Insight

Whitepaper

Microsoft

When "As Secure As Possible" Isn't Enough:

Why Now Is the Time to Move to Microsoft 365 E5

You may think that your data and systems are secure as possible with your current Microsoft 365® E3 license, but are you really prepared for the evolving threats and challenges of today's digital landscape? How confident are you that you can prevent, detect and respond to cyberattacks, protect your sensitive information and comply with regulatory requirements? How much time and money are you spending on managing multiple security solutions that may not work well together or cover all your needs?

If you are not sure about the answers to these questions — or if you are worried about the risks and costs of a security breach — you may want to consider upgrading to Microsoft® 365 E5. This is the most comprehensive and advanced security offering from Microsoft, designed to help you achieve a Zero Trust security posture across your identity, devices, data, apps and infrastructure.

With M365 E5, you can enjoy the following benefits:

Enhanced threat protection
with Microsoft Defender for Endpoint, Office 365® and Identity, which leverage artificial intelligence, behavioral analytics and cloud scale to provide proactive and unified defense against sophisticated attacks

Data Loss Prevention (DLP) and governance
with Microsoft Information Protection, Cloud App Security and Compliance Manager, which help you classify, label, protect and monitor your sensitive data across devices, apps and cloud services, and simplify compliance with industry standards and regulations

Streamlined security management and operations
with Microsoft Secure Score, Microsoft 365 Security Center and Microsoft 365 Compliance Center, which provide you with a centralized and integrated dashboard to assess your security posture, prioritize recommendations and automate workflows

Reduced complexity and costs
with a single vendor, a single license and a single support contract, which eliminates the need for multiple security solutions and vendors and lowers your total cost of ownership

Data is one of the most valuable assets for any organisation, but it also comes with many challenges and risks. How can you protect your sensitive data from unauthorised access or misuse? How can you comply with the data protection regulations and standards in your industry or region? How can you monitor and audit your data activities and access logs, and generate reports and alerts for compliance and governance purposes?

The following questions will help you gauge how your current approach compares to best practices and benchmarks.

Can you confidently say that your company's credentials have never been compromised? And if they were, did you have an automated means to monitor and mitigate the situation?

If your company is using M365 E3, you might not be aware of the potential security risks that exist in your environment. M365 E3 relies on basic password policies and multi-factor authentication to protect your credentials, but these measures are not enough to prevent or detect credential theft and misuse. Hackers can use phishing, malware or brute-force attacks to obtain your passwords and bypass your defenses.

M365 E5 offers a superior level of security for your credentials with Microsoft Entra™ ID Premium P2, which includes advanced features such as:

- **Identity Protection:** This feature uses machine learning to detect suspicious activities and risky sign-ins based on user behavior, location, device and network. It also provides real-time alerts and recommendations to help you respond and remediate the issues.
- **Privileged Identity Management:** This feature allows you to manage and monitor the access of users who have elevated privileges, such as administrators, owners or contributors. You can enforce just-in-time and just-enough access policies, require multi-factor authentication and approval workflows, and review audit logs and reports to ensure compliance and accountability.

With M365 E5, you can confidently say that your company's credentials are protected by the most advanced and comprehensive identity and access management solution in the market. You can also benefit from an automated and proactive approach to monitor and mitigate any potential threats, and reduce the complexity and costs of managing multiple security solutions and vendors.

Are you fully aware of the nature and location of all your sensitive data, and do you have a clear understanding of how your sensitive data is safeguarded from potential exposure?

The M365 E5 license with Microsoft's Purview can help you gain more visibility and control over your sensitive data within Microsoft 365 apps and services, such as SharePoint®, OneDrive® and Exchange. Unlike M365 E3, which only provides basic data protection and compliance features, M365 E5 and Purview can scan and classify your data across different locations and devices, and automatically apply consistent policies and labels based on your business needs and industry regulations. You can also use Purview to discover and map your data sources and flows, and monitor and audit the access and usage of your sensitive data. With M365 E5 and Purview, you can ensure that your sensitive data is safeguarded from potential exposure and misuse, and that you have a clear understanding of how it is stored, processed and shared.

How effective is your system in categorising sensitive data, and how do you guarantee it's secure from unauthorized access?

M365 E5 and Purview enable you to discover, classify and protect sensitive data across your hybrid data estate, including on-premises, cloud and multicloud environments. You can use built-in or custom classifiers to identify more than 100 types of sensitive data, such as Personally Identifiable Information (PII), financial data or health records. You can also apply sensitivity labels and encryption to your data at rest or in transit, ensuring that only authorized users can access it.

You might be using DLP solutions, but can they respond to and limit access based on risky behaviors? How do you monitor and detect risky behaviors across your data sources and devices?

