Optimizor Services Catalogue

Contents

Introduction

Optimizor specializes in managing IT infrastructures and optimizing IT processes for Fortune 100 and global industry leaders in the USA, UK, and EU. With a 98.7% satisfaction rate, Optimizor is committed to giving time back to your team.

Mission

Your IT vision optimized and uninterrupted.

Services Offered

Long-Term Partnerships

IT Managed Services

General presentation

Our Managed Services model ensures that you don't have to worry about the well-being of your end-users. We guarantee that all your systems operate smoothly and remain current with the latest patches and versions. You'll have access to three tiers of skilled engineers and IT architects, each bringing over 15 years of IT experience to your company.

I.   Support Services (Reactive):

Our subscription-based support services provide comprehensive management and optimization of IT environments. This includes Office 365 user support, Active Directory identity management, and user lifecycle automation. We ensure seamless operation of IT devices through Intune, robust antivirus protection with Microsoft Endpoint Protection, and efficient file sharing solution using SharePoint. Additionally, we handle and manage IT incidents reported by the client's helpdesk team.

Our services also include dedicated ticketing system management, IT procedure implementation, and continuous monitoring and optimization. Our skilled support team, available at various expertise levels, addresses all your IT needs.

Support services are available during business hours, excluding public holidays, with a response time of 2 hours and a resolution time of 2 business days. The service package includes remote IT

support and one on-site intervention per month at any of the client's three locations. The subscription can be adapted to client's needs.

1. Office 365 Support:

- User support for the following Office 365 services: email, SharePoint, Azure AD, Teams, Office apps, email security, user security.
- The support team will continuously monitor and optimize Office 365 services based on client needs and Microsoft recommendations.

2. Support for Windows Servers and RDP Technologies

We provide comprehensive support for Windows Server versions 2012R2, 2016, 2019, and 2022, including administration and optimization of essential services such as:

- Active Directory Domain Services (ADDS)
- File Services (FS)
- Active Directory Certificate Services (ADCS)
- Active Directory Rights Management Services (ADRMS)
- Internet Information Services (IIS)
- Windows Server Update Services (WSUS)
- Windows Deployment Services (WDS)
- Active Directory Federation Services (ADFS)
- DNS, DHCP, Remote Desktop Protocol (RDP), VPN

3. Microsoft Active Directory (Identity) Management:

- We will manage Azure Active Directory services and/or on-premises Windows Active Directory.
- We will resolve user issues related to these services.
- We will implement, optimize, and manage the Azure SSPR password reset service.
- We will implement, optimize, and manage user security services: Azure MFA and Azure Conditional Access.
- We will implement, optimize, and manage Group Policy.
- We will implement, optimize, and manage DNS services.

4. Ticketing Systems:

- We will work with existing IT incident management platforms or enroll the client in our system (IT Ticketing system).
- We will create a dedicated IT portal for users on the SharePoint platform, providing access to IT procedures and recommendations.

5. IT Procedures:

- We will implement, optimize, and manage the Change Management process.
- We will implement, optimize, and manage the Business Continuity process.

6. Description of Roles and Resources Available

Throughout the contract, the client will have access to a team of shared resources:

- **Service Delivery Manager (SDM):** The SDM is responsible for overseeing all IT support processes. Their role involves coordinating the technical team operationally, identifying time-consuming processes and proposing optimizations/automations, mediating unusual/difficult situations in IT support processes, and reporting to the client's management. The SDM serves as a Single Point of Contact (SPoC) for the client for any issues related to service delivery and quality.

- **Technical Account Manager (TAM):** The TAM is a highly skilled technical expert with knowledge across multiple technological areas. They are responsible for the technical design of solutions that include components from various expertise areas and for creating medium and long-term IT development plans. The TAM is involved in resolving complex or high-priority issues.

- **Scrum Master:** A person responsible for coordinating projects for our clients, adhering to Agile principles.

- **Level 1 Support Engineer:** This is the first level of support, handling routine user issues. Most problems in a company are typically resolved at this level. The operations performed by these individuals are based on procedures written by members of higher support levels. If issues cannot be resolved at this level, they are escalated to Level 2 support. (provided by the client)

- **Level 2 Support Engineer:** Responsible for solving issues beyond the scope of Level 1. They implement solutions proposed by Level 3 engineers/architects/TAM. These engineers usually have high expertise in specific technological areas and can address any requirements related to those technologies. Therefore, there are various Level 2 engineer profiles specialized in different areas (e.g., Networking, virtualization, operating systems, databases, etc.).

