datanetworks

SECURITY, COMPLIANCE, & IDENTITY

Microsoft Solutions from **Data Networks**.

Protect user identities and data, guard against threats, and secure your environment.

The current digital security landscape can accurately be described in one word: complicated. There are an escalated number of advanced threats, more nebulous and complex compliance requirements, and more difficult infrastructure to secure. Simply put, keeping data, workloads, and users secure is more than a full-time job - but Data Networks can help you keep up.

Our Security, Compliance, & Indentity Microsoft Solutions ensure enterprise clients are secured and help your organization effectively handle patching, malware threats, and intrusion detection.

Our Security, Compliance, & Identity Microsoft Solutions services include capabilities for:

- Identity & Access Management
- Threat Protection
- Information Protection
- Security Management
- Compliance

Microsoft Partner
Microsoft

Gold Messaging
Gold Cloud Productivity
Silver Collaboration and Content
Silver Datacenter
Silver Windows and Devices

Data Networks is a leading Microsoft Gold Certified Partner and Microsoft Cloud Solution Provider (CSP).

COMPETENCIES

- Gold Messaging
- Gold Cloud Productivity
- Silver Collaboration & Content
- Silver Datacenter
- Silver Windows & Devices

CLOUD SOLUTION PROVIDER

As a Cloud Solution Provider, Data Networks can directly manage your entire Microsoft cloud lifecycle, including provision, management, and support of your Microsoft subscriptions.

Learn more online at **datanetworks.com/solution/microsoft-solutions/**

Identity & Access Management

Manage identities, access controls, and stop breaches before they escalate.

Increased threats in the cybersecurity landscape means organizations are under more regulatory pressure than ever to protect access to sensitive data and resources. An effective Identity & Access Management solution enables your organization to initiate, capture, record, and manage user identities and their related access permissions in an automated manner. We use behavioral analysis to provide actionable insights to ensure you have a sound approach to manage your users and groups, as well as secure access to on-premises and cloud applications.

Safeguard and Manage Identities

When moving to the cloud, security boundaries between different parts of sensitive data are important to preserve. Keep your users' identities and data secure by implementing Azure Key Vault, a centralized service for storing sensitive application data. Using a key vault to securely store sensitive data allows you to logically isolate the data you are storing. Each key vault is a collection of cryptographic keys and cryptographically protected data (known as secrets), and the key vault controls access to the keys and secrets. Data Networks' expert Microsoft engineers can implement Azure Key Vault to keep your organization's user IDs and sensitive data secure.

- Azure Key Vault - cloud service for securely storing and accessing secrets

Detect and Respond to Identity-Based Threats

With identity-based attacks on the rise, organizations require the ability to detect when attackers exploit, misuse, or steal enterprise identities. Given the penchant for attackers to use credentials and leverage Active Directory (AD), it is now more critical than ever to detect identity-based activity by protecting credentials, privileges, cloud entitlements, and the systems that manage them.

Our team can design your identity-based threat response using solutions that leverage your on-premises Active Directory signals to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization.

- Microsoft Defender for Identity – an on-premises platform that leverages on-premises Active Directory signals to help protect your organization from advanced targeted attacks by automatically analyzing, learning, and identifying normal and abnormal entity behavior.
- Microsoft Defender for Cloud Apps – brings the security capabilities traditionally available to on-premises systems to SaaS cloud applications like Dropbox, Office 365, G Suite, and Salesforce. It enables deeper visibility, comprehensive controls, and enhanced protection against cloud security issues.

Protect Against Password Attacks

Help protect your organization against breaches due to lost or stolen credentials by implementing a strong authentication method.
Password attacks are among the most common threats to any organization. From brute-force to social engineering to dictionary attacks, there are countless methods attackers use to obtain your users' passwords. The best way to reduce password vulnerabilities and keep your data safe is to eliminate passwords entirely with solutions like Windows Hello, which allows users to sign in using biometrics.

Get started by enabling Multi-Factor Authentication (MFA) across all your accounts, which requires users to sign in with at least two authentication factors: something they know (like a password or PIN), something they are (such as biometrics), and/or something they have (such as a trusted device).

- Windows Hello – a reliable, fully integrated biometric authentication based on facial recognition or fingerprint matching.
- Multi-Factor Authentication (MFA) – adds a layer of protection to the sign-in process by requiring users to provide additional identity verification, such as scanning a fingerprint or entering a code received by their phone.
- Windows Defender Credential Guard – prevents attackers from being able to retrieve credentials from operating system memory by maintaining them in a virtualized environment that is only accessible by privileged system software and is not directly accessible by privileged users.

Threat Protection

Proactively guard against threats, identify breaches, and respond to attacks.

For even the most adept IT and incident response teams, effectively handling patching, malware threats, and intrusion detection can be cumbersome to manage. An effective Threat Protection solution enables your organization to remain constantly aware of the current landscape and identify attackers – and the attacks they are using – before they cause damage.