M365 E5 and Purview offer advanced DLP solutions that can detect and respond to risky behaviors across your data sources and devices. You can define policies and rules to automatically block, quarantine or notify users when they attempt to share or transfer sensitive data outside your organization or to untrusted recipients. You can also leverage behavioral analytics and machine learning to identify and remediate insider threats, such as data exfiltration, sabotage or theft.

M365 E5 and Purview provide comprehensive visibility and insights into your data activities and risks. You can use the Microsoft 365 Compliance Center to monitor and audit your data events, such as creation, access, modification, deletion or sharing. You can also use Microsoft Cloud App Security to discover and assess the usage and risk level of your cloud apps and services. Additionally, you can use Microsoft Defender for Endpoint to detect and investigate malicious or anomalous activities on your endpoints, such as malware, ransomware or phishing attacks.

How do you enforce granular policies and controls to prevent unauthorized access, sharing or leakage of sensitive data?

With M365 E5, you can enforce granular policies and controls to prevent unauthorized access, sharing or leakage of sensitive data by using the sensitivity labeling and protection capabilities of Purview. Sensitivity labeling allows you to classify and label your data based on its sensitivity and business value, and apply encryption, access restrictions and visual markings to protect it throughout its lifecycle. You can also use sensitivity labeling to automatically scan and discover your sensitive data across your cloud and on-premises environments, and apply consistent policies and controls to them. With Purview and M365 E5, you can also cover other data sources and scenarios, such as Microsoft Teams®, Outlook®, Word, Excel®, PowerPoint®, Power BI®, Windows® 10 devices, third-party cloud apps, and on-premises file servers and network shares. You can also leverage more sophisticated and customizable DLP policies and rules, such as exact data match, trainable classifiers or sensitive information types, to detect and protect your data with higher accuracy and precision.

M365 E5 and Purview offer more advanced and comprehensive DLP solutions than M365 E3, which only includes basic DLP capabilities for Exchange Online, SharePoint Online and OneDrive for Business. Additionally, you can integrate your DLP solutions with other security and compliance tools, such as Microsoft Compliance Manager or Microsoft Secure Score, to enhance your data protection and governance. You can also use Microsoft Endpoint Manager, which is included in M365 E5, to manage and secure your Windows 10 devices and enforce compliance policies.

How do you respond to data incidents and breaches in real time and remediate them effectively?

One of the key benefits of M365 E5 and Purview is that they enable you to respond to data incidents and breaches in real time and remediate them effectively. With M365 E5 and Purview, you can:

- **Monitor and audit your data activities and events** across your cloud and on-premises environments using the unified audit log and the advanced auditing capabilities.
- **Receive alerts and notifications** when a data incident or breach occurs, such as when a user tries to access, share or exfiltrate sensitive data, or when a malicious actor attempts to compromise your data.
- **Investigate and analyse the data incident or breach**, using the Microsoft 365 Security Center, the Microsoft 365 Compliance Center and the Purview Data Map. You can also leverage the advanced eDiscovery and Advanced Threat Protection (ATP) features of M365 E5 to collect and preserve evidence, identify and track the source and scope of the data incident or breach, and assess the impact and risk level of the data incident or breach.
- **Remediate and resolve the data incident or breach**, using the built-in actions and workflows of M365 E5 and Purview. You can also use the Microsoft Defender for Cloud Apps and Microsoft Defender for Endpoint features of M365 E5 to block or revoke access, quarantine or delete data, apply or remove sensitivity labels, enforce encryption or protection policies, or initiate a data breach notification process.

M365 E5 and Purview provide more value and improved security than M365 E3, which does not include the advanced auditing, eDiscovery, ATP, Defender for Cloud Apps or Defender for Endpoint features. M365 E3 also has limited capabilities to monitor, investigate, and remediate data incidents and breaches across multiple data sources and scenarios.

How do you ensure compliance with data privacy and security regulations and standards?

To ensure compliance with data privacy and security regulations and standards, you need to have a comprehensive and consistent approach to managing and protecting your sensitive data across your entire organisation. M365 E5 and Purview can help you achieve this by providing the following benefits:

- **M365 E5 and Purview enable you to discover and classify your sensitive data across various data sources**, such as SharePoint, OneDrive, Exchange, Teams, Azure®, third-party cloud apps and on-premises servers, using built-in or custom sensitivity labels and data classification policies. You can also use the Purview Data Map to gain a holistic view of your data landscape and lineage, and identify any data quality, governance or compliance issues.
- **M365 E5 and Purview allow you to apply and enforce data protection and retention policies** based on your sensitivity labels and compliance requirements. You can use the Microsoft Purview® Information Protection and Microsoft Compliance Manager features of M365 E5 to encrypt, restrict or expire access to your sensitive data, as well as monitor and remediate any policy violations or conflicts. You can also use the Purview Data Insights and Data Catalog features to track and report on the usage and compliance status of your data assets.
- **M365 E5 and Purview help you respond and adapt to changing data privacy and security regulations and standards**, such as GDPR, CCPA, HIPAA or ISO 27001. You can use the Microsoft Compliance Score and Microsoft Privacy Assessment features of M365 E5 to assess your current compliance posture and identify any gaps or risks. You can also use the Purview Data Policy Management and Data Access Governance features to create and update your data policies and permissions in accordance with the latest regulatory and industry best practices.

M365 E5 and Purview provide more value and improved security than M365 E3, which does not offer the same level of data discovery, classification, protection, retention, monitoring, reporting and governance capabilities. M365 E3 also has limited support for cross-platform and cross-application data compliance scenarios, and does not include the advanced features of Purview that enable you to manage and secure your data at scale and across hybrid environments.

How do you measure and improve the effectiveness and efficiency of your DLP solutions?

To measure and improve the effectiveness and efficiency of your DLP solutions, you need to have a comprehensive and consistent view of your data across your organisation. You also need to be able to track and report on the compliance status and actions taken on your data, as well as evaluate the impact of your policies and controls. M365 E5 and Purview enable you to do this by providing the following features:

- **Data Loss Prevention Dashboard:** This dashboard gives you a centralized place to manage and monitor your DLP policies and alerts across Microsoft 365 apps and services, such as Exchange Online, SharePoint Online, OneDrive for Business, Teams and Power Platform®. You can also integrate with third-party data sources, such as Box, Dropbox, Google Drive, Amazon® S3 and Salesforce, using the Microsoft Cloud App Security connector. The dashboard provides you with insights into the types, locations and volumes of sensitive data in your organization, as well as the potential exposure and risk levels. You can also see the trends and patterns of data loss incidents and violations, and drill down into the details and context of each event. You can use this information to fine-tune your policies and rules and take corrective actions to prevent or mitigate data loss.
- **Purview Data Insight:** This feature allows you to discover, catalog and classify your data across your hybrid data estate, including on-premises, cloud and multicloud environments. You can use Purview to scan and index your data sources, such as SQL Server®, Azure SQL Database, Azure Synapse Analytics, Azure Data Lake Storage, Azure Blob Storage, Azure Cosmos DB, Power BI and more. You can also use the Purview Data Map to visualize the lineage and relationships of your data across different systems and applications. Purview Data Insight helps you understand the nature, sensitivity and value of your data, and apply the appropriate data protection and retention policies based on your business and compliance requirements.
- **Purview Data Governance:** This feature enables you to define and enforce your data policies and permissions across your data estate and ensure that your data is accessed and used in accordance with your data governance standards and principles. You can use Purview to create and assign data roles and responsibilities, such as data owners, stewards, consumers and experts, and manage their access rights and privileges. You can also use Purview to implement data quality rules and validation checks and monitor the compliance status and health of your data assets. Purview Data Governance helps you ensure that your data is accurate, trustworthy and secure, and that you can demonstrate compliance with internal and external regulations and standards.

M365 E5 and Purview provide more value and improved security than M365 E3, which does not offer the same level of data discovery, classification, protection, retention, monitoring, reporting and governance capabilities. M365 E3 also has limited support for cross-platform and cross-application data compliance scenarios and does not include the advanced features of Purview that enable you to manage and secure your data at scale and across hybrid environments. By upgrading to M365 E5 and Purview, you can enhance your DLP solutions and reduce the risk of data breaches and compliance violations.

Can you detect and respond to data incidents and breaches across multiple devices, platforms and applications in real time?

Below are some of the ways that M365 E5 and Purview help you detect and respond to data incidents and breaches across multiple devices, platforms and applications in real time.

- **Purview Data Map:** This feature gives you a holistic, up-to-date view of your data landscape, including where your data is stored, how it flows, who accesses it and what it contains. You can use the Data Map to discover and catalog your data sources, scan and classify your data assets, and track the lineage and dependencies of your data. The Data Map also integrates with Microsoft Purview to apply consistent policies and labels to your data, and enforce data protection and compliance rules.
- **M365 Compliance Center:** This feature allows you to manage and monitor your data compliance posture across M365 and other cloud services, such as Azure, AWS®, Salesforce and Google Workspace. You can use the Compliance Center to create and assign compliance policies and actions, such as retention, deletion, encryption and audit, and apply them to your data based on its type, location, sensitivity and regulatory requirements. You can also use the Compliance Center to generate reports and dashboards that show your compliance status and performance, and identify any gaps or issues that need your attention.
- **Purview Audit (Premium):** This feature enables you to capture and retain more granular and longer-term audit logs of your data activity and usage, and analyze them for forensic and investigative purposes. You can use Advanced Audit to access up to 10 years of audit data, search and filter by various criteria, such as user, device, app and action, and export the results for further analysis. You can also use Advanced Audit to set up alerts and notifications for specific events or patterns, such as data exfiltration, unauthorized access or policy violations, and trigger automated responses or workflows to address them.
- **Purview Insider Risk Management:** This feature helps you to detect and mitigate insider threats, such as data leakage, theft, sabotage or fraud, by using advanced analytics and machine learning to identify risky or malicious user behaviors and activities. You can use Insider Risk Management to define risk indicators and thresholds, such as data movement, access frequency or network anomalies, and monitor your users for any deviations or violations. You can also use Insider Risk Management to investigate and resolve insider incidents, and provide evidence and documentation for legal or disciplinary actions.

By upgrading to M365 E5 and Purview, you can leverage these features and capabilities to enhance your data security and compliance, and protect your data from internal and external threats.

How can I ensure that my data is encrypted, classified, labeled and protected according to its sensitivity and value?

The way to ensure that your data is encrypted, classified, labeled and protected according to its sensitivity and value is to use Microsoft 365 E5 Data Loss Prevention (DLP). This feature helps you prevent the accidental or intentional leakage of your sensitive data, such as personal information, financial data or intellectual property, by detecting and blocking potential data breaches across Microsoft 365 services, such as Exchange Online, SharePoint Online, OneDrive for Business, Teams and Outlook. You can use DLP to define rules and policies based on the content and context of your data, such as the sensitivity labels, the recipients or the location, and apply actions such as notify, block, encrypt or retain. By using DLP, you can protect your data from unauthorized or inappropriate sharing and comply with industry standards and regulations.

Compared to Microsoft 365 E3, which offers limited DLP capabilities for Exchange Online, SharePoint Online and OneDrive for Business, Microsoft 365 E5 provides advanced and comprehensive DLP features for all Microsoft 365 services, including Teams and Outlook. Additionally, Microsoft 365 E5 includes Microsoft Defender for Cloud Apps, which extends DLP to third-party cloud applications, such as Dropbox, Box or Salesforce. Microsoft 365 E5 also enables you to use auto-labeling by endpoints, which allows you to automatically apply sensitivity labels to your data based on the content and metadata, and enforce encryption and protection policies on your devices, such as Windows 10, iOS® or Android.

Finally, consider the possible difficulties you might encounter without the security value proposition of Microsoft M365 E5:

- You may **lose visibility and control over your sensitive data** across different devices, platforms and applications, and expose your data to unauthorized access or misuse.
- You may **fail to comply with the data protection regulations and standards** in your industry or region, such as GDPR, HIPAA or PCI DSS, and incur legal penalties or reputational damage.
- You may **experience data breaches or leaks** that compromise your data confidentiality, integrity and availability, and cause financial losses or customer dissatisfaction.
- You may **miss out on the opportunities to optimize** your data governance and management, and enhance your data quality, security and value.
- You **may not be able to detect and respond to advanced identity-based threats**, such as compromised accounts, insider risks or malicious apps, or mitigate the potential damage to your data and systems.
- You **may not be able to enforce granular and conditional access policies** based on user, device, location and risk factors, or prevent unauthorized or risky access to your data and resources.
- You **may not be able to protect your sensitive data** from accidental or malicious sharing, deletion or alteration, or apply DLP policies across your cloud and on-premises environments.
- You **may not be able to discover, classify, label and protect your sensitive data** across its lifecycle, or comply with the data protection requirements and regulations in your industry or region.
- You **may not be able to monitor and audit** your data activities and access logs, or generate reports and alerts for compliance and governance purposes.

Driving innovation with digital transformation

At Insight, we help clients enable innovation with an approach that spans people, processes and technologies. We believe the best path to digital transformation is integrative, responsive and proactively aligned to industry demands. Our client-focused approach delivers best-fit solutions across a scope of services, including the modern workplace, modern applications, modern infrastructures, the intelligent edge, cybersecurity, and data and AI.

Learn more at marketing.APAC@insight.com

About the author

Norm Andersch is a senior cybersecurity architect with Insight's modern workplace team. His focus is on creating professional and managed services specifically for security and compliance to help clients strengthen their security programs. Norm holds numerous Microsoft certifications for Azure security, Azure AD and the entire suite of Microsoft Defender solutions.

Insight

marketng.APAC@insight.com