A SPRINGBOARD FOR SUCCESS

Advanced Specialization
Microsoft Partner
Microsoft

Cloud Security
Threat Protection
Identity and Access Management
Microsoft Azure Virtual Desktop
Information Protection and Governance
Calling for Microsoft Teams
Adoption and Change Management

Microsoft Intelligent Security Association

Microsoft

Microsoft Verified Managed XDR Solution

Microsoft Solutions Partner

Customer

Azure Done Right: Infrastructure Optimization Service

NETSURIT

Table of Contents

1 Summary of the service 3

2 Scope 4

2.1 Overview of the engagement 4

2.2 Activities in scope 4

3 Azure Managed Service Parameters 9

3.1 Managed Service Duration 9

3.2 Managed Service Staffing 9

3.3 Managed Service Hours 9

3.4 SLA and success criteria 9

3.5 Service Level Management for Managed Service 9

4 General engagement parameters 11

4.1 Assumptions 11

4.2 Dependencies 11

4.3 Azure costs 12

4.4 Microsoft Partner Association 13

5 Fees 14

5.1 Azure Optimization service fee 14

5.2 Notes on costs 14

1 Summary of the service

1. The solution should be scalable, workloads should be added and removed as and when required
2. Ensure that the workloads migrated are accessible from all sites.
3. Monitor the Solution to ensure that workloads are running within the set thresholds/budget.
4. Ensure Disaster Recovery and Backup strategies for the identified workloads are in place for business continuity purposes.
5. Meet security goals.
6. Provide the necessary analytics to give the Customer management a constant insight on the Customer Azure environment.
7. Knowledge transfer to Customer personnel.

2 Scope

2.1 Overview of the engagement

The running Azure environment will be constantly reviewed to identify opportunities to improve in parameters such as reliability, security, availability, manageability, cost-effectiveness, performance, etc. The basis of this process will be proactive monitoring, assessment, and risk identification. Additional services may be designed and implemented, or configurations changes applied. Where possible, tasks will be automated.

2.2 Activities in scope

1. Maintain standards and processes
    1.1. Perform all required tasks related to implementation of quality management, maintenance of all certified and qualified processes, process change control, reliability data analysis, failure analysis and qualification status of technologies, as mandated by Customer.
2. Azure service enhancement.
    2.1. Proactively monitor and evaluate the state of all Azure services.
    2.2. Participate in developing service enhancement plans.
    2.3. Recommend Azure service enhancements.
3. Assess the current Customer Azure infrastructure to identify the following:
    3.1. Suitability of the infrastructure meeting current and future business requirements.
    3.2. Configurations that may lead to operational inefficiency, excessive costs inadequate performance or security risks.
    3.3. Operational processes that are not adequate for current or future requirements.
    3.4. Alignment to the recommendations contained in the Azure Cloud Adoption Framework (CAF) and Azure Well-Architected Framework (WAF).
4. Review application architecture for new apps or proposed changes to apps, to identify potential risks that may impact security, performance, reliability, cost or functionality; recommend changes to architecture or implementation plans to improve outcomes.
5. At the initiation of the engagement, perform a Well Architected Review of the entire Azure environment, against all five pillars of the Microsoft Azure WAF.
6. Implement custom reports, dashboards, and workbooks, to improve visibility of the state of Azure resources for required stakeholders.

7. Implement enhancements to management and governance of the Customer Azure environment including the following:
    7.1. Enhanced Role Based Access Control (RBAC).
    7.2. Intensive use of Azure policies for enforcing compliance with required settings and controls.
    7.3. Template based (ARM, Bicep, etc.) deployment of Azure resources utilising Azure DevOps or other Infrastructure-as-Code technologies.
    7.4. Optimized network configuration to improve performance, availability, reliability, and security.
    7.5. Enhanced monitoring based on Azure Monitor and other technologies.
    7.6. Extending Azure management tools to the on-premises environment using Azure Arc.
    7.7. Enhanced security monitoring and management based on Azure Sentinel and Microsoft Defender for Cloud.
    7.8. Proactive cost management.
    7.9. Enforced tagging to facilitate improved reporting.
8. Automation
    8.1. Identify common Azure operational procedures and tasks that can benefit from automation.
    8.2. Develop or find automation scripts.
    8.3. Automate execution of scripts using Azure Automation, Logic Apps, Azure Monitor alerts etc.
    8.4. Document Azure automation procedures.

