NODE4

SECURITY FUNDAMENTALS WITH MICROSOFT 365

SECURING YOUR CLOUD SECURITY WITH NODE4 AND MICROSOFT 365

The “Security Fundamentals with Microsoft 365” package is tailored to raise the baseline security profile of your organisation using core technologies widely adopted by businesses around the world. Our goal is to help you achieve a level of security that protects your data, devices, and identity from ever-evolving threats.

The package helps businesses meet the requirements that are becoming the entry level for Cyber Insurance, ensuring that data is protected and that policy clauses are being met.

With this package, you can leverage the power of Microsoft 365 security features, such as Entra ID, Conditional Access, Multi-factor Authentication and Intune, and address third-party patching using Patch My PC.

The package will ensure that all staff and devices are protected by multi-factor authentication, that all business data is encrypted and that all critical software vulnerabilities are quickly patched.

Node4 will work with you to assess your current usage and configuration of Microsoft 365 security features. The impact of adopting enhanced security practices will be reviewed, resulting in a Solution Configuration Document and Test Plan unique to your requirements.

Each new configuration will then be applied by our Microsoft certified, UK based consultant team. The Test Plan and subsequent training will ensure that all changes work as designed and that internal IT resources understand the day-to-day tasks following completion of the engagement.

Key Features:

- Meet the requirements of Cyber Insurance policies whilst enhancing the overall security of the organisation.
- Increase ROI for the existing Microsoft 365 estate by lighting up non-configured services to improve your security posture.
- Protect Business Data on Personal Devices
- Provide flexibility for staff with a BYOD policy whilst remaining in control of business data.
- Training and support for your staff and IT team on how to use and manage the new security features.
- Fully managed project from a Microsoft certified, UK based team delivering class leading technical excellence

These benefits showcase how Microsoft Intune, Entra ID and Patch My PC can be pivotal tools in managing and securing an organisation's users, devices, and apps, aligning with the needs of a modern workforce.

Unified Endpoint Management: Microsoft Intune provides a comprehensive solution for managing apps and devices across various platforms, including Android, iOS, Windows, and macOS. It simplifies the management of both corporate-owned and personal devices, ensuring secure access to organizational resources.

Security and Compliance: Intune enhances security by allowing administrators to set and enforce policies across devices and apps. It supports the Zero Trust security model, ensuring that only compliant devices can access sensitive data, thus maintaining the organization's compliance posture.

Flexible App Management: With Intune, businesses can deploy, update, and remove apps seamlessly. It supports a range of app types, including Microsoft 365 apps, Win32, and line-of-business (LOB) apps, providing a built-in app experience that protects data within apps.

Device Enrolment Options: Intune offers various enrolment options to suit different business needs. Automatic enrolment for seamless integration, bulk enrolment for efficiency, and user-driven enrolment for flexibility are all available, making device management more streamlined.

Access Control: Administrators can define detailed access controls, including the ability to allow or deny user access to specific apps or URLs. This granular control helps prevent unauthorized access to company information and reduces the risk of data breaches.

Cloud-native Solution: As a cloud-based service, Intune allows employees to work from anywhere, on any device. This flexibility is crucial for supporting modern work environments that are increasingly mobile and remote.

Cost-Effective: By centralising the management of devices and apps, Intune reduces the need for multiple management tools, which can lead to significant cost savings for organisations. It also minimizes the need for manual interventions, further reducing operational costs.

Policy Automation: Intune automates the deployment of policies for security, device configuration, and compliance. This automation ensures that policies are consistently applied across the organisation, reducing the potential for human error.

Integration with Microsoft Ecosystem: Intune integrates seamlessly with other Microsoft services and apps, providing a cohesive experience for users and simplifying the management for IT administrators.

Data Protection Without Enrolment: For organisations that do not require full device management, Intune offers app protection policies that secure data on unmanaged devices. This feature is particularly useful for BYOD scenarios where full control over personal devices is not feasible.

Entra ID: With Entra, you can implement consistent security policies for all users, apps, devices, and workloads, ensuring least privilege access and maintaining compliance. Its user-friendly interface reduces IT friction and enhances the hybrid workforce experience with seamless access, single sign-on, and automated lifecycle workflows.

Conditional Access: Conditional Access is a tool within Microsoft Entra that allows organizations to implement automated access control decisions for accessing their cloud apps, based on conditions. It is a critical component of a Zero Trust strategy, providing granular security controls based on user, location, device state, and behavior. Conditional Access policies help protect against threats by ensuring that only trusted users and devices can access sensitive information.

Patch My PC: Patch My PC simplifies the process of updating third-party software, reducing the security risks associated with outdated applications. It offers an extensive catalogue of updates for common enterprise software, which can be deployed automatically through Microsoft Intune. This ensures that all devices within an organisation are running the latest and most secure software versions, thereby minimising vulnerabilities and enhancing overall security posture.