- **Level 3 Support Engineer:** The highest level of expertise in a broad technological area. Unlike Level 2 support, Level 3 engineers have extensive horizontal development, covering multiple technologies and enabling them to solve more complex problems or design new solutions. If Level 3 engineers cannot resolve an issue, a ticket can be opened with the vendor, provided there is an active support contract from the client.

7. Company Certifications

Reactive IT support services are delivered in accordance with ITIL standards, while proactive support services follow Agile methodology. Additionally, Optimizor holds two ISO accreditations: ISO 20000-1:2018 (Service Management System) and ISO 9001:2015 (Quality Management System).

8. Team Certifications

Below is a list of the technical certifications held by our engineers:

- Microsoft Certified: Azure Administrator Associate
- Microsoft 365 Certified: Messaging Administrator Associate
- Microsoft® Certified Solutions Developer: Azure Solutions Architect
- Microsoft® Certified Solutions Associate: Cloud Platform
- Microsoft® Certified Solutions Expert – Communications
- Microsoft® Certified Solutions Expert - Server Infrastructure
- Microsoft® Certified Solutions Expert – Private Cloud
- Microsoft Certified: Security, Compliance, and Identity Fundamentals
- Microsoft Certified: Identity and Access Administrator Associate
- Microsoft 365 Certified: Messaging Administrator Associate
- Microsoft Certified: Information Protection Administrator Associate
- Microsoft® Certified Solutions Associate - Server 2012

9. Services Not Covered

- Implementation, optimization, and management of core application lifecycles: browsers, antivirus, Office apps, PDF readers.
- On-premises infrastructure support: this can be discussed separately if needed.
- Hardware support for printers: we expect you to manage printers internally or use a Managed Printers service (we can recommend other partners if needed).
- Computer hardware maintenance: we do not cover hardware issues for your company's desktops or laptops. We will interact with your support provider to coordinate the device pickup process.
- Network support: we expect you to manage network devices. We will only assist end-users in connecting or managing WIFI connection issues.
- Physical facility work (e.g., moving equipment, installing televisions, etc.)

10.   Contractual Details

- **Azure Conditional Access Policies:** Focus on MFA authentication and IP restrictions.
- **Microsoft Intune Application Management:** Configured with automatic patching and requires end-user testing. For complex applications or those needing extensive testing, a separate offer may be necessary.
- **Microsoft Intune Device Management:** Includes up to 10 device configurations, device compliance, or device security policies.
- **Group Policy Management:** Limited to one standard policy for the default domain, computers, users, and servers, and up to 10 custom GPOs for specific end users.
- **User Lifecycle Automation:** Limited by the capabilities of the current HR platform and requires automatic export functionality using CSV files.
- **Power Platform Automations:** Must go through a discovery phase and are considered projects not included in the current offer.
- **Device Patching:** Scheduled at regular intervals and fully automated.
- **File Sharing Management:** Limited to managing end-user permissions. Complex migrations to modern file-sharing solutions (Azure File Share, SharePoint, OneDrive) require a discovery phase and will be treated as additional projects not included in the current offer.
- **Security Software Interaction:** Focused on monitoring normal software operation, updating central software, and implementing whitelists or restrictions for devices, IPs, or URLs. We do not provide monitoring and protection against day-to-day attacks or improvements to your security posture. These services are part of our Managed Security package – please contact us for more details.
- **Growth Adaptation:** As your company grows, we grow with you. Every 6 months, we conduct a comprehensive review of our support services and IT infrastructure to ensure your satisfaction and provide full support for your users.
- **Additional IT Processes:** Our team can manage other specific IT processes for your company, such as VPN management, cloud workload migrations, and vendor management as needed. This will be subject to a new engagement review.
- **Contract Termination:** The contract can be terminated with a 3-month' notice after the first year.
- **Annual Contract Renegotiation:** Based on the current and projected number of users, incident volume, and IT environment complexity. National socio-economic conditions (inflation, minimum wage, exchange rate, etc.) will also be considered.

II.   Project-based services (Proactive):

Optimizor provides a variety of stand-alone, project-based services to tackle specific IT challenges, whether identified by the client or discovered through our proactive assessments. These services can

be offered individually or combined into a tailored subscription package to meet the unique needs of each business. Our commitment includes delivering continuous improvement proposals and actions, enhancing the performance and security of your IT infrastructure.

