



CASE STUDY

Al Wifaq Medical Group

K7 supports reliable physical
health enablement with
dependable digital safety

"Every organisation in the healthcare sector has to worry about cyberattacks, especially ransomware. We were additionally concerned about the performance impact and manageability of cybersecurity solutions. K7 EPS has allayed both concerns. The behaviour-based ransomware protection has stopped every attack across our branches without slowing down any device. We are also very happy with the easy monitoring, responsive support, and flexible licensing."

Pawan Kumar

Head - IT, Al Wifaq Medical Group

The Al Wifaq Medical Group stands for safety and reliability in physical health. K7 Security has the same reputation in digital security, and helps them serve customers without cyber risk.

Client Snapshot

- » Headquartered in Riyadh, Saudi Arabia
- » Provides medicine, health, beauty and well-being services
- » Brands include Al Wifaq Medical Pharmacy, Al Qefary Pharmacy, and Safe Pharmacy

Pharmacy customers need to know their medicines will work as expected. The Al Wifaq Medical Group gives them this confidence by providing dependable dispensary services across multiple branches and brands. Their reputation for reliability is critical – a reputation that cybercriminals would threaten for monetary gain if they find any gap in their cyber defences.

Enabling Physical Wellbeing Requires Sound Digital Health

Dispensing medicines and therapeutic supplies needs to be done safely and discretely. The customer should know that the supplier is reliable and will provide the treatment exactly as prescribed. This requires an equally safe and reliable digital infrastructure. The Al Wifaq Medical Group wished to secure their computing resources, and decided on several priorities for their cybersecurity solution:

- Reliable detection and blocking of cyberattacks, especially ransomware
- Unimpaired hardware performance, to avoid compromising customer experience
- Ability to manage cybersecurity across dozens of endpoints spread over multiple branches
- Ensuring responsible use of IT assets across branches without being physically present
- Centralised listing of endpoint security status

K7 Protects Pharmacies by Stopping Digital Infections

The Al Wifaq Medical Group understands why cybercriminals would like to target them, especially with ransomware. The entire healthcare value chain faces this cyber risk. Their leaders wish to be proactive in countering this threat and maintain their reputation for safety, reliability, and flawless customer experience.

Unmatched Cyberthreat Protection

K7's Endpoint Security (EPS) is built around extensive research into cyberthreats and how they try to infiltrate enterprise networks. This comprehensive defence mechanism gives the Al Wifaq Medical Group the confidence that their operations will not be compromised by a cyberattack.

Multilayered Detection and Prevention

K7 EPS combines Artificial Intelligence with multiple layers of protection to stop malware, block phishing websites, protect against exploits, and prevent zero-day attacks. A firewall with Intrusion Detection System and Intrusion Prevention System empowers the Al Wifaq Medical Group to monitor all data traffic flowing into and out of their network to identify any malicious activity.

Ransomware Protection

Ransomware has become the cyberattacker's preferred weapon against the healthcare sector. K7 augments signature-based protection with behaviour-based protection, spotting and stopping malicious encryption for their cybersafe pharmacy operations.

Enterprise-grade Features

K7 EPS is designed for the enterprise with emphasis on performance, scalability, and manageability. The licensing model also allows the Al Wifaq Medical Group to expand across branches without being hampered by inflexible licensing policies.

User-group Based Restrictions

K7 EPS provides centralised control over whether USB device access is enabled, what applications can be installed and which websites can be accessed. These features, coupled with the intuitive UI that enables them to make quick changes to these settings, makes it easy for the group to enforce cybersecurity standards across multiple branches.

Low-impact Protection

K7 EPS has been tested by AV-Comparatives and is proven to provide powerful protection without slowing down the device, allowing the Al Wifaq Medical Group to protect endpoints without upgrading hardware.

Flexible Licensing

K7 provides a single license that can be used across multiple sites. This enables their IT team to allocate IT assets across branches based on business requirements without worrying about individual branch licenses.

At-A-Glance Monitoring

K7 EPS provides an intuitive dashboard that helps the Al Wifaq Medical Group's IT team quickly monitor and understand the security status across the organisation without spending much time at the console, which allows them to act immediately on threat warnings and secure the organisation.

Expert Support

K7 Security ensures close collaboration between Support and Engineering teams. This enables our support team to respond rapidly to any concerns from the Al Wifaq Medical Group, proving to them that we are committed to ensuring their cybersecurity.

How K7 Meets Al Wifaq Medical Group's Priorities

- Multilayered cyberthreat detection and prevention
- Dedicated ransomware module
- Centralised user-group based restrictions
- Certified low-impact protection
- Multi-site control with flexible licensing
- At-a-glance security status monitoring
- Quick, knowledgeable support

K7 Security's Endpoint Security enables the Al Wifaq Medical Group to focus on providing safe and reliable health services to their customers while we ensure that they remain safe from cybercriminals. [Contact Us](#) to learn more about our enterprise cybersecurity solutions that provide effective, unobtrusive protection.



Copyright © 2020 K7 Computing Private Limited, All Rights Reserved.

This work may not be sold, transferred, adapted, abridged, copied or reproduced in whole or in part in any manner or form or any media without the express prior written consent of authorised personnel of K7 Computing Private Limited. All product names and company names and logos mentioned herein are the trademarks or registered trademarks of their respective owners.

www.k7computing.com