2025

MICROSOFT DYNAMICS 365

SECURITY CHECKLIST

Contents

DATA PROTECTION & CLASSIFICATION *(Microsoft Purview & DLP)*

1. Enable Microsoft Purview classification and labeling across Dataverse entities and D365 apps

D365 FO?
Partially – D365 FO does not use Dataverse natively, unlike model-driven Power Apps like D365 Sales or Customer Service.

- D365 FO data is not stored in Dataverse by default, so native Microsoft Purview classification and labeling does not apply directly.
- However, if you are using Virtual Entities or exporting D365 FO data to Dataverse or via Synapse Link, Purview can classify that data.
- Integration is possible via Azure Synapse Analytics or data lakes.

Verdict: Limited direct support. Requires integration.

2. Define and apply sensitivity labels (e.g., "Confidential – Finance")

D365 FO?
Not directly in FO forms or data fields.

- Sensitivity labels (from Microsoft Purview or MIP) are primarily used in Microsoft 365 apps (Word, Excel, Outlook, Teams).
- Indirect support:
    - If data from D365 FO is exported to Excel or PDFs, and you have sensitivity labels configured in Microsoft 365, then they can be applied at the document level.
    - Email notifications from workflows in D365 FO can inherit labels via Outlook policies.

Verdict: Not natively in FO, but applicable via Microsoft 365 integrations.

3. Create and enforce DLP policies for PII, PHI, and financial data in D365, Outlook, Teams, and SharePoint

D365 FO?
Only partially applies to D365 FO.

- DLP policies in Microsoft 365 compliance center cover:
    - Email (Exchange)
    - Teams
    - SharePoint
    - Dataverse-based apps
- D365 FO is not natively integrated with Microsoft DLP, but:
    - If data is accessed via Power Platform (e.g., Power Apps, Power Automate), you can apply DLP policies to connectors.
    - For example, block a flow that takes data from FO and sends it to Dropbox.

Verdict: Supported via Power Platform DLP connector policies.

4. Configure contextual policy scope (emails, exports, connectors) to prevent accidental exposure

D365 FO?
Can be supported indirectly:

- Emails: You can apply Exchange DLP policies to workflow notifications sent from D365 FO via Outlook.
- Exports: Use Microsoft Information Protection (MIP) and sensitivity labels in Excel for exports.
- Connectors: Power Platform DLP policies let you restrict data flow between D365 FO and external services (like Gmail, Twitter, etc.).

Verdict: Yes, with a combination of MIP, Exchange DLP, and Power Platform DLP.

5. Monitor and review DLP alerts and policy violations in unified audit logs

D365 FO?
Not directly logged in Microsoft Purview Audit unless data is being accessed through Microsoft 365 or Power Platform.

- Unified Audit Log (UAL) in Microsoft Purview collects signals from:
    - Exchange, SharePoint, OneDrive, Teams, etc.
    - Power Platform (if D365 FO data is accessed via flows, apps, connectors)
- D365 FO-specific activity logging happens inside FO (via Security logs, database logs, etc.), but not automatically in UAL.

Verdict: Only if data flows through Power Platform or M365 services. Otherwise, use FO audit tools.

ENCRYPTION STANDARDS (At Rest & In Transit)

1. Validate encryption at rest for D365 database, blobs, and storage (Microsoft-managed or CMK)

D365 FO?
Yes – Supported

- Encryption at Rest is enabled by default in D365 FO:
    - All data stored in Azure SQL databases, Azure Blob Storage, and Azure-managed disks are encrypted using Microsoft-managed keys (MMK).
    - Uses AES-256 encryption.
- Customer-Managed Keys (CMK) support:
    - Available for Azure SQL and Azure Blob Storage if your D365 FO environment is configured with Azure Key Vault.
    - CMK for D365 FO specifically is not natively configurable directly in FO — it is managed at the Azure layer.

Verdict: Yes, with Azure-level control for CMK.

2. Ensure TLS 1.2+ encryption in transit for all connections to and from Dynamics 365

D365 FO?
Yes – Fully enforced.

- Microsoft enforces TLS 1.2 or higher for:
    - All client-server communications
    - API and OData calls
    - Integrations (e.g., with Power Platform, custom apps)
- TLS versions below 1.2 are deprecated and not supported in production D365 environments.

Verdict: Fully enforced by default.