1. O365 setup

We will implement a new Office 365 tenant with all necessary components: Office 365 licenses, DNS configuration, Admin roles setup, Break-glass accounts, etc.

This includes:

•   O365 license recommendations

•   O365 setup

•   DNS setup

2. Migration to a new tenant

Optimizor will assist with the following activities:

- **Physical Server Migration:** Assistance with reconfiguring Active Directory in VMWare infrastructure.
- **File Server Migration to SharePoint:** For better integration, we recommend migrating directly to SharePoint.
- **User Mailbox Migration:** Migration of 20 user mailboxes.
- **SharePoint and Teams Migration:** Full migration of SharePoint and Teams environments.
- **Computer Migration to Active Directory:** Migration of 20 computers to the new Active Directory.

3. Azure Virtual Desktop Migration

We offer the implementation of an Azure AVD Remote App Streaming solution. Technologies Covered: Azure AVD technology

Scope Limitations: This solution focuses solely on AVD Remote App Streaming and does not include a Full Desktop AVD solution.

Implementation Details

- **Discover and Analyze (20 hours):** Assess the current Citrix setup to understand load and usage patterns.
- **Design and Implement (15 hours):** Design and implement the AVD Remote App Streaming solution.
- **Test and Proof of Concept (10 hours):** Conduct testing during implementation and initiate a PoC phase with a select group of users.
- **Deploy to All Users (25 hours):** Deploy the AVD Remote App Streaming solution to all users and phase out the existing Citrix solution.
- **Post-Deployment Support (30 hours):** Provide up to 10 hours of support per month for 3 months after deployment.
- **Timeline:** The project timeline ranges from 2 weeks to 2 months, depending on the discovery phase and client engagement.

4. Antivirus Management:

- We will implement, optimize, and manage antivirus solutions: Microsoft Endpoint Protection.

We will monitor the antivirus solution to protect all client computers.

5. Email Security

We will implement core O365 email security features: external banner, SPF, DKIM, DMARC, anti-phishing, anti-spam, email quarantine.

This includes:

•   client description document which describes each feature and feature setting requiring client input

•   end-user guide: document to be shared with end-user before implementation.

6. Conditional Access

We will implement Azure conditional access, including MFA with number matching.

This includes:

•   client description document: describes each feature and feature setting requiring client input

•   end-user guide: document to be shared with end-user before implementation.

7. Azure PIM

We will implement Azure PIM to control administrative access to Office 365 and Azure.

This includes:

• O365 license requirements

• client description document: describes Azure PIM and feature setting requiring client input

• end-user guide: document to be shared with end-user before implementation.

8. Azure Entra Cloud only joined devices and Intune

We will implement Hybrid Entra cloud only computer management and required Azure settings to support this configuration.

This includes:

• Implementation steps: POC wave and final waves

• Recommended settings

• End-user guides

9. Intune Configuration Profiles

We will implement Intune computer configuration profiles, including corporate device configuration profile, BitLocker drive encryption for all drives, screen saver settings, Windows Hello for Business, Wifi configuration.

This includes:

• client description document: describes each feature and feature setting requiring client input

• end-user guide: document to be shared with end-user before implementation.

• Implementation steps: POC wave and final waves

10.   Intune Device Management:

• We will manage the lifecycle of IT devices (computers) using the Intune platform.
• We will implement, optimize, and manage system update processes using Intune Patching.

- We will implement, optimize, and manage computer configuration and security policies, including device encryption using Microsoft BitLocker.
- We will work with users/existing IT departments for the initial setup of new computers using Intune Autopilot.

11.   OneDrive User Profile Sync

We will implement Intune OneDrive User Profile sync, allowing user windows profile data to be stored in OneDrive

This includes:

•   client description document, which describes each feature and feature setting requiring client input

•   end-user guide: document to be shared with end-user before implementation.

•   Implementation steps: POC wave and final waves

12.   Intune Core App management

We will implement Intune App management focusing on core apps: TeamViewer, Office suite, Teams, Anti-virus software, Browsers, Acrobat Reader, iManage app, VPN client.

This includes:

•   client description document: describes each feature and feature setting requiring client input

•   end-user guide: document to be shared with end-user before implementation.

