CASE STUDY

MUSA INTEGRATES MICROSOFT SECURITY INTO GOOGLE WORKSPACE FOR TWO GROWING BIOPHARMA ORGANIZATIONS

CHALLENGE

For many biopharma organizations, Google Workspace remains the preferred collaboration platform. Scientists and research teams depend on Gmail, Google Drive, and Google Sheets—tools familiar from their academic roots. But as these companies expanded, their need for enterprise-level security, compliance, and device management exceeded what Google provides. Addressing these needs early is especially important in biotech, where reaching preclinical stages with compliance gaps can create avoidable risks for both the science and the business.

The client needed a way to strengthen security and compliance without disrupting the Google-based workflows their teams relied on daily. In essence, they needed a hybrid setup that connected Google Workspace with Microsoft's security and identity tools. While many managed service providers would simply suggest the client migrate to Microsoft, musa understood how important Google was to the way the culture of their company operated and developed a more secure integration.

SOLUTION

musa started with a unifying framework that connected Google Workspace with Microsoft's security and identity tools. Across both projects, they implemented Microsoft Entra for single sign-on (SSO) and multi-factor authentication (MFA), Intune for device management, and conditional access policies to control global logins and strengthen compliance. Additionally, they automated user provisioning to simplify onboarding and reduce manual administration. From there, they tailored their approach based on each company's unique environment and needs:

Mid-sized biopharma (~60 users): musa integrated Microsoft's identity and compliance controls into an existing Google Workspace environment, improving security without changing how users worked day to day.

Emerging biopharma startup (~10 users): musa built a new environment from the ground up, creating a compliant IT foundation that combined Google's productivity tools with Microsoft's governance and security framework.

RESULTS

Both organizations now use Google for collaboration, secured by Microsoft's identity management.

The combined environments delivered:

- A unified login experience through Microsoft Entra with SSO and MFA.
- Automated user provisioning and deprovisioning across both platforms.
- Centralized control of devices and policies through Microsoft Intune.
- Conditional access enforcement for improved compliance and data protection.
- A secure, scalable foundation that allows each company to expand without replatforming.

The musa team's rare ability to blend Microsoft and Google ecosystems positioned both clients for secure, compliant growth from day one and saved the costly rework and disruption many biotechs face when they wait until clinical stages to formalize security controls.