FORTINET

CASE STUDY

Boosting Internet Security for the Airport International Group

مجموعة المطار الدولي
Airport International Group

The Airport International Group (AIG) is the strategic Jordanian investor responsible for operating, maintaining and redeveloping Jordan's Queen Alla International Airport (QAIA) – Jordan's largest airport. AIG has invested nearly USD 1 billion in the redevelopment of QAIA's two original terminals, replacing them with a new, state-of-the-art terminal that has bolstered Jordan's ability to accommodate rising passenger numbers and support its thriving tourist industry.

The Cybersecurity Challenges Facing Airports

As a major international airport operator, internet security is of paramount concern for AIG. When the group assumed operational oversight of QAIA in 2007, it inherited an IT infrastructure that included a mix of traditional security measures, including firewalls, IPS, end user anti-virus tools, anti-spam and mail security. While these tools were able to manage QAIA's internet security needs at the time, the evolving cybersecurity threat landscape necessitated a review of its requirements.

AIG understood the vulnerability of airports with cybersecurity threats, which have the potential to infiltrate virtually any part of its distributed networks. As a result, impacts on the airport could be extremely serious, ranging from disrupted daily operations, to service interruptions, data leakage and data loss.

Overhauling Internet Security

AIG conducted a review of its cybersecurity needs and found that a lack of integrated automated information security across their entire network was a major issue. It was quickly determined that its existing tools weren't capable of meeting AIG's needs.

Additionally, AIG understood that the constantly evolving cybersecurity threat landscape presented a major challenge to its day to day information security operations. They needed fast and accurate threat intelligence, capable of identifying and quickly securing the group against cyber threats. The ability to obtain a 360 view of information security and cybersecurity threats and proactive response was considered a priority.

A further challenge that AIG faced was that its IT professionals had to conduct manual threat analysis, detection, and mitigation with its existing cybersecurity tools, which took significant time and effort. In some cases, the accuracy of detection and response was not efficient enough to take action at early stages of an incident. Also, the growing number of threats and their rapidly-changing nature, made it extremely difficult for the company to respond in a timely manner.

> *"AIG's security management evolved tremendously after implementing Fortinet security technologies. Automated threat detection analysis and prevention using a single management tool gives us world-class cybersecurity capabilities."*
>
> *– Waseem Al Rusan,*
> *IT Director of the*
> *Airport International Group*

Considering the nature of the challenges it faced, AIG determined that it had a critical need to implement automated technology to detect and secure against cybersecurity threats. Specifically, it required a fully integrated technology solution that could effectively secure and provide real-time information security and threat visibility for the entire network and its devices.

After reviewing the security market, AIG decided to implement Fortinet's products because it offered fully integrated security intelligence and cybersecurity threat management solution.

According to Waseem Al Rusan, IT Director of AIG: "A key reason for selecting Fortinet was that it offered holistic information security visibility across the enterprise network of the airport, enabling IT to respond in real-time to the cyber threats effectively".

Implementing Advanced Threat Intelligence

"Real time security threat visibility, detection, analysis and automated prevention that incorporates artificial intelligence and machine learning has provided us with significantly enhanced cybersecurity capabilities," noted Al Rusan.

"Fortinet gives us broad visibility and protection across the cyberattack surface for the entire network, including integrated detection and response to advanced threats, as well as automated operations and analytics via a single console. It also incorporates sophisticated cyberattack technologies, such as artificial intelligence and machine learning that reduce the time from intrusion to attack."

In just a few months, the Fortinet Security Fabric has enabled AIG to detect and respond to over 40 undetected threats using advanced threat protection; reduce spam emails by 50 per cent; and to automatically respond to over 100 web application attacks on a monthly basis.

The Fortinet Security Fabric has decreased the complexity of AIG's security infrastructure thus reducing the cost of the resources needed to integrate security controls. As Fortinet enables one-click seamless integrations, it has also reduced operational costs in terms of the effort needed to manage these controls.

Based on the success of its cybersecurity overhaul, AIG is planning future expansions of Fortinet's solutions as it undertakes further infrastructure development.

Details

Customer: Airport International Group

Industry: Aviation

Location: Jordan

Solutions

- FortiGate
- FortiWeb
- FortiMail
- FortiClient
- FortiAnalyzer
- FortiSIEM

Business Impact

- Strengthened the internet security defences
- Simplified provisioning of services and support with an integrated solution
- Improved visibility into long-term IT strategy planning

FORTINET®

www.fortinet.com