9. Integration with IT Service Management (ITSM) systems (if this exists)
    9.1. As part of the optimisation component of the service, the team will work with the owners of the existing ITSM system in Customer to enable as much integration as possible.
    9.2. The goal will be to implement two-way integration, so that an alert/incident on the Azure side, as detected by e.g., Azure Monitor, will cause an incident ("ticket") to be logged in the ITSM system, for allocation to resolvers and tracking. Similarly, when an incident is closed on the ITSM system, the status should be written back to the monitoring system in Azure.
    9.3. Another goal should be to ensure that existing Configuration Management Database (CMDB) systems are automatically updated with information about Azure resources.
10. Review and enhance security of the Azure environment.
    10.1. Ongoing assessment of the security state of existing Azure services and workloads.
    10.2. Identify Azure resources whose security configuration does not comply with Microsoft recommendations.
    10.3. Develop a plan for remediating identified security risks and issues.
    10.4. Work with the SOC and other operational support teams to perform remediation of identified security risks and issues.
    10.5. Interaction with the SOC and other operational support teams to resolve security risks and incidents.

11. Review application development, deployment, and lifecycle management practices, to identify security risks or opportunities to enhance security by implementing DevSecOps practices or tools. Assist with implementation of DevSecOps tools and processes.
12. Implement and configure Azure security workloads

    Work with security architects and other operational teams to implement and configure security-specific workloads in the Customer Azure environment, in accordance with security designs and standards; this may include the following:

    12.1. Microsoft Defender for Cloud (including workload protection features)
    12.2. Microsoft Defender External Attack Surface Management (MDEASM)
    12.3. Microsoft Defender Threat and Vulnerability Management
    12.4. Azure Key Vault
    12.5. Azure Policy
    12.6. Network Security Groups
    12.7. Azure Firewall
    12.8. Azure Web Application Firewall (WAF)
    12.9. Azure Front Door integrated with WAF
    12.10. Azure App Gateway integrated with WAF
    12.11. Azure DDoS protection
    12.12. Azure Bastion
13. Implement and configure Microsoft Entra security features to enhance Azure security Work with security architects, the SOC (if this exists) and other operational teams to implement and configure security-specific workloads in the Customer Azure environment, in accordance with security designs and standards; this may include the following:

    13.1. Entra ID Privileged Identity Management (PIM)
    13.2. Entra ID Conditional Access Policies
    13.3. Entra Permissions Management
14. Maintain an operations guide describing the following:

    14.1. List of common operational tasks required to support the Azure services and workloads.
    14.2. Operations calendar specifying tasks to be performed on a daily, weekly, and monthly basis.
    14.3. Procedures for common operational tasks

15. Maintain and update the design and operations documents for the Azure environment to accommodate changes.

3 Azure Managed Service Parameters

3.1 Managed Service Duration

This proposal is based on a 1-month agreement.

3.2 Managed Service Staffing

1. Netsurit will determine the staffing requirements to support Customer.
2. The service will be staffed using shared services provided by Netsurit.
3. Service desk services will be provided 8x5.
4. Remote monitoring and incident response will be provided 8x5.

3.3 Managed Service Hours

Service Hours	Service Hours refers to the time when the service staff are available to react immediately to incidents logged.

The current proposal is based on the following service hours:

1. Service Desk: 8 Hours a day, 5 days a week, Monday to Friday.
2. Remote support: 8 Hours a day, 5 days a week, Monday to Friday.
3. Remote monitoring and incident response: 8 Hours a day, 5 days a week, Monday to Friday.

3.4 SLA and success criteria

This engagement does not imply a Service Level Agreement (SLA).

3.5 Service Level Management for Managed Service

By firstly stabilising your IT, then by executing on agreed upon project initiatives, it gives capacity for IT management to play a more innovative and strategic role in the business. Strategic input from IT allows agility and support for increased paths to business (scalability, staff empowerment, new products, innovation, and competitiveness).

