CASE STUDY

BAA puts identity management on auto-pilot with Defender® two-factor authentication and reduces costs

Key Facts

Company
BAA

Industry
Airport operator

Country
United Kingdom

Website
www.baa.com

Challenges

Whilst its current solution fully satisfied BAA's demanding security requirements, the tokens were due to expire and would have to be replaced. Rolling out new tokens to 3,500 staff would require substantial time, effort and expense.

Results

- Delivered two-factor authentication on time and ensured future scalability
- Reduced costs with tokens that last 67 percent longer than the previous solution's tokens
- Simplified identity management and improved security
- Expected to deliver 100 percent ROI within four years

Products

Defender®

BAA is one of the world's leading transport companies and a major UK infrastructure organisation. BAA owns six airports in the UK, including the largest (London Heathrow) and is involved in almost every aspect of airport life, from day-to-day security and retail to strategy and investment. When needing to upgrade its solution for providing staff with secure IT access, BAA turned to One Identity.

BAA is considered to be a world leader in security, with almost half of its staff working in this area. BAA was using two-factor authentication to provide 3,500 staff with secure IT access. This method involves proving your identity with two methods: 'something you know' (such as a password or PIN) plus 'something you have' (such as a smart card, token or fingerprint).

ONE IDENTITY

> "BAA will save money because Defender tokens last at least **67 percent longer** than our previous solution, and last for the life of the battery rather than having a defined life of three years."
>
> *Fiona Hayward, IT Programme Manager, BAA*

Whilst its current solution fully satisfied BAA's demanding security requirements, the tokens were due to expire and would have to be replaced. Rolling out new tokens to 3,500 staff would require substantial time, effort and expense. Therefore, BAA decided to review its requirements with a view to potentially adopting a more cost-effective, two-factor authentication solution.

Scalability was an essential requirement of the solution. BAA was already providing IT access to 3,500 internal staff members and external contractors and suppliers. As part of a back-office improvement programme, new applications (such as roster scheduling) were being launched for BAA's 4,000 security staff, who would also need remote IT access. So the two-factor authentication solution had to be expanded to 7,500 users, and potentially to more users in the future.

BAA was also working to simplify its technology, so the two-factor authentication solution also had to integrate with Microsoft technologies, particularly Active Directory (AD).

The One Identity Solution

BAA reviewed the market and identified Defender as being able to meet its requirements. Defender enhances security by enabling two-factor authentication to network, Web and application-based resources. All administration and identity management is based on an organisation's existing investment in Active Directory; organisations do not need to spend time and money setting up and maintaining proprietary databases. In addition, Defender works with any OATH-compliant hardware token, so each organisation can select the most appropriate token for its users.

Of particular importance to BAA was Defender's ability to co-exist with BAA's existing solution, which would facilitate a roll-out with minimal impact on airport operations.

BAA also liked the flexibility of the tokens that are used by Defender. Both hard (e.g., physical) and soft (e.g., software) tokens can be used, and users can self-register to receive a token, which would reduce IT overhead. Users can have multiple tokens and multiple users can share one token, which BAA felt would simplify disaster recovery procedures for third-party users, such as external contractors and suppliers.

Furthermore, Defender tokens last for the life of the token battery, which is typically between five and seven years. This was at least 67 percent longer than the tokens for BAA's existing solution, which had a three-year life span.

The Bottom Line

Defender's fast roll-out ensured that BAA met its deadline for delivering IT access to its 4,000 security staff members. "From an employee-relations perspective, our extremely tight six-week deadline was set in stone," said Fiona Hayward, IT programme manager at BAA. "Defender facilitated a fast yet phased implementation, helped by its ability to co-exist with our previous solution, which ensured our 4,000 security staff members got access to the new IT systems as they'd been promised."

Defender's ability to co-exist with BAA's previous solution also ensured that continuity of service was maintained during the roll-out. "With over two million passengers passing through our airports every week, any impact on our productivity affects customers and can have horrific consequences," explained Hayward. "Our operational users need constant access to their IT systems to keep the airport running smoothly. Defender enabled us to adopt a phased approach and ensured no adverse impact on airport operations or on the IT help desk."

Defender's longer and variable token life will deliver significant cost savings. "BAA will save money because Defender tokens last at least 67 percent longer than our previous solution, and last for the life of the battery rather than having a defined life of three years," said Hayward. "We can renew users' tokens when they expire, as a help desk business-as-usual process, instead of issuing 7,500 tokens in one go and incurring the costs associated with running such a project."

By using Defender, BAA has been able to simplify administration and identity management. "Integrating with our existing Microsoft AD is a huge plus point for Defender because it simplifies identity management," noted Hayward. "For example, if a user leaves the organisation and is deleted from AD, that user's token automatically becomes invalid. This provides BAA with a second line of security."

Overall, Defender will deliver 100 percent ROI within four years. "When we factor in implementation, support and maintenance costs, we expect the solution to have paid for itself in three to four years," added Hayward.

About One Identity

The One Identity family of identity and access management (IAM) solutions, offers IAM for the real world including business-centric, modular and integrated, and future-ready solutions for identity governance, access management, and privileged management.

Learn more: OneIdentity.com