersicht über ihre vernetzten medizinischen Geräte – vom Perfusor bis zum MRT. Dies ist riskant für die Sicherheit und hinderlich für Verwaltung und Maintenance des Geräteparks. Die IoMT-Lösung (Internet of Medical Things) von Medigate erstellt ein komplettes, stets aktuelles Inventar, erkennt durch Analyse des Netzwerkverkehrs potenziell gefährliche Vorgänge, hilft Sicherheitsrichtlinien durchzusetzen und liefert Erkenntnisse für das Management – bis hin zum Nutzungsgrad kostspieliger Geräte wie Tomografen. Medigate ist als offene Plattform konzipiert und arbeitet mit Cybersecurity- und Directory-Lösungen zusammen.

- Erstellt exaktes Inventar des medizinischen Geräteparks
- Erkennt Anomalien in der Gerätenutzung und im Datenverkehr
- Verhindert zusammen mit Firewall/NAC-Lösungen Cyberangriffe und illegitimen Datenabfluss
- Liefert Erkenntnisse über Auslastung der Geräte

www.boll.ch/de/medigate/index.html

SEPPMAIL

Sicheres E-Mail für Microsoft 365

Immer mehr Unternehmen setzen für E-Mail auf Microsoft 365. Um einen sicheren Informationsaustausch zu garantieren und gesetzliche Anforderungen wie die DSGVO zu erfüllen, sollte der E-Mail-Verkehr verschlüsselt ablaufen – und zwar möglichst so, dass weder Absender noch Empfänger komplizierte Bedienschritte durchführen müssen. Das Secure E-Mail Gateway von SEPPmail ist eine komplette, äusserst nutzerfreundliche Verschlüsselungslösung, die transparent und automatisch im Hintergrund arbeitet und sich nahtlos und fast ohne Aufwand als Schnittstelle zwischen dem Internet und Exchange Online integrieren lässt.

- Sicherer, DSGVO-konformer E-Mail-Verkehr mit Exchange Online
- GINA-Technologie für verschlüsselte E-Mails an Empfänger ohne eigene Verschlüsselungslösung
- Automatische Vergabe von Signatur-Zertifikaten
- Unterstützt alle gängigen Standards wie S/MIME, TLS und openPGP

www.boll.ch/de/seppmail/index.html

Alcatel·Lucent Enterprise

Homeoffice leicht gemacht

Bei Homeoffice sollte der sichere Anschluss ans Firmennetzwerk möglichst einfach vonstattengehen. Alcatel-Lucent Enterprise hat sich der Herausforderung angenommen und liefert mit den eleganten Remote Access Points der Stellar-Linie eine clevere Lösung: Der Remote-AP nimmt automatisch Verbindung mit dem Firmennetz auf, wo er in der Managementplattform OmniVista anhand von Seriennummer und MAC-Adresse erkannt und passgenau konfiguriert wird – nach dem Plug&Play-Prinzip praktisch ohne Aufwand aufseiten des Nutzers. Im Hintergrund arbeitet der OmniVista VPN Server, der sichere Tunnels für Management- und Nutzdaten bereitstellt.

- Sichere, unkomplizierte, kosteneffiziente Zugangslösung für Homeoffice und kleine Niederlassungen
- Stellar Remote Access Points für automatische Verbindung zum Firmennetzwerk
- Managementplattform OmniVista als Cloud-Lösung Cirrus oder als On-Premises-Lösung Enterprise verfügbar
- OmniVista VPN Server stellt sichere Tunnels automatisch bereit

www.boll.ch/de/alcatel/index.html