3. If using Customer Managed Keys (CMK), confirm key management procedures: rotation, revocation, storage

D365 FO?
Yes, but through Azure services – not directly in FO

- Key management for CMK is handled via:
    - Azure Key Vault
    - Supports:
        - Key rotation (manual or automatic)
        - Key revocation
        - Role-based access control (RBAC)
        - Logging via Azure Monitor / Defender
- You need to work with your Azure administrator or Compliance team to implement this.
- FO does not manage keys directly but inherits the encryption model from underlying Azure services.

Verdict: Yes, with proper Azure Key Vault integration.

4. Audit encryption implementation and key usage logs for compliance

D365 FO?
Partially – Requires Azure-side auditing.

- D365 FO does not expose encryption or key logs directly.
- Instead, auditing of encryption and key usage is done via:
    - Azure Key Vault logs (via Azure Monitor, Log Analytics, Microsoft Defender for Cloud)
    - Azure Storage logs for blob access
    - Azure SQL auditing for access to encrypted data
- These logs can be sent to SIEM tools, like Microsoft Sentinel.

Verdict: Yes but requires Azure-side log configuration.

AUDITING & COMPLIANCE TRACKING *(GDPR & HIPAA Focus)*

1. Enable full audit logging for user actions, data exports, and configuration changes in D365

D365 FO?
Yes – Supported natively.

- D365 FO provides comprehensive auditing tools, including:
    - Database Log: Tracks insert, updates, deletes for selected tables/fields.
    - Security Audit Trail: Captures login/logout and role assignment activity.
    - Workflow History: Records approvals, rejections, and status changes.
    - Electronic Reporting Logs: Tracks data exports via ER framework.
- You can also enable monitoring for system configuration changes, including setup data (e.g., GL parameters, tax setups).

Limitations:

- Not all user actions are logged by default — you must configure what to track.
- No native "export log" unless you track via ER or custom logging.

Verdict: Yes, with proper configuration.

2. Automate Data Subject Request (DSR) workflows: access, deletion, correction

D365 FO?
Partially supported – Some manual steps involved.

- Microsoft provides guidance and tools for GDPR-related DSRs, including:
    - Data discovery: Use Person Search Report to retrieve all records tied to a person (e.g., customer or employee).
    - Data deletion/anonymization: Via Retail module or custom data entities.
    - Correction: Standard editing capabilities exist for correcting personal data.
- There is no out-of-the-box workflow automation for DSRs.

    - You can use Power Automate to create approval workflows.
    - Microsoft's Compliance Center also supports DSR tracking (mostly for M365/Dataverse, not FO directly).

Verdict: Partial – manual with some automation possible.

3. Use Purview Compliance Manager to score and track compliance posture for GDPR/HIPAA

D365 FO?
Indirect – Compliance Manager does not directly monitor FO actions.

- Microsoft Compliance Manager provides:
    - Pre-built GDPR/HIPAA assessments
    - Control scoring
    - Documentation mapping (to Microsoft-managed controls and customer responsibilities)
- Limitation:
    - D365 FO is not directly connected to Compliance Manager telemetry.
    - You will need to manually update control scores related to D365 FO or integrate Azure-level logs.

Verdict: Supported in process, not via direct telemetry.

4. Generate and retain audit-ready reports aligned with regulatory retention schedules

D365 FO?
Yes – With configuration

- D365 FO supports:
    - Document archiving (e.g., invoices, journal entries)
    - Audit trails for financial transactions and approvals.
    - Export to secure storage (SharePoint, Azure Blob)
- You can configure:
    - Document retention using electronic reporting.

    - Storage location and access policies
- Regulatory requirements (e.g., 7-year retention for finance) must be mapped to:
    - Backup retention
    - Audit log export/archiving.

Verdict: Yes – with proper retention/archiving setup.

5. Periodically test anonymization, data minimization, and retention policies

D365 FO?
Supported manually or via customization.

- Microsoft offers tools like:
    - Anonymization in Retail module
    - Data retention policies (custom development or ER logic)
- Testing:
    - No built-in framework for automated testing of these policies
    - Can be done via:
        - Custom batch jobs
        - Power Platform automation
        - Audit reports for validation.

Verdict: Supported via customization or manual testing.

THREAT DETECTION & RESPONSE *(Microsoft Defender)*

1. Enable Microsoft Defender for Cloud Apps integration with Dynamics 365 for threat alerts

D365 FO?
Partially supported via Microsoft Defender for Cloud Apps (MCAS)

- MCAS (now part of Microsoft Defender for Cloud Apps) can:
    - Monitor user activity in D365 Online apps that are based on the Dataverse (like D365 Sales, Customer Service).
    - D365 FO is not natively integrated into MCAS (unlike SharePoint, OneDrive, etc.).

