Managed Services Environment Security

We are
The NAV People
The 365 People

Table of Contents

Overview

Security vulnerabilities from equipment to facilities in a business can range from open ports, to outdated patches to physical locations.

Security in today's IT infrastructure is absolutely critical and success is more about layers than a single point of defence. Protecting the outer layer of the network as well as a strong Security Endpoint and Antimalware solution are important for this success.

In this document, you will find information about how The NAV People & The 365 People deal with the security of the Managed Services environment.

Physical security

All components of the Managed Services offering are hosted in the Microsoft Azure Cloud. Azure helps provide a highly secure foundation, built from the ground up, to host the infrastructure, applications and data. Microsoft has invested over a billion dollars in security, including the physical security of the Azure platform, and it includes the most comprehensive portfolio of internationally-recognised standards and certifications.

Local network security

A local network is understood as being local on The NAV People & The 365 People Managed Services Azure infrastructure. The NAV People & The 365 People use Windows Networking as the core security platform and all servers use Windows Server 2012 or the newer version of Windows Server installed and patched by Microsoft.

User-level security management is undertaken using Active Directory where appropriate or Local Security accounts. There are multiple levels of security and a layered approach to secure each customers area ensuring data which belongs to a customer cannot be accessed by any other customer.

Infrastructure management

There are multiple servers, applications and underlying infrastructure that is shared across installations on The NAV People & The 365 People's Managed Services infrastructure. These resources support general needs including and not limited to:

- Shared SQL Servers
- Active Directory
- Automation accounts
- Monitoring tools
- Azure Security Centre

All servers can be accessed by dedicated Customer and The NAV People & The 365 People users. All critical endpoints are configured to be accessible from dedicated IPs, such as The NAV People & The 365 People or Customer offices using IP filtering technologies.

Network external access

Access to the Azure network is managed using the Azure Network Security (NSG) groups. The NSG can limit the traffic to resources in a virtual network. Access control security rules are applied by default to each endpoint to deny any inbound network traffic. The endpoints that require inbound network traffic are only open by Customer requests or as part of the service provisioning rules.

DDoS protection

Distributed Denial of Service (DDoS) attacks are one of the biggest security concerns facing customers who are moving their applications to the cloud. A DDoS attack attempts to exhaust an application's resources, making the application unavailable to legitimate users. DDoS attacks can be targeted at any endpoint that is publicly accessible through the Internet.

Customers of The NAV People & The 365 People Managed Services benefit from the Azure DDoS Protection. This is part of the platform, at no additional charge. Always-on traffic monitoring and real-time mitigation of common network-level attacks provide the same defence utilised by Microsoft's online services.

Data protection, in transit, at rest

The NAV People & The 365 People Managed Services environments are created by default under The NAV People & The 365 People's own domain and contain a matching security certificate. Every Dynamics NAV endpoint has SSL enabled for all the available services, e.g. Windows Client, SOAP, OData and Web Client. The data transfer between the client and the server running in Azure is encrypted using the security certificate.

The NAV People & The 365 People Managed Services infrastructure uses the Azure Storage Service Encryption for data at rest. With this feature, all the components used by the service to store data are automatically encrypted. The handling of encryption, encryption at rest, decryption, and key management in the Storage Service Encryption is automated, transparent and without impact to users. All data written to Azure Storage is encrypted through 256-bit AES Encryption, one of the strongest block ciphers available.

All services where Azure SQL databases are used also benefit from the transparent data encryption. Transparent data encryption helps protect Azure SQL Databases against the threat of malicious activity. It performs real-time encryption and decryption of the database, associated backups, and transactional log files at rest.

Continuous security assessment

Azure Security Centre is the core service employed by The NAV People & The 365 People Managed Services to provide a unified security management and advanced threat protection across all the environment workloads.

The Azure Security Centre helps the Managed Services team to monitor, prevent and remediate security vulnerabilities of machines, networks, storage and data services.

The continuous security assessment performed by the service discovers potential security issues, such as systems missing security updates, unsecured and exposed network ports. The team uses this information during the detect, assess and diagnose stages to successfully respond and mitigate any incidents.

More info on the services used can be found here:

Azure Certifications

Azure Security Centre

Azure Security Groups

Azure Storage Service Encryption

Transparent data encryption for SQL Databases