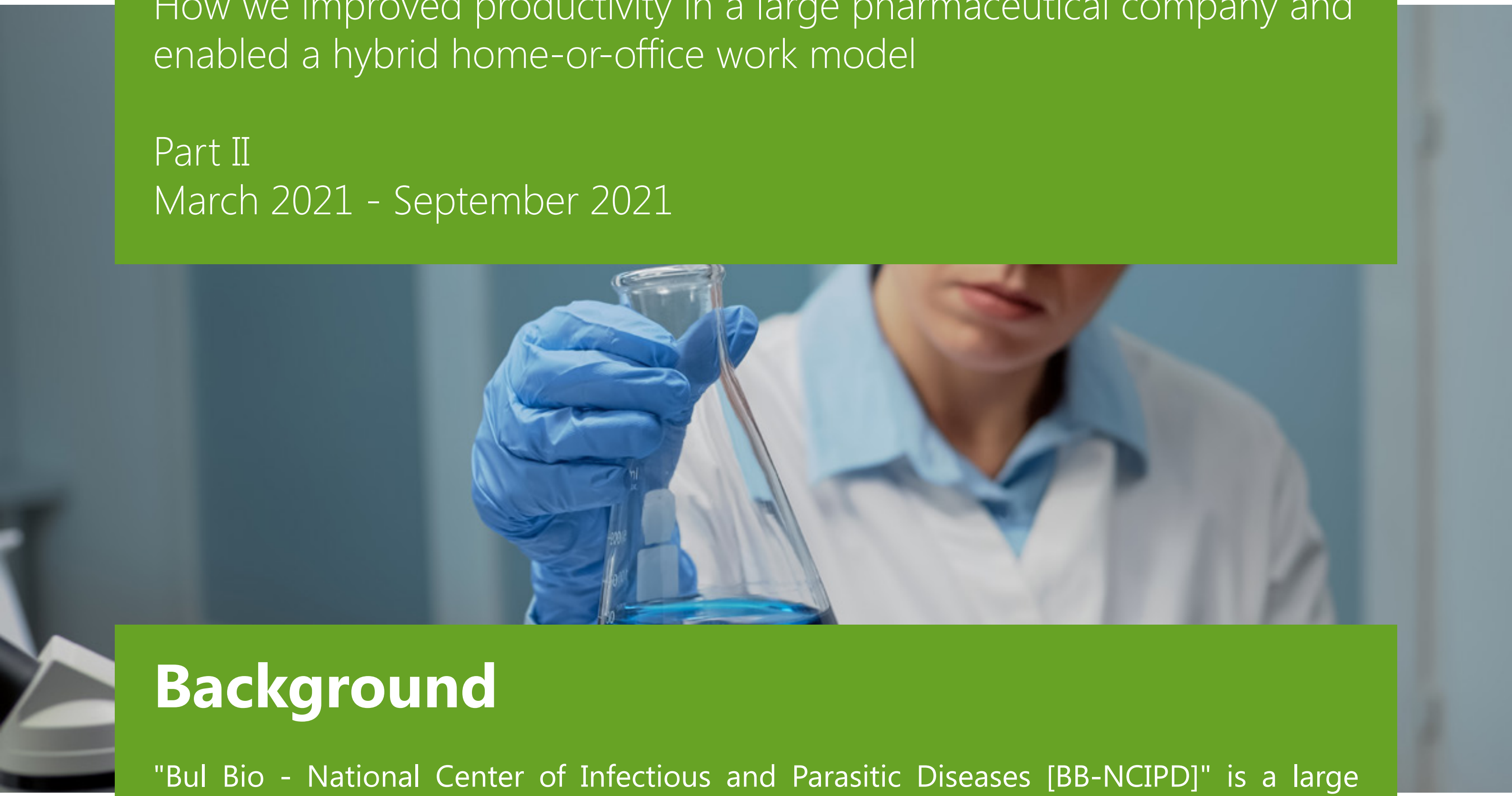
БУЛ БИО - НЦЗПБ ЕООД

Case study:

How we improved productivity in a large pharmaceutical company and enabled a hybrid home-or-office work model

Part II
March 2021 - September 2021



Background

"Bul Bio - National Center of Infectious and Parasitic Diseases [BB-NCIPD]" is a large state-owned company. It manufactures vaccines, immunostimulants, bioproducts, blood derivatives, and other pharmaceutical consumables. The company is one of the oldest in the country. It has been at the forefront of medical innovation for 150 years. Its product portfolio spans over 600 medications, including the BCG vaccine, which Bul Bio exports worldwide.

In the wake of the Covid-19 pandemic, Bul Bio was forced to organize work for its employees in a way that would allow them to access company resources remotely and securely.