Workarounds:

- Integrate D365 FO via API logs, Power Platform usage, or custom connectors.
- Use Azure AD Sign-in logs (since FO is Azure AD-backed) to track logins and access attempts.
- You can also create custom app policies in MCAS for suspicious OAuth token use, risky sessions, or impossible travel.

Verdict: Partial support; requires custom integration.

2. Configure detection for anomalies: unusual login, privilege escalation, data exfiltration

D365 FO?
Yes – Partially through Azure AD + Defender

- Unusual logins / Impossible travel:
    - Detected via Microsoft Entra ID Protection (formerly Azure AD Identity Protection).
    - You can get alerts for:
        - Sign-ins from unusual locations.
        - Login attempts with leaked credentials.

        - Sign-ins from anonymous IPs or TOR
- Privilege escalation:
    - You can audit role assignments in D365 FO.
    - But alerting on this requires:
        - Custom audit reports in FO
        - Or external alerting via Azure Monitor or Defender
- Data exfiltration:
    - No native detection in D365 FO.
    - You can monitor export activity via:
        - Electronic Reporting (ER) logs
        - Power Automate logs (if data is accessed via flows)

Verdict: Partially supported; relies on Azure AD + custom logging.

3. Set up Power Automate playbooks to automate responses: lock accounts, notify admins, isolate sessions

D365 FO?
Yes – Supported via Defender + Power Automate integration.

- Microsoft Defender supports Power Automate playbooks.
    - You can trigger actions based on Defender alerts, such as:
        - Locking a user in Azure AD
        - Sending admin alerts (email, Teams)
        - Logging the incident into Sentinel or ServiceNow
- In D365 FO, users are controlled by Azure AD, so disabling or locking a user account in Entra ID impacts D365 access too.
- You can also call D365 APIs or custom endpoints in playbooks if you need app-specific actions (e.g., change user roles, suspend workflows).

Verdict: Yes – effective integration with Power Automate + Azure AD.

4. Leverage threat intelligence dashboards and incident graphs in Defender

D365 FO?
Yes – for identity-level activity

- Microsoft Defender 365 dashboards provide:
    - Alerts on user behavior, malware, phishing, etc.
    - Incident timelines, graphs, and correlations
    - Role-based dashboards for SOC analysts
- D365 FO itself does not send telemetry directly to Defender, but:
    - Identity-related events from Azure AD (which governs FO access) are fully visible in Defender.
    - If FO data is accessed through Power Platform or other Microsoft 365 services, Defender may surface related activity.

Verdict: Yes – for user identity and integrated services.

SECURITY ECOSYSTEM & ENDPOINT INTEGRATION *(Sentinel & Intune)*

1. Forward D365 audit and Defender logs into Microsoft Sentinel for SIEM correlation

D365 FO?
Partially supported – mostly via Azure AD, not direct FO logs.

- D365 FO does not send logs directly to Sentinel, but:
    - Azure AD sign-in and audit logs (which control FO access) can be streamed into Sentinel.
    - Defender for Endpoint, Defender for Cloud Apps, and Microsoft 365 logs also integrate with Sentinel for threat correlation.
    - If FO logs (e.g., Database log, ER logs) are exported to Azure Log Analytics, they can be forwarded to Sentinel.

Integration methods:

- Use Azure Monitor Diagnostic Settings
- Set up custom connectors or Azure Functions to pull logs from FO (via OData, Data Lake, or SQL exports)

Verdict: Partial – Azure AD & Defender logs integrate easily; FO logs require custom setup.

2. Set up analytics rules to detect cross-service threats and insider indicators

D365 FO?
Yes – With Sentinel

- In Microsoft Sentinel, you can:
    - Define analytics rules to correlate events across:
        - Azure AD
        - Microsoft 365 (Outlook, Teams)
        - Defender for Endpoint

        - Intune
    - Detect insider threats by analyzing:
        - Abnormal login behavior
        - Privilege escalation
        - Access to sensitive data across services
- While FO does not directly send events, identity-based threats are visible through Azure AD logs (e.g., role changes, logins, session hijacks).

Verdict: Yes – works well for cross-service identity threats.

3. Enroll user endpoints in Microsoft Intune for mobile device compliance and protection

D365 FO?
Yes – Through M365 integration

- D365 FO is accessed through:
    - Browsers (Edge, Chrome)
    - Mobile apps (e.g., Dynamics 365 for phones/tablets)
    - Excel add-ins
- All of these endpoints can be governed by Microsoft Intune policies:
    - Enforce encryption, antivirus, updates.
    - Monitor device risk via Defender for Endpoint
    - Apply mobile application management (MAM) policies.

