Accelerate your General Data Protection Regulation (GDPR) Compliance Journey with Microsoft 365

Embrace the GDPR with the most complete, secure and intelligent solution for digital work.

Microsoft

Table of Contents

Disclaimer

This white paper is a commentary on the GDPR, as Microsoft interprets it, as of the date of publication. We've spent a lot of time with GDPR and like to think we've been thoughtful about its intent and meaning. But the application of GDPR is highly fact-specific, and not all aspects and interpretations of GDPR are well-settled.

As a result, this white paper is provided for informational purposes only and should not be relied upon as legal advice or to determine how GDPR might apply to you and your organization. We encourage you to work with a legally qualified professional to discuss GDPR, how it applies specifically to your organization, and how best to ensure compliance.

MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS WHITE PAPER. This white paper is provided "as-is." Information and views expressed in this white paper, including URL and other Internet website references, may change without notice.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this white paper for your internal, reference purposes only.

Published September 2017

Version 1.0

Executive Summary

The General Data Protection Regulation (GDPR) is causing organizations to evaluate their data processing systems, especially the critical platforms they choose to enable their workforce. The GDPR is compelling every organization to consider how they will respond to today's security and compliance challenges. It may require significant changes to how your business gathers, uses, and governs data.

Microsoft has brought together Office 365, Windows 10, and Enterprise Mobility + Security into a single, always-up-to-date solution called Microsoft 365 – relieving organizations from much of the cost and complexity of multiple, fragmented systems that were not necessarily designed to be compliant with current standards.

We recently made several Microsoft 365 security and compliance announcements and updates - enabling organizations to simplify their journey to compliance with the General Data Protection Regulation (GDPR). These announcements at Ignite add to our extensive capabilities that organizations are already using to secure and manage their data, users, and devices.

This white paper provides you with an understanding of: a) the GDPR and its implications on organizations, b) an approach to moving toward GDPR compliance and how the capabilities of Microsoft 365 Enterprise edition can accelerate that journey, and c) what you can do to get started now.

Choose a platform you can trust, and verify

We understand that organizations with GDPR responsibilities will have additional needs to demonstrate compliance, and we're investing in tools to help them achieve those goals.

Microsoft 365 users enjoy the built-in security and compliance for the apps, services, and devices that they use every day. Microsoft has a long history of transparency, defense-in-depth, and privacy-by-design that enabled us to be the first enterprise cloud services provider to implement the rigorous controls needed to earn approval for the EU Model Clauses, the first to achieve ISO's 27018 cloud privacy standard, and the first to offer contractual commitments to the GDPR.

Introducing Compliance Manager – We understand that achieving your organizational compliance goals can be very challenging. It's hard to stay up-to-date with all the regulations that matter to your organization, and to define and implement the controls.

We're pleased to introduce Compliance Manager, a new compliance solution that helps you to manage your compliance posture from one place. Compliance Manager enables you to conduct real-time risk assessment, providing one intelligent score that reflects your compliance performance against data protection regulatory requirements when using Microsoft cloud services.

You will also be able to use the built-in control management and audit-ready reporting tools to improve and monitor your compliance posture. Read our Tech Community Blog to learn more about Compliance Manager, and sign up for the preview program, which will be available starting in November 2017.

Simplify how you govern data

Organizations face ever increasing quantities of complex electronic data. Gaining control over this data overload so that you know what to keep and find what's relevant – when you need it – is critical for both security and compliance purposes. Today we are introducing several new features which further enhance the already rich set of capabilities available with Microsoft Information Protection and Advanced Data Governance.

Companies of all sizes and industries need to protect their sensitive data and ensure that it doesn't get into the wrong hands. Employees are using more SaaS apps, creating more data, and working across multiple devices. While this has enabled people to do more, it has also increased the risk of data loss – it is estimated that 58% of workers have accidentally shared sensitive data with the wrong person.

Microsoft's Information Protection solutions help you identify, classify, protect and monitor your sensitive data – as it is created, stored, or shared. We made several investments across our information protection solutions – helping provide more comprehensive protection across the data lifecycle. A key part of our vision is to provide a more consistent and integrated classification, labeling, and protection approach across our information protection technologies, enabling persistent protection of your data – everywhere. Microsoft Cloud App Security now deeply integrates with **Azure Information Protection** to classify and label files that reside in cloud applications.

Use intelligent tools to better discover and control your data

Many organizations are evaluating how to find and protect the personal data they collect. With the explosion of data and its increasing value – many organizations cannot adequately manage their assets with traditional manual processes.

Unfortunately, even once you know where all the data is and how it should be managed, you must constantly ensure it is protected from threats. The GDPR requires organizations take appropriate measures to prevent unauthorized access or disclosure and to notify stakeholders in the case of breach. Today, on average attacks exist for over 90 days in an environment prior to detection. Microsoft continues to invest in tools that help detect attacks sooner and then remediate, as well as in pre-breach attack prevention tools.

Analysis of non-Office 365 data with Advanced eDiscovery: While the amount of data being generated and stored in Office 365 is growing at an exponential rate, many organizations still have data in legacy file shares and archives., Data is also being generated in other cloud services which may be relevant for an eDiscovery case surrounding a Data Subject Request. Analysis of non-Office 365 data allows organizations to import the case-specific copy of such data into a specifically assigned Azure container and analyze it using Office 365 Advanced eDiscovery. Having one eDiscovery workflow for both Office 365 and non-Office 365 data provides organizations with the consistency they need to make defensible decisions across the entire data set of a case.

To better protect your users against threats, we also improved our anti-phishing capabilities in **Office 365 Advanced Threat Protection**, with a focus on mitigating content phishing, domain spoofing, and impersonation campaigns. Office 365 Advanced Threat Protection is also expanded to help secure SharePoint Online, OneDrive for business, and Teams. In Windows, we added **Windows Defender**

Application Control, which is powered by the Microsoft Intelligent Security Graph to make it less likely that malicious code can run on that endpoint.

On the post-breach detection side, we announced the limited preview of a brand-new service – **Azure Advanced Threat Protection** for users – that brings our on-premises identity threat detection capabilities to the cloud and integrates them with the Microsoft Intelligent Security Graph. Finally, as previously announced earlier in the month, **Windows Defender Advanced Threat Protection** is integrating Hexadite's AI technology to automatically investigate new alerts, determine the complexity of a threat, and take the necessary actions to remediate it.

Office 365 security management updates – We have also made a few updates to Advanced Security Management to give you even better visibility and control over Office 365. To help organizations in the EU meet their compliance obligations, starting in October, we will begin hosting Advanced Security Management in our EU datacenter region. We are also giving you additional visibility into the service by adding support for activities from Skype for Business, Yammer and Office 365 Threat Intelligence. The signals from these services will be used to generate activity alerts and be factored into anomaly detection alerts. Lastly, to better align our Microsoft 365 investments, we are renaming Advanced Security Management to Office 365 Cloud App Security.

Taking the next step on your GDPR compliance journey

We believe privacy is a fundamental right. The GDPR is an important step forward to further clarify and enable individual privacy rights and look forward to sharing additional updates how we can help you comply with this new regulation and, in the process, advance personal privacy protections.

As a global company with hundreds of millions of customers around the globe, we are subject to many stringent regulations including the GDPR and we understand the challenges you face. As your trusted partner, we are committed to going beyond our minimum responsibilities and always working on behalf of your best interests. To that end, Microsoft is an active participant in a community of compliance experts that can support all aspects of your GDPR journey - such as audit and consulting, cloud migration assistance, as well as delivering specific point solutions.

Make Microsoft 365, including the best of Office 365, Windows 10, and Enterprise Mobility + Security, the foundation of your journey and start accelerating your compliance with the GDPR by:

- Choosing a platform you can trust, and verify
- Simplifying your approach to information governance
- Using intelligent tools to help discover and control data
- Leveraging the expertise of our community

Introduction

This paper is designed to introduce Microsoft 365 to IT, Security and Compliance managers who are preparing their organization for the GDPR - and to help them understand the many relevant capabilities of Microsoft 365. We will provide a little background on the GDPR and then go into specific aspects of Microsoft 365 that will help accelerate your GDPR compliance journey.

The GDPR and Its implications

The GDPR is a complex regulation that may require significant changes in how you gather, use and manage personal data. Microsoft has a long history of helping our customers comply with complex regulations, and when it comes to preparing for the GDPR, we are your partner on this journey.

The GDPR imposes rules on organizations that offer goods and services to people in the European Union (EU), or that collect and analyze data tied to EU residents, no matter where those businesses are located. Among the key elements of the GDPR are the following:

- Enhanced personal privacy rights - strengthened data protection for residents of the EU by ensuring that they have the right to access their personal data, to correct inaccuracies in that data, to erase that data, to object to processing of their personal data, and to move it;
- Increased duty for protecting personal data - reinforced accountability of organizations that process personal data, providing increased clarity of responsibility in ensuring compliance;
- Mandatory personal data breach reporting - organizations that control personal data are subject to stringent reporting and notification requirements in the event of a personal data breach
- Significant penalties for non-compliance - steep sanctions, including substantial fines that are applicable whether an organization has intentionally or inadvertently failed to comply.