•   Implementation steps: POC wave and final waves

•   Investigate how to migrate Chrome user profile data

13.   Intune Autopilot

We will implement Intune Autopilot OS deployment for configuring and reconfiguring computers.

This includes:

•   client description document: naming convention and hardware purchasing requirements

•   end-user guide: document to be shared with end-user before implementation.

- Implementation steps: diagram and procedure

14.   Intune Device Patching

We will implement Intune Windows Patching rings for Windows OS computer patching.

This includes:

- client description document: patching rings including QA testing ring

- end-user guide: document to be shared with QA end-user before implementation.

15.   Defender Endpoint Protection

We will implement Intune Microsoft Defender for Endpoint Protection including basic monitoring, malware protection and attack surface reduction.

This EPIC must include:

- O365 license requirements

- client description document, which describes each feature and feature setting requiring client input

- end-user guide: document to be shared with QA end-user before implementation.

- Implementation steps: monitoring only wave and final waves

16.   Azure Cloud Printing

We will implement Azure Cloud Printing for managing network printers and access control to printers.

This includes:

- client description document: outline hardware requirements, describes each feature and feature setting requiring client input

- end-user guide: document to be shared with end-user before implementation.

17.   Entra AD DS

We will implement Azure Entra AD DS service which can be commonly used to implement WIFI Azure Entra ID integration or VPN technology integration

This includes:

•   Azure pricing

•   client description document, which describes AD DS service, costs and benefits.

•   end-user comms guide: to be shared with end-user before implementation.

•   Implementation steps: POC wave and final waves

18.   Intune MDM – Android Full Corporate devices

We will implement Intune Mobile Device Management for Android Corporate owned devices

This includes:

•   Android Enterprise account setup steps

•   Intune Configuration Profiles

•   client description document, which describes each feature and feature setting requiring client input

•   end-user guide: document to be shared with end-user before implementation.

•   Implementation steps: testing wave, PoC wave and final waves

19.   Intune MDM – iOS Full Corporate devices

EPIC to implement Intune Intune Mobile Device Management for IoS Corporate owned devices

This includes:

•   O365 license requirements

•   Apple Enterprise account setup steps

•   Intune Configuration Profiles

•   client description document, which describes each feature and feature setting requiring client input

- end-user guide: document to be shared with end-user before implementation.

- Implementation steps: testing wave, PoC wave and final waves

20. Intune MDM – Android BYOD devices

We will implement Intune Intune Mobile Device Management for Android BYOD personal devices

This includes:

- Create Intune Compliance Profiles

- client description document, which describes each feature and feature setting requiring client input

- end-user guide: document to be shared with end-user before implementation.

- Implementation steps: testing wave, PoC wave and final waves

21. Intune MDM – iOS Full BYOD devices

We will implement Intune Intune Mobile Device Management for IoS BYOD personal owned devices

This includes:

- Create Intune Compliance Profiles

- client description document, which describes each feature and feature setting requiring client input

- end-user guide: document to be shared with end-user before implementation.

- Implementation steps: testing wave, PoC wave and final waves

22. FileShare to SharePoint

We will help migrate from on-premises File Shares to SharePoint.

This includes:

- Migration license requirements

- SharePoint recommended Site structure

• Client required documentation: folder structure, folder access mapping structure (folder to Department), using Azure Entra Groups for access management

• end-user guide: document to be shared with end-user before implementation which describes SharePoint site and folder structure

• Migration steps: analysis, data migration, cut over.

23. Cloud only migration

We will help migrate on-prem computers and users to cloud-only.

This includes:

• Prerequisites: required steps to be implemented before a cloud only migration can be performed

• Client description document, which describes transformation step, end state and end-user impact.

• End-user comms guide: to be shared with end-user before implementation.

• Implementation steps: POC wave and final waves.

Optimization Services

Leveraging the power of Microsoft 365 - including SharePoint Online, Power BI, and Microsoft Power Apps - we design solutions that address clearly identified needs. The great part, since we've been doing this for some time, we have a lot of optimizations pre-built but we can develop new automation solutions specifically designed for our client's business needs.

1. Employee Registry

We will implement Employee Registry and Lifecycle automation flows: Onboarding and Offboarding.

This includes:

• O365 license requirements, KeepIT license requirements

• SharePoint IT Automation site creation

• User onboarding automation flows depending on client state (on-premises vs cloud only).