Protect Against Malware Attacks

Modern malware comes in a bewildering variety of forms, from computer viruses to worms to spyware. With so much of our lives spent online, and crucial files stored on our devices, it's important to have protection against viruses that can wreak havoc. In addition to personal vigilance and not opening suspicious links from unfamiliar or impersonating email accounts, protecting against malware attacks requires protective tools, such as Microsoft Defender and Windows Defender Device Guard. These tools constantly search and defend against security threats:

- Microsoft Defender Antivirus – an antivirus protection program that offers tracking prevention to help manage how websites track your data, routinely updates, and has a password generator and monitor that informs you if any of your passwords have been compromised.
- Windows Defender Device Guard – a security feature designed to use application whitelisting and code integrity policies to protect users' devices from malicious code that could compromise the operating system.

Manage Mobile Devices and Applications

Organizations and their workforces rely on mobile devices like smartphones, tablets, and laptops to complete their jobs. Since working remotely has become the new normal, mobile devices have become vital tools for productivity and efficiency. With these mobile devices accessing critical business data, they can threaten security if hacked, stolen, or lost. Protect your organizational data by implementing a mobile device management strategy leveraging modern capabilities such as Microsoft Endpoint Manager and Microsoft Enterprise Mobility + Security (EMS).

- Microsoft Endpoint Manager – a cloud-based service that helps provide endpoint security, device management, and intelligent cloud actions within a unified management platform by leveraging Microsoft Intune and Configuration Manager.
- Microsoft Enterprise Mobility + Security (EMS) – provides an identity-driven mobile device security solution that offers a holistic approach leveraging a suite of security products, including Azure Active Directory, Microsoft Intune, Azure Information Protection, Microsoft Cloud App Security, Microsoft Advanced Threat Analytics, and Azure Advanced Threat Protection.

Security Management

Increase your resilience to protect against threats due to internal vulnerabilities.

Within the context of an organization's security program, the concept of "threat detection" is multifaceted, and even the best security programs must plan for worst-case scenarios when someone or something has slipped past defensive barriers and becomes a threat. Identify and mitigate potential threats to your organization due to breaches, misconfigurations, authentication misuse, loss of sensitive data, and other weaknesses by employing a security management solution.

Detect and Respond to Threats

Detect and properly neutralize threats before they can exploit any present vulnerabilities with Microsoft solutions that analyze the entirety of your security ecosystem to identify any malicious activity that could compromise your network.

- Microsoft Sentinel – delivers intelligent security analytics and threat intelligence across the enterprise, providing a single solution for attack detection, threat visibility, proactive hunting, and threat response.
- Microsoft Defender for Cloud – strengthens the security posture of cloud resources and protects workloads running in Azure, hybrid, and other cloud platforms.
- Azure Advisor – provides recommendations based on your deployed Azure services configuration so you can enhance and refine your Azure services' cost, security, reliability, operational excellence, and performance.
- Microsoft Defender for Endpoint – delivers preventative protection, post-breach detection, automated investigation, and response.

Protect Against Threats

Strengthen your security posture, protect against evolving threats, and continuously monitor and assess your security state across Azure, other clouds, and on-premises environments with Microsoft solutions that provide visibility into your virtual networks and can detect a wide variety of threats targeting your infrastructure.

- Windows Server – uses transparent data encryption with Microsoft SQL Server to protect data at rest with real-time I/O encryption and decryption of data and log files.

- Microsoft Defender for Cloud – strengthens the security posture of cloud resources and protects workloads running in Azure, hybrid, and other cloud platforms.
- Microsoft Defender for Endpoint – delivers preventative protection, post-breach detection, automated investigation, and response.

Gain Visibility into Security Health

Keep tabs on your network's security with the monitoring capabilities built in to the Azure platform to triage false positives from real alerts, proactively act upon real alerts, and monitor application performance and operation health. Our team can help setup the dashboards and reports on your network's system health that provide the most meaningful and valuable information to your organization.

- Microsoft Sentinel – delivers intelligent security analytics and threat intelligence across the enterprise, providing a single solution for attack detection, threat visibility, proactive hunting, and threat response.
- Microsoft Defender for Cloud – strengthens the security posture of cloud resources and protects workloads running in Azure, hybrid, and other cloud platforms.
- Azure Network Watcher – provides tools to monitor, diagnose, view metrics, and enable or disable logs for resources in an Azure virtual network.
- Azure Monitor – collects, analyzes, and acts on telemetry data from your Azure and on-premises environments.
- Microsoft Secure Score – uses intelligent insights and guidance to strengthen your security posture.
- Microsoft 365 Defender – analyzes threat data across domains and builds a complete picture of each attack in a single dashboard.
- Microsoft Cloud App Security – provides rich visibility, control over data, and sophisticated analytics to identify and combat cyberthreats across all Microsoft and third-party cloud services.