Verdict: Yes – full Intune support for endpoints accessing D365.

4. Implement conditional access based on device compliance status

D365 FO?
Yes – Fully supported via Azure AD Conditional Access

- D365 FO uses Azure AD for identity and access management.
- You can create Conditional Access policies to:
    - Allow access only from compliant devices.

    - Block access from unmanaged or risky devices.
    - Require MFA for non-compliant access attempts.

Common scenarios:

- Block mobile access to FO from non-corporate devices.
- Require compliant desktop/laptop with antivirus and updates.
- Enforce sign-in only from specific geographies.

Verdict: Yes – highly recommended for FO environments.

5. Enable remote wipe or block access for non-compliant or compromised devices via Intune

D365 FO?
Yes – Through standard Intune capabilities

- Devices accessing D365 FO via browser, mobile apps, or Excel add-ins can be:
    - Blocked or wiped if they become non-compliant.
    - Managed with MAM policies to protect corporate data without wiping personal data.
- This is particularly useful for:
    - BYOD (Bring Your Own Device) environments.
    - Mobile workforce
    - Enforcing compliance before access

Verdict: Yes – fully supported with Intune.

ONGOING MONITORING & GOVERNANCE

1. Use Secure Score or Compliance Manager metrics to measure your security posture

D365 FO?
Indirect – Secure Score does not include FO directly, but it still helps.

- Microsoft Secure Score:
    - Tracks security posture across Microsoft 365, Azure AD, Defender, Intune, etc.
    - Does not include D365 FO-specific metrics, but covers the infrastructure it relies on (identity, device, conditional access, etc.).
- Microsoft Compliance Manager:
    - Including GDPR, HIPAA, ISO 27001, etc.
    - Contains assessments and control mappings that cover D365 services — including shared responsibilities for D365 FO.
    - You can manually update implementation details for FO-specific controls.

Verdict: Yes – indirectly covers FO security posture through broader Microsoft 365 metrics.

2. Schedule quarterly security reviews: role audits, policy tuning, incident postmortems

D365 FO?
Yes – Fully supported but requires scheduled internal governance.

- Role and access review:
    - D365 FO includes Role-based security with Segregation of Duties (SoD) checks.
    - You can export security role assignments and run periodic audits.
- Policy tuning:
    - Review workflow approvals, conditional access, audit logs, and ER export paths.
- Post-incident reviews:

    - Gather input from Azure AD logs, FO change logs, Sentinel incidents, etc.

Tools to assist:

- Azure Monitor / Sentinel
- Excel exports of user-role mappings
- Custom Power BI dashboards

Verdict: Yes – best practice for FO environments.

3. Conduct penetration testing and Dynamic Application Security Testing (DAST) periodically

D365 FO?
Limited support – Requires Microsoft approval for penetration tests.

- Microsoft allows pen tests on D365 FO, but:
    - You must follow the Microsoft Cloud Penetration Testing Rules of Engagement.
    - Notify Microsoft before testing anything hosted on their infrastructure.
- DAST:
    - You can test custom-developed extensions, APIs, and integrations with DAST tools like:
        - OWASP ZAP
        - Burp Suite
        - Veracode
    - FO's core app is sealed, but your customizations and external services should be tested.

Verdict: Possible with Microsoft approval – mostly for custom components.

4. Train users on risks, phishing, compliance roles, and security best practices

D365 FO?
Yes – Supported externally.

- Not handled within FO directly, but Microsoft ecosystem offers:

    - Microsoft Defender for Office 365: Simulated Phishing Attacks
    - Microsoft Learn and Compliance Manager: User training material.
    - Custom LMS platforms (or Teams + SharePoint) for delivering security awareness.
- In FO, you can:
    - Use custom alerts or workflow messages to remind users of data handling policies.
    - Restrict UI access based on role (least privilege principle)

Verdict: Yes – train through M365 ecosystem, enforce via FO roles and messaging.

5. Evaluate third-party integrations to ensure secure configurations and limited permissions

D365 FO?
Yes – Crucial and fully possible

- D365 FO supports integration via:
    - OData
    - Custom services (REST/SOAP)
    - Azure Data Lake, Synapse, Power Platform
- You should:
    - Assign App registrations least-privilege permissions (using Azure AD app roles)
    - Monitor API traffic and OAuth scopes.
    - Review connected apps via Azure AD Enterprise Apps blade.
- Use Azure AD Conditional Access to limit third-party access.

Verdict: Yes – requires governance over connected apps and APIs.