A Netsurit service manager will be assigned to Customer. The service delivery manager will act as a communications channel between Customer management and the Netsurit services; The objective of this service component is to ensure the managed services are providing the required value and identify opportunities to improve the service.

The responsibilities of the Netsurit service manager include the following:

- Monitor service delivery as part of this engagement.
- Identify risks or issues that may impact the quality-of-service.
- Work with the Netsurit delivery team and the customer to eliminate or mitigate issues impacting service delivery effectiveness.
- Provide feedback to client management.
- Act as a conduit to facilitate effective communication between the Netsurit delivery team and the customer.
- Create and track schedules for planned activities.
- Verify that planned activities are completed on time and on specification.
- Verify that scheduled document deliverables are provided to the specified recipients on time.
- Act as an escalation point for issues reported by the customer.
- Schedule and attend update meetings between the Netsurit delivery team and the customer.

4 General engagement parameters

4.1 Assumptions

1. All required cloud services subscriptions will be provided by Customer.
2. Internet connectivity will be available for all devices.

4.2 Dependencies

This solution proposal is based on the following pre-requisites being met:

1. Customer will provide Azure Monitor workspaces in Azure.
2. The project team must be delegated the Owner role on the Azure subscriptions to be managed.
3. All pre-requisites for Microsoft cloud services must be met, including hardware, software, network, and firewalls.
4. A primary contact or liaison person at Customer to which status feedback can be given along with resolving any matters which could cause the engagement to be delayed.
5. Reasonable Internet access on the Customer network for the members of the project team.
6. Creation of required service accounts and delegation of permissions in the Customer Group on-premises AD forest or other required services.

4.3 Azure costs

1. The Azure Management or Azure Optimization services are provided on a BYOL (Bring Your Own License) model.
2. All costs for Azure resources deployed in the Customer Azure subscriptions will be paid for by Customer directly to Microsoft.
3. Netsurit will not provide any software licenses or subscriptions for use by this engagement.
4. Licenses or subscriptions needed to deliver the Azure Management or Azure Optimization service will be aid for by Customer out of their own Azure or other Microsoft subscriptions.
    4.1. At a minimum, Customer will have to provide licenses for two Netsurit administrators, covering the following products:
        4.1.1. Entra ID P2
        4.1.2. Power BI Pro
        4.1.3. Exchange Online
5. Netsurit will provide estimates of subscription costs for any Azure resources it intends to deploy.
6. Customer must approve implementation of new Azure resources that will have a cost implication.
7. Netsurit cannot be held accountable for reduced management or security functionality if Customer does not approve costs for recommended resources.

4.4 Microsoft Partner Association

1. Customer will associate Netsurit to the Azure resources used in this engagement through the Partner Admin Link (PAL) association.
    1.1. Microsoft partners provide services that help customers achieve business and mission objectives using Microsoft products. When acting on behalf of the customer managing, configuring, and supporting Azure services, the partner users will need access to the customer's environment. Using Partner Admin Link (PAL), partners can associate their partner network ID with the credentials used for service delivery.
    1.2. PAL enables Microsoft to identify and recognize partners who drive Azure customer success. Microsoft can attribute influence and Azure consumed revenue to the partner organization.
    1.3. If other Microsoft partners are working in the same customer environment, more than one partner can PAL against Azure resources.
2. Microsoft uses the Claiming Partner of Record (CPOR) model to manage the associations partners have with Microsoft 365 tenants. Customer needs to confirm the CPOR status for any Microsoft 365, Microsoft 365 Defender or Microsoft Purview workloads that Netsurit may implement as part of this engagement.

5 Fees

5.1 Azure Optimization service fee

The Azure optimization service will be delivered for a fixed fee per month by Netsurit Professional Services.

Netsurit will provide the following services for a period of 1 month:

Service components	Hours per month	Cost per month (ZAR Incl. VAT)
Azure Optimization Service	40	R69 000,00
Total per month (ZAR incl. VAT)		**R69 000,00**

5.2 Notes on costs

1. The listed amounts include VAT unless explicitly specified otherwise.
2. The offer will be paid for in advance on the Azure Market Place.
3. Netsurit reserves the right to stop work on the project should invoices not be paid within the agreed time frames.