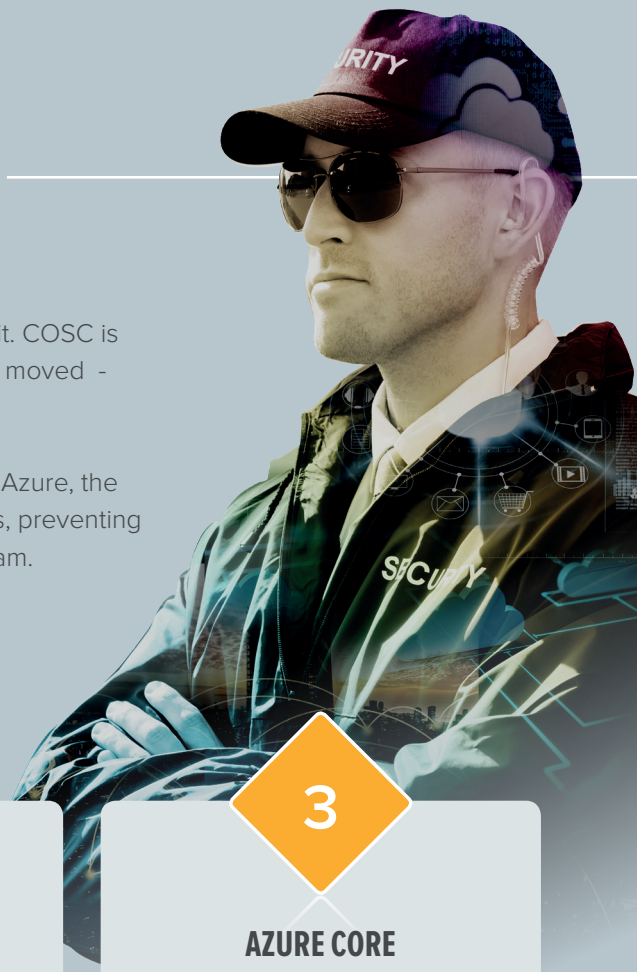
TO SERVE AND PROTECT.

CLOUD OPERATIONS AND SECURITY CENTRE.



Introducing the Cloud Operations and Security Centre (COSC) from Netsurit. COSC is designed to provide pro-active remote assistance for customers who have moved - or are in the process of moving – into the cloud.

With a focus on Microsoft Office 365, Enterprise + Mobility Suite (EMS) and Azure, the COSC specialises in proactive maintenance and prevention. In other words, preventing problems before they occur. The COSC is run by a highly skilled central team.

WHAT COSC OFFERS

1

MICROSOFT 365 TENANT ADMINISTRATION SERVICE

Ongoing administration and management of the Office 365* productivity suite (outlook, Word, Excel, PowerPoint, Access, OneNote, team SharePoint site, online meeting room with HD video and screen sharing capability.

2

MICROSOFT SECURITY ADMINISTRATION SERVICE

With cyber threats becoming increasingly sophisticated, the window between an initial compromise and a full-scale attack is shrinking from months to hours. A lot of companies cannot afford this risk. Having this service in a central facility allows for the cost to be shared and significantly reduced.

3

AZURE CORE ADMINISTRATION SERVICE

Customers often make use of their own applications, which allows for flexibility but increases complexity. Customers with their own applications such as ERP, HR programs and Operations benefit as Netsurit will run them through Azure* and manage them through COSC. Once again, reducing cost and increasing efficiency.

SERVICE TIERS

Each of these services will be offered in 3 tiers:

GOLD

Monitoring, maintenance and service enhancement. COSC will proactively monitor, manage, maintain and action everything for its customers.

Services will be priced on a per-user basis for Office 365 services and per-workload for Azure services.

SILVER

Monitoring and maintenance only. COSC will proactively monitor our customers' systems and advise if action should be taken.

BRONZE

Monitoring only. Netsurit will monitor from COSC and supply customers with reports through dashboards and information services.

*Customers are responsible for their own M365 and Azure licensing.

netsurit inobits

SUPPORTING THE DREAMS OF THE DOERS

AZURE CORE ADMINISTRATION SERVICES

AZURE SERVICE ENHANCEMENT

- Proactively monitor and evaluate the state of all Azure services.
- Implement service enhancements.

MANAGE DELEGATION AND ADMIN ROLES IN AZURE

- Provide a facility to query and modify delegations in Azure.
- Receive and evaluate requests for new administrators.
- Assign users to administrative roles.
- Design and implement custom administrative roles.
- Provide periodic reports.

INVESTIGATE SECURITY REQUIREMENTS AND CAPABILITIES IN AZURE SERVICES

- Cost containment
- Excess Capacity
- Containment

MANAGE INTEGRATION WITH IDENTITY AND AUTHENTICATION SERVICES

- Ensure required changes are made to resolve directory synchronization.
- Analyse standard reports and make recommendation where relevant.
- Delegate the appropriate roles to pull built-in reports.

MONITOR AZURE USING AZURE MONITOR

- Assist Customer support teams with logging of support calls to Microsoft Premier Support Services for issues relating to the security of the Azure tenant and subscriptions.

AZURE REPORTING

- Workload-related services.
- Configure customised monitoring of networks, applications and on-premises workloads.
- Team proactively implements changes based on Azure Monitor findings.
- Provide reports, alerts and recommendations.

PROACTIVELY MONITOR AZURE SECURITY STATUS

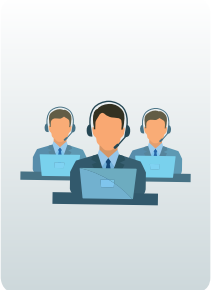
- Forward and review of security alerts and reports generated by the Azure Security Centre, Azure Identity Protection, Azure Monitor and other related services.
- Notify appropriate customer operational teams of security incidents and issues, and resolve accordingly.
- Provide recommendations to customer for potential changes to infrastructure configuration, policies and operational processes.

MANAGEMENT AND ENHANCEMENT OF AZURE SECURITY STATE

- Implementation of changes to enhance security.
- Interaction with operational support teams to resolve security risks and incidents.
- Documentation of findings and recommendations.
- Develop and update a monthly Security State Report.

CREATE RESOURCES FOR NEW AZURE SERVICES

- Create new Azure subscriptions, resource groups and management groups.
- Create Azure network components.
- Create JSON templates for new Azure resources.



COLLABORATE WITH OTHER SUPPORT TEAMS

- Work with other support teams who focus on admin of specific Azure services, as well as related on-premises services.
- Receive, evaluate and execute requests for changes and other activities performed.

ACCOUNT MANAGEMENT – DEDICATED PERSON

BUT WAIT, THERE'S MORE!

Space prevents us from going into more detail on these and all the other services we offer.
For more information, please contact **solutions@netsurit.com**

netsurit inobits
SUPPORTING THE DREAMS OF THE DOERS

SECURITY ADMINISTRATION SERVICES

SECURITY INCIDENT INVESTIGATION AND REMEDIATION

- Identify new Office 365 services that are not yet fully deployed in production in customer environment; e.g., Teams, Planner, Sway, Video, PowerApps, Flow and Delve.
- Identify and document security and access requirements for new Office 365 services and data.
- Verify configuration and operational procedures for all Office 365 services comply with security requirements and policies.

MICROSOFT 365 SECURITY ENHANCEMENT

- Ongoing assessment of the security state of the Customer's Microsoft 365 infrastructure.
- Monitor the Microsoft Secure Score rating for the Customer's Office 365 tenant; evaluate the findings and recommendations provided by the tool.
- Documentation of findings and recommendations.

SECURITY ALERT MANAGEMENT

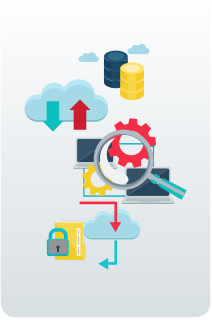
- Daily - review alerts sent by Microsoft.
- Forward alerts to other operational teams if action is required.
- Initiate any required remedial action to resolve alerts.

IDENTITY SERVICES MONITORING AND MANAGEMENT

- Monitor on-premises identity services that integrate with Office 365.
- This will include enforcing security standards and policies and assisting with the implementation of any required security-related configuration changes.
- This will include managing the Multi Factor Authentication (MFA) functionality in Azure AD and Office 365, the Self-Service Password Reset (SSPR) service and Azure AD application integration.

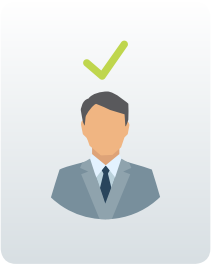
SECURITY FOCUSSED REPORTS

- Gather requirements for which security-related reports are needed by whom.
- Ensure that authorised users who need frequent access to Office 365 or Azure AD reports are delegated the appropriate roles to be able to pull built-in reports.
- Where users are not able to access required reports themselves, the tenant security operations team should configure periodic scheduled generation of reports or data exports, and then provide the reports to users by indirect means, e.g. e-mail or publishing to SharePoint Online sites.



MONITORING, MANAGEMENT AND ADMINISTRATION OF M365 SECURITY SERVICES

- Develop and document procedures to monitor the Customer Office 365 tenant and related services.
- On an ongoing basis, use available Microsoft tools to monitor the Customer Office 365 tenant and related services.
- Respond to all security alerts generated by monitoring tools, relating to Office 365 security.



MANAGE DELEGATION OF RIGHTS ON OFFICE 365 TENANT AND SERVICES

- Receive and evaluate requests for new administrators to be assigned membership of administrative roles in the tenant.
- Approve requests that comply with requirements and policies.

CALL LOGGING WITH MICROSOFT

- Assist Customer support teams with logging of support calls to Microsoft Premier Support Services for issues relating to the security of the Office 365 tenant and services.

ACCOUNT MANAGEMENT – DEDICATED PERSON

BUT WAIT, THERE'S MORE!

Space prevents us from going into more detail on these and all the other services we offer.
For more information, please contact **solutions@netsurit.com**

netsurit inobits
SUPPORTING THE DREAMS OF THE DOERS