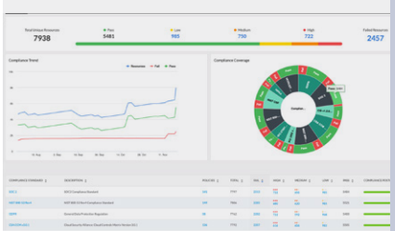

paloalto NETWORKS

Beste Sicherheit für Cloud-Umgebungen

Umfassende Sicherheit für die zunehmend komplexeren Multi- und Hybrid-Cloud-Umgebungen lässt sich nur mit einer cloudnativen Security-Plattform (CNSP) mit zentraler Verwaltung, laufender Überwachung, vollständigem Inventar aller Ressourcen und durchgängiger Visibilität erreichen, die Prävention und Transparenz unter einem Dach vereint.

Prisma Cloud von Palo Alto Networks schützt Anwendungen, Daten und cloudnative Technologien wie Container mit branchenführenden Sicherheits- und Compliancefunktionen in fünf Kernbereichen während des gesamten Lebenszyklus.

- Komplettes Management des Cloud-Sicherheitsniveaus
- Schutz für sämtliche Cloud-Workloads
- Management der Infrastruktur-Zugriffsrechte
- Cloudübergreifende Netzwerksicherheit
- Sicherheit für DevSecOps- und Shift-Left-Entwicklungs- und -Betriebsmodelle

Weitere Informationen
www.boll.ch/info/Prisma-Cloud

MEDIGATE

Medigate: Wirksame Sicherheit für medizinische Geräte

Cyberattacken auf Spitäler nehmen stark zu und erfolgen vielfach über die schwächsten Einstiegspunkte: die mit dem Netzwerk verbundenen medizinischen Geräte. Diese sind in der Regel nicht darauf ausgelegt, professionell durchgeführten Angriffen zu widerstehen. Die Folgen reichen von Diebstahl und Manipulation von Patientendaten bis hin zur Erpressung.

Die Inventarisierungs- und Sicherheitsplattform Medigate ist speziell auf vernetzte medizinische Geräte ausgelegt und unterstützt Healthcare-Organisationen dabei, ihren medizinischen Gerätepark sicher und effizient zu betreiben.

- Exaktes Inventar aller vernetzten medizinischen Geräte
- Detaillierte Informationen zu jedem Gerät und dessen Status
- Erkennen von Anomalien in Gerätenutzung und Datenverkehr
- Blockieren von illegitimem Datenabfluss (zusammen mit Firewalls/NAC-Lösungen)
- Informationen über die Auslastung der Geräte

Weitere Informationen
www.boll.ch/medigate/index.html

kaspersky

Flexibler Endgeräteschutz für jede Situation

Beim Endgeräteschutz können klassische Antiviruslösungen nicht mehr voll punkten. Das Zauberwort heisst EDR. Endpoint Detection and Response erkennt auch komplexe, dateilose und zielgerichtete Bedrohungen und sorgt durch Echtzeitüberwachung, zentrale Visibilität, tiefgreifende Analyse und Automatisierung für eine passgenaue Abwehr.

Kaspersky bietet mit EDR Optimum, Managed Detection and Response (MDR), der Expertenlösung XDR und einer äusserst flexiblen Lizenzierung Endgeräteschutz per EDR für jeden Bedarf – vom Anwender mit wenig eigenem Security-Know-how bis hin zum Spezialisten, der sich täglich mit Cybersecurity beschäftigt.

- Rasche Abwehr von Angriffen – wichtig bei Ransomware-Attacken
- Automatisierung entlastet die IT-Security-Abteilung
- Volle Transparenz über die Vorgänge an den Endgeräten
- Detaillierte Vorfallsdaten und unverzügliche Behandlung von Vorfällen
- Keine gefährlichen Überbleibsel von Angriffen – auch Advanced Persistent Threats werden eliminiert

Weitere Informationen
www.boll.ch/datasheets/HF_Kaspersky_EDR_D.pdf