TRANSPUTEC

END USER COMPUTE AT BLOCKSPACE GROUP LIMITED

The Customer

Blockspace Group Limited is a hub for digital ventures, providing a foundation for collaborative digital services across multiple partners and services. Their digitalfrontier.com website focuses on tech-focused media and events that step beyond the daily news cycle to produce deeply reported stories on the future of business, finance, and culture.

The Challenges

Blockspace transitioned into a managed service from Transputec in February 2024. During discovery, it was identified that there was a manual process for deploying end-user devices, which was time-consuming. Assets in use included Microsoft Surface 5, MacBook Pro M2 16", MacBook Pro M2 14", and MacBook Air M2 13". Laptops were provisioned to end users with OEM out-of-the-box configuration, no standard image or centralised process.

Basic Entra RBAC (role-based access control) was used for M365 resource access. End users created their local user account during un-boxing OOBE (Out of Box Experience) with admin rights on their laptops, not necessarily using their company email. Company identities, i.e., M365 accounts, were created as general users/contributor roles except for the C-suite, which was assigned the global admin role in M365. With no central management of devices, identities, security, and policies, it was agreed that standard processes for identity, device provisioning, lifecycle management, patching, asset management, etc. were needed to create a more uniform and more easily managed end-user device environment.

Our Approach

Transputec undertook a programme of works to implement Identity & Access Management, leveraging Microsoft Entra ID, integrating it with Apple Business Manager and enabling Single Sign-On on macOS. We also implemented device management leveraging Microsoft Intune to manage company-owned MacBooks and Windows laptops, as well as BYOD management leveraging Microsoft Intune to secure data accessed via personally owned devices. Additionally, Transputec implemented endpoint security leveraging Microsoft Defender for

★★★★★

"Transputec's comprehensive approach, technical expertise, and collaborative spirit were instrumental in guiding us through this process, positioning the company for enhanced efficiency, security, and collaboration in the digital age."

Robert Jones
CTO - Blockspacer

Endpoint, BitLocker encryption, and Conditional Access.

The Outcome

Transputec's comprehensive setup and configuration delivered significant benefits to the client. By implementing custom domains, company branding, and tailored app settings, the system provided a personalised experience that aligned with the organisation's identity and requirements. The inclusion of self-service password reset (SSPR) enhanced user convenience, reducing the burden on IT support staff. Security was significantly improved through the implementation of robust authentication methods, single sign-on (SSO), and multi-factor authentication (MFA). These measures ensured that only authorised users could access the system, protecting sensitive data and resources.

The integration with Apple Business Manager streamlined management for the macOS environment, enabling efficient deployment and maintenance. For macOS devices, Transputec's setup ensured compliance with security best practices. FileVault encryption policies safeguarded data, while standard application deployment via Intune using Apple VPP apps, Intune packages, and bash scripts facilitated efficient software distribution. Compliance and update policies kept the system up-to-date and secure. On the Windows side, the Entra-joined Autopilot profile and Enrolment status page provided a seamless onboarding experience for new devices. Windows Hello for Business enhanced security by enabling biometric authentication, while OneDrive folder redirection ensured data backup and synchronisation. BitLocker encryption policies protect sensitive information and update rings-maintained system stability and security.

Endpoint Security Setup and Configuration was a critical aspect of the project, ensuring comprehensive protection for all devices. Disk encryption policies safeguarded data in the event of loss or theft, while Defender for Endpoint deployment and policies provided robust threat prevention. Conditional Access policies allow the organisation to control access based on specific conditions, such as device location or user risk level. By blocking BYOD personal devices from MDM enrolment and allowing only MAM, Transputec ensured that sensitive data remained secure on corporate-owned devices. App protection policies further safeguard sensitive information by restricting data sharing and preventing data leakage.

TRANSPUTEC

Transputec, House 19 Heather Park Drive,
Wembley, London HA0 1SS

+44 (0) 20 8584 1400 (Enquiries)
+44 (0) 20 8584 1440 (Support Desk)

www.transputec.com