Case

Bul Bio lacked the capabilities to adapt its business processes to the work restrictions stemming from the Covid-19 pandemic. The company felt insufficiencies in terms of resources and viable workarounds. This prevented them from being able to create a hybrid home-or-office work model.

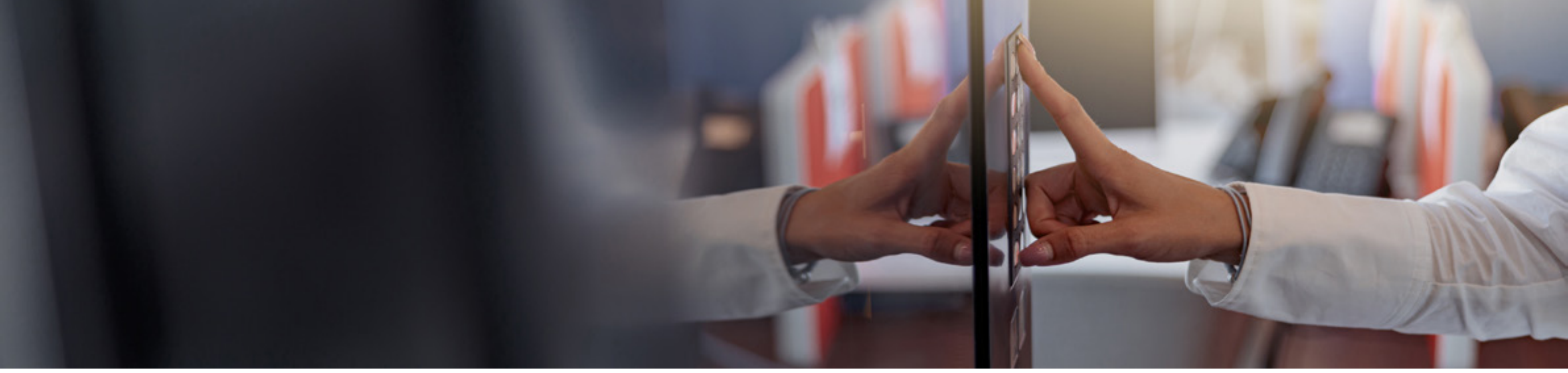
As a result, employees and partners were limited in their ability to collaborate effectively when working remotely. The situation had to be resolved, as it impeded the overall productivity of the team.

Outline
Make Target
Level.h
Level :: Level()
Level :: OnLoad(char*)
Level :: OnRender(SDL_Int
Level :: GetTile(int, int)
Level :: GetTile(int, int)
Level :: GetTile(int, int)

Solution

After an in-depth examination of the existing Bul Bio infrastructure and processes, we selected Microsoft 365 [M365] as the most feasible solution. M365 is the only cloud service that offers a fully diversified portfolio of services. The tools provided by M365 synergize perfectly to enable a complete transformation of the organization's way of work.As always, we approached the project with an emphasis on personalization. However, this time, we also utilized an internally-created best practices checklist designed specifically to facilitate M365 integrations. This kind of quality control is essential when implementing something so complex, and yet so personalized, within large organizations. The checklist serves to set the foundation for the implementation of the M365 toolset, and then to match every step of the process to what is considered the best way to do it. And so, the project unfolded in two main phases:

1. Analysis of the existing Bul Bio infrastructure via an initial audit - a step that allowed us to gain a full understanding of how M365's services could be used to transform existing processes.
2. M365 toolset implementation and checklist examination - a phase that consists of four different components, namely the setup of an Azure Active Directory, Intune Endpoint Manager and Exchange Online mail server, as well as collaboration governance to secure and validate the process with internal and external regulations. The best practices checklist was used by the team as a configuration guide and a reference throughout this entire phase.



Azure Active Directory

The first point of reference in our M365 checklist was related to the Azure Active Directory. The Azure Active Directory enables identity and data security, and solves some of the main challenges that have arisen during the Covid pandemic. Contemporary work models include remote work and therefore require remote access and enhanced flexibility. Employees and other members must be able to perform any digital activity from any location, making the traditional, office-exclusive model obsolete. The standard work model secures the company's IT infrastructure via firewalls or network segmentation. However, new security challenges could arise during the transition from a traditional to a modern work model. The Azure Active Directory helps minimize these risks with a zero-trust approach. The zero-trust approach is a modern solution for securing an organization's data, where every user or device is considered compromised by default. All users and devices are therefore thoroughly checked when attempting to access company resources, regardless of their location. This approach is enabled via a cloud infrastructure that doesn't depend on geolocation but instead allows users to access the digital corporate environment from anywhere. The zero-trust approach is enforced by conditional access policies and functions in three steps:

1. Signal - a user attempts to log into the company system
2. Decision - a decision is made on whether the user is eligible to receive access based on AI-enhanced risk cores and policies. If the user meets certain criteria, they are granted access. In cases where the user doesn't meet the criteria, there are additional conditions for verification, like two-factor authentication and other real-time checks.
3. Enforcement - depending on the login process, the user is allowed into the system with full or limited access.

