KRANKENHÄUSER BENÖTIGEN UMFANGREICHEN CYBERSCHUTZ – HP WOLF SECURITY LIEFERT IHN

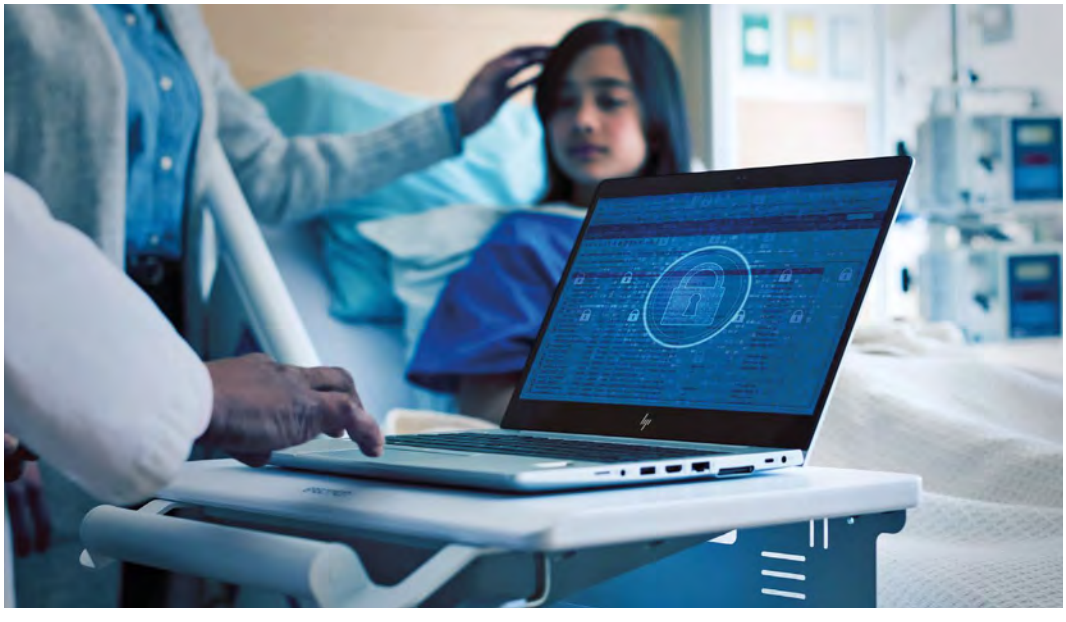
HP WOLF SECURITY Krankenhäuser müssen ihre IT-Architektur besonders gut vor Cyberangriffen schützen, immerhin muss die Versorgung von Patienten kontinuierlich gewährleistet sein. Deswegen gehören sie laut Definition des Bundes zur sogenannten kritischen Infrastruktur (KRITIS). Als solches sind sie dazu verpflichtet, ihre Systeme besonders gut zu sichern – und erfolgreiche Angriffe umgehend zu melden.

Wie in Unternehmen suchen Cyberkriminelle auch bei Kliniken nach Schwachstellen bei Endgeräten, die sie als Einfallstore nutzen können. Integrierte Maßnahmen sind daher unerlässlich, um die Sicherheit sensibler Daten – aber auch die Sicherheit von Patienten beispielsweise während einer Operation – zu gewährleisten. Hier setzt HP Wolf Security an: Das integrierte Security-Portfolio Wolf Security umfasst Sicherheitslösungen für Kliniken jeder Größe – maßgeschneidert auf die Bedürfnisse der Nutzer und kompakt auf einer Plattform bereitgestellt.

HP WOLF ENTERPRISE SECURITY: KONTINUIERLICH WACHSAM

Die Sicherheitsmaßnahmen unterstützen Security-Teams. Denn Endgeräte sind häufig der erste Angriffspunkt von Cyberkriminellen. HP bietet eine Reihe von Services, um diese zu schützen. Indikatoren für Angriffe und Sicherheitsverletzungen helfen beispielsweise, Dateien in Quarantäne zu verschieben. Dabei verfolgt HP Wolf Security das Zero-Trust-Prinzip, sprich: Die mit HP Wolf Security ausgestatteten Anwender und Geräte können sicher arbeiten, während externe Inhalte und Webseiten isoliert und gesichert geöffnet werden. Somit kann kein Schadcode auf das Endgerät oder in das Unternehmensnetzwerk gelangen. Kliniken und deren Security-Teams können sicher sein, dass von diesen Mitarbeitern oder Applikationen keine Gefahr ausgeht.

Zwei Werkzeuge im HP Wolf Security Portfolio – HP Sure Click Enterprise und HP Sure Access Enterprise – sorgen für zusätzliche Sicherheit. HP Sure Access Enterprise basiert auf dem Zero-Trust-Prinzip und findet Verwendung bei der sicheren Administrierung unternehmenskritischer Assets. Wird das Endgerät eines Benutzers kompromittiert, stellt dies dank einer vollständigen Isolierung kein Risiko für die Remote-Anwendung und die darin enthaltenen vertraulichen Daten dar. Ein weiterer Schutzmechanismus ist HP Sure Click Enterprise. Die Anwendung öffnet Dateien, E-Mail-Anhänge oder Websites in virtuellen MicroVMs und schützt so Rechner und Netzwerk vor möglichen Bedrohungen. Schließt der Nutzer die Datei oder den Anhang, wird die Malware automatisch gelöscht. Auch unbekannte Dateien lassen sich so öffnen, ohne dass Gefahr droht. Das Prinzip der Virtualisierung schützt allerdings nicht nur den Anwender, sondern auch kritische Management-Applikationen, die in einem isolierten Browser betrieben werden. HP Wolf Security sichert Kliniken somit umfangreich ab und reduziert ihre Sicherheitsrisiken deutlich – und schützt somit Patienten, deren Daten und auch die Klinik insgesamt.



HP Deutschland GmbH
Herrenberger Straße 140, 71034 Böblingen
Tel.: +49-(0)7031-450 70 00
E-Mail: dominic.scholl@hp.com
www.hp.com/de-de/security/endpoint-security-solutions.html