- User offboarding automation flows based on client state (on-premises vs cloud only).

2. Computer Registry

This includes:

- O365 license requirements

- SharePoint IT Automation list creation

- Computer onboarding automation flow diagram depending on client state (on-premises vs cloud only).

- Computer offboarding automation flows based on client state (on-premises vs cloud only).

3. Guest Management

This includes:

- O365 license requirements

- SharePoint IT Automation guest list requirements

- Guest management flows diagrams

- End-user guide

4. Application Registry

- O365 License Requirements: Requires an O365 license that includes access to SharePoint and advanced application management tools.
- SharePoint IT Automation Guest List Requirements: Guests who need access to the Application Registry must be listed in the SharePoint IT automation guest list.
- Guest Management Flows Diagrams: Diagram detailing how guests interact with the Application Registry, including how they access application data, link to servers, and manage support expiration dates.
- End-User Guide: Comprehensive guide for users on how to manage and update the list of applications, including linking applications to servers and managing contracts and support expirations.

5. Server Registry

In terms of who is responsible for a particular server, where various aspects are checked daily, the Server Registry (SR) includes:

- Integration with a monitoring tool to ensure server performance and security,
- Detailed records of server history and hardware specifications,
- Links to the Application Registry (AR) for tracking associated applications,
- Status of server decommissioning and other lifecycle management details.

This automation, created using SharePoint lists, serves as the equivalent of the Computer Registry for servers, ensuring comprehensive oversight without needing validation against the Entitlement Registry (ER).

6. Entitlement Registry

In terms of who is assigned to a particular computer, where various aspects are checked daily, such as:

- Integration of security tools (Intune, Microsoft Defender),
- Licensing details from the provider,
- Constraints and identification regarding who is assigned to a particular computer,

Security Upgrade Services

From analysis to ongoing support, our security upgrade process is designed to ensure your IT infrastructure is resilient against threats:

- Action plan development
- Microsoft 365 security configurations
- Infrastructure security upgrades
- Customized implementation
- Continuous improvement and industry recommendations

How it works:

Step 1: Security Assessment

We analyze your latest pen test, IT risk, and audit assessments, or conduct a detailed Microsoft security audit to pinpoint vulnerabilities and missing security controls.

Step 2: Action Plan Development

Developing a tailored plan of action, we address identified security issues leveraging Microsoft 365's security capabilities or through enhancements at the infrastructure level.

Step 3: Implementation and Testing

Upon plan approval, we meticulously implement the security upgrades and rigorously test to ensure robust defense mechanisms are in place.

Step 4: Continuous security process monitoring

Our commitment extends beyond implementation. We provide regular monitoring and proactive improvements based on the latest technology and security updates, ensuring your defenses remain strong.

IT BCP

Our approach to IT BCP, BIA, and disaster recovery relies on detailed IT assessments, strategic IT-focused planning, and ongoing enhancement to address risks and safeguard your digital operations, tools and key people.

Step 1: IT assessment & scoping

- Assess current IT people, tools and processes to identify potential IT risks and dependencies.
- Define the IT-specific scope and objectives for BCP and BIA initiatives, focusing on digital assets and technologies.

Step 2: IT risk identification & impact analysis

- Pinpoint and prioritize potential IT risks that could interrupt digital operations.
- Conduct an IT-specific BIA to evaluate how identified risks affect critical business processes.

Step 3: IT strategy development & documentation

- Craft tailored IT BCP strategies to neutralize identified risks and guarantee digital continuity.
- Clearly document IT BCP and BIA findings, strategies, and action plans, with an emphasis on technological solutions.

Step 4: Testing & validation

- Regularly execute IT BCP drills through simulation exercises and real-world IT scenarios to test digital resilience.
- Assess the effectiveness of IT BCP and BIA strategies, adjusting address new or evolving IT challenges.

Step 5: Continuous improvement & communication

- Iteratively refine IT BCP and BIA plans drawing from test results, technological advancements, and evolving IT landscapes.
- Ensure clear communication of IT BCP protocols and roles to all stakeholders, maintaining a state of continuous IT readiness.

For more information about our services and solutions, or to request a price list, please reach out to us at hello@optimizor.com or Izabela Matei, Marketing & Sales Project Manager at izabela.matei@optimizor.com . You can also contact us directly by phone at +40 740 010 686.