Examples of criteria, which could impose additional login checks or limit the access include unusual login locations, the use of private devices, unsecure internet access, suspicious user behavior and more. All of this makes the zero-trust approach an essential part of securing a safe environment when it comes to remote work. What's more, for a company of national significance such as Bul Bio, this type of security is absolutely critical.

Intune Endpoint Manager

The next component in our M365 checklist was Intune Endpoint Manager. The checklist enabled us to determine the best way to set up this application based on the needs of the organization. Intune Endpoint Manager is a service used for application and device administration, including computers, laptops, phones, tablets, and more. It enables the security, management, and monitoring of all instances of access to corporate resources. Data protection is enforced in two layers - both with regards to company-issued devices, and when it comes to productivity apps dealing with corporate information. For example, an employee can access their email from a private device, but the organization has remote access to the way the email environment functions. The company can prohibit copying information, creating screenshots, downloading files, and other activities. In addition, any device issued to employees by the company can be remotely controlled. If a corporate device gets stolen or lost, all of its data can be deleted, regardless of its location. It only needs to be connected to the Internet.

Finally, due to Bul Bio's considerable size, the company can utilize Intune Endpoint Manager to conduct performance analytics, which reveals information about the computational productivity of separate devices. As a result, Bul Bio can enjoy more accurate and efficient device replacement when the need arises.

Exchange Online Mail Server

Our initial analysis of Bul Bio's infrastructure revealed that the existing mail server did not meet the organization's requirements. Some of the insufficiencies were related to missing address lists and calendars, the inability to book meeting rooms or resources like corporate vehicles, and others. Ultimately, the burden of administrating these activities was too high for a service that is not the main focus of the business. A quick checklist examination revealed that the best way to deal with these issues was to set up an M365 Exchange Online mail server. M365's Exchange features two sets of functionalities - one related to productivity and one related to security.

On the productivity side, it is configured to include all available meeting rooms, along with information on where the room is located, its capacity, and the number of employees or participants in the organization. This optimizes the process of scheduling meetings and enables users to see the currently available rooms, how many people will participate in a given meeting, and what resources can be booked. Users can enjoy automatic filters which make the discovery of the right room and access to resources quick and easy.

There are additional features provided by Exchange, like the option to share calendars with others, a request-and-approval process for company car booking, integration with MS Teams coupled with automatic link generation for conference calls, and more.

When it comes to security, Exchange allows for the audit of all activities taking place on the server. For instance, the service can alert administrators of unusual employee behavior such as the forwarding of an email to an external mail server. It also protects employees from suspicious attachments and links.

Crucially, it provides the option to enforce a litigation hold, which is paramount to pharmaceutical companies, as it improves information security related to medication manufacturing. What's more, the system allows critical data to be stored for certain amounts of time, and be discoverable even after deletion. By honing in on the time period that the data has been marked as crucial, administrators are able to recover it even if it has been erased.

Collaboration governance

Finally, we used the best practices checklist to determine the optimal way to configure SharePoint, OneDrive, and Teams.

- SharePoint - a shared collaboration space with dynamic work groups that grant access to specific data. The level of access is determined based on the department or group, in which the user partakes. For example, once a new employee joins the organization, they automatically receive access to corporate environments and resources based on their job title and department.
- OneDrive - a backup-enabled personalized storage solution, which we set up for Bul Bio. This allows for the restoration of files in cases of damaged or stolen computers.
- Teams - enables the organization to manage all activities. Working groups from SharePoint are synchronized with Teams, creating the opportunity for all organizational project assets and resources to be grouped in a single location.

Statistics & Impact

0-TO-100

enablement of secure remote access to company resources

35%

increase in overall labor productivity due to implementation of M365 toolset

68%

increase in data security due to M365 capabilities

MYSYNERGY
Value Digital Health & Care

Conclusion

Implementing a custom Microsoft 365 toolset without a proper guideline can reduce its positive effect on the company's operations and impede them. Using an internally-created best practices checklist enabled us to personalize the services and tailor them to the organization's specific needs.

In doing so, we guaranteed a flawless transition from the traditional work model to a modern, hybrid model, allowing employees to work from home safely and securely.

Visit our website for more solutions

Our community: