CASE STUDY

King Fahad Medical City Depends on Infoblox for Secure Access Service Edge and Cybersecurity

Customer: King Fahad Medical City (KFMC)
Industry: Healthcare
Location: Saudi Arabia

Initiatives:
• Migration of hardware-based approach to virtual appliances
• Secure modern networking approaches including SD-WAN and SASE
• Enable safe, secure access for both on-premises and remote workers
• Achieve DNS protection compliance according to Essential Cybersecurity Controls published by National Cybersecurity Center

Outcomes:
• Increased capacity to support users
• Aligned with regulatory compliance mandates for cybersecurity
• Improved security to defend against DNS attacks
• Helping KFMC comply with local regulatory mandates on cybersecurity

Solution(s):
• BloxOne™ Threat Defense (hybrid DNS firewall)
• Infoblox secure DDI

The Customer

Based in Riyadh, the capital city of Saudi Arabia, the King Fahad Medical City (KFMC) is the largest medical facility in the country. Its four hospitals have a workforce of over 10,000 employees. The medical complex supports more than 30,000 inpatients and 500,000 outpatients a year and is recognized as one of the top medical facilities in the Middle East.

From an IT perspective, KFMC operates two data centers that support its medical facilities. KFMC first deployed Infoblox DDI hardware a few years ago to support IP address management (IPAM) demands, including internal and external DNS and DHCP, across its distributed network environment. Associate executive director of IT operation Abdullah Alismail, chairperson of system department Samer AlShlayan and infrastructure team lead Mohamed Selim are primarily responsible for planning and carrying out the KFMC strategy for digitally transforming, managing and protecting the entire KFMC network.

The Challenge

For the medical facility, the impact of COVID-19 has been particularly profound. The operational demands on KFMC increased exponentially as the pandemic placed new restrictions on movements and significantly accelerated the need for remote access.

The changing network environment overall has been another key challenge facing KFMC. In recent years, the emergence of the secure access service edge (SASE) as well as software-defined WAN (SD-WAN) paradigms has changed the way many organizations, including KFMC, look at network architecture. KFMC wanted to have IPAM and security devices in place that reflect and embrace those approaches. KFMC’s IT team also needed to address compliance rules defined by the Kingdom of Saudi Arabia’s National Cybersecurity Authority, which has introduced controls to help protect digital infrastructure.
In addition, KFMC needed to introduce enhanced DNS security. Just prior to KFMC rolling out its Infoblox refresh, it experienced a targeted attack against its DNS infrastructure. For KFMC, IPAM and secured access are not luxuries—these technologies literally could mean the difference between life and death for its patients.

Adapting to the Evolving Threat Landscape

Until recently, the ministry’s cybersecurity strategy and cybersecurity incident response strategy have sufficiently protected against existing threats. However, after further investigating the rapidly evolving threat landscape, the ministry identified an evolutionary need to leverage advanced DNS security and firewalling for a more robust solution that would protect against emerging cyber Threats.

If malware cannot be detected or blocked during the attack stage of delivery, DNS transactions can be checked again on execution of the exploit, C&C and objective, thus increasing the probability of blocking unauthorized communications that slipped through during the attack stage. Table 1 presents the interaction of attack stage and content with logs.

Table 1

<table>
<thead>
<tr>
<th>Attack Stage</th>
<th>Attack Content that can be Detected in Logs</th>
<th>Log Acquisition Target Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Reconnaissance</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>2 Weaponisation</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>3 Delivery</td>
<td>Sending of emails with malware attached by attackers</td>
<td>Mail server</td>
</tr>
<tr>
<td>4 Exploit</td>
<td>Callback (communications sent outside the company without going through a web proxy server)</td>
<td>Firewall</td>
</tr>
<tr>
<td>6 C&amp;C</td>
<td>Callback (communications sent outside the company without going through a web proxy server)</td>
<td>Firewall</td>
</tr>
<tr>
<td>7 Execution of the purpose</td>
<td>Callback (communications sent outside the company without going through a web proxy server)</td>
<td>Firewall</td>
</tr>
</tbody>
</table>

Source: “Using Logs for the Early Detection and Analysis of Sophisticated Cyber Attacks,” by the JPCERT Coordination Center

Taking a Hybrid Approach to Threat Defense

As a core part of the network refresh, KFMC embraced the Infoblox BloxOne Threat Defense Advanced (hybrid solution) to help solve its security challenges. BloxOne Threat Defense Advanced is Infoblox’s subscription-based, hybrid security platform that uses cloud infrastructure to identify and protect against both known and unknown threat attack vectors.

As a hybrid solution, BloxOne Threat Defense Advanced also integrates with KFMC’s on-premises systems, providing a layer of protection that isn’t possible with a system that relies entirely on the cloud. With BloxOne Threat Defense Advanced, both on-premises and remote users of the KFMC network are secured and protected against threats that impact their ability to conduct their life-saving work.

Improving Operational Efficiency with Lower Cost

By moving to a virtual appliance model, KFMC has been able to recognize an improved return on investment. Instead of having a capital expenditure with hardware, KFMC now has an operational expenditure with a subscription-based model that scales to deliver the technology that is needed.
KFMC has also been able to save money by deploying BloxOne Threat Defense Advanced. Instead of needing to acquire, manage and operate a host of different security controls, the Infoblox approach enables consolidation and cost optimization.

**Enabling Digital Transformation with the Cloud**

Digital transformation is critical for organizations of all types, especially in times of crisis, because it enables them to do more with less. A key part of digital transformation is about using the cloud and benefiting from the operational and scalability advantages it provides.

In healthcare, scalability and security are not optional components; they are essential for human survival. With solutions from Infoblox, KFMC is now more aligned with its digital transformation efforts and is well positioned to accelerate that transformation in the months and years ahead as it continues its important work.

---

**For More Information**

Learn more about how you can proactively detect malware and protect your users and data via DNS. Speak with an Infoblox representative or start your free trial of our BloxOne Threat Defense technology today.