As you might anticipate, the GDPR may have a significant impact on your business potentially requiring you to update privacy policies, implement and strengthen data protection controls and breach notification procedures, deploy highly transparent policies, and further invest in IT and training.

Where do you begin? How do you start the journey toward GDPR compliance utilizing Microsoft 365?

In the general whitepaper "Beginning your General Data Protection Regulation (GDPR) Journey", we addressed topics such as an introduction to GDPR, how it may impact you and what you can do to begin your journey today. We also recommended that you begin your journey to GDPR compliance by focusing on four key steps:

- **Discover**—identify what personal data you have and where it resides.
- **Manage**—govern how personal data is used and accessed.
- **Protect**—establish security controls to prevent, detect, and respond to vulnerabilities and data breaches.
- **Report**—execute on data requests, report data breaches, and keep required documentation.

For each of the steps, we outlined example tools, resources, and features that can be used to help you address the requirements of that step, and included links for you to learn more at Microsoft.com/GDPR. Here you will find an online GDPR Assessment tool that will allow you to privately benchmark your readiness for the GDPR and recommendations for next steps.

Given how much may be involved, you should not wait any longer to prepare until GDPR enforcement begins. You should review all of your privacy and data management practices now. The balance of this white paper focuses on how the Microsoft 365 technology platform complies with regulations and standards like the GDPR as well as the capabilities and recommended practices that can accelerate your GDPR compliance journey.

This will likely address most of the data and business processes that directly concern your employees and direct work force. The goal of this white paper is to help you simplify those common aspects of productivity including email, chat, documents, etc. and will need to be incorporated into your overall compliance program that addresses every data subjects you collect personal data on. Microsoft 365 is perhaps the most comprehensive product offering that will help you address many of your GDPR technology requirements.

Regardless of your needs, Microsoft is committed to GDPR compliance across our cloud services when enforcement begins May 25, 2018, and has provided GDPR related assurances in our contractual commitments

Personal and Sensitive data

As part of your effort to comply with the GDPR, you will need to understand how the regulation defines personal and sensitive data and how those definitions relate to data held by your organization. Based on that understanding you will be able to discover where that data is created, processed, managed and stored.

The GDPR considers personal data to be any information related to an identified or identifiable natural person. That can include both direct identification (e.g., your legal name) and indirect identification (i.e., specific information that makes it clear it is you the data references). The GDPR makes clear that the concept of personal data includes online identifiers (e.g., IP addresses, mobile device IDs) and location data where the EU Data Protection Directive had previously been somewhat unclear.

The GDPR introduces specific definitions for genetic data (e.g., an individual's gene sequence) and biometric data. Genetic data and biometric data along with other sub categories of personal data (personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; data concerning health; or data concerning a person's sex life or sexual orientation) are treated as sensitive personal data under the GDPR. Sensitive personal data is afforded enhanced protections and generally requires an individual's explicit consent where these data are to be processed.

Information relating to an identified or identifiable natural person (data subject) - examples

- Name
- Identification number (e.g., SSN)
- Location data (e.g., home address)
- Online identifier (e.g., e-mail address, screen names, IP address, device IDs)
- Pseudonymous data (i.e., using a key to identify individuals)
- Genetic data (e.g., biological samples from an individual)
- Biometric data (e.g., fingerprints, facial recognition)

Your GDPR Compliance Journey

The GDPR defines two important roles – that of "controller" and "processor" – and your organization may fall under either one or both of these definitions. A "controller" alone or jointly with others, determines the purposes and means of the processing of personal data whether on-premises or while using a third-party cloud provider's IT technology, whereas a "processor" processes personal data on behalf of a controller.

While an organization cannot be both a controller and a processor of the same data, it is possible for an organization to be a controller of one set of data and a processor of yet another. For example, Microsoft is a controller with respect to personal data that it collects from its employees and its consumer service offerings like Bing. However, Microsoft is a also processor with respect to personal data that its commercial customers collect and Microsoft processes on their behalf (such as through solutions like Office 365). With respect to data sets where Microsoft is the controller, Microsoft is directly responsible for responding to data subject requests under the GDPR. With respect to data sets where Microsoft is the processor, Microsoft ensures that its commercial customers (who are the controllers) are using a trusted platform and have the capabilities needed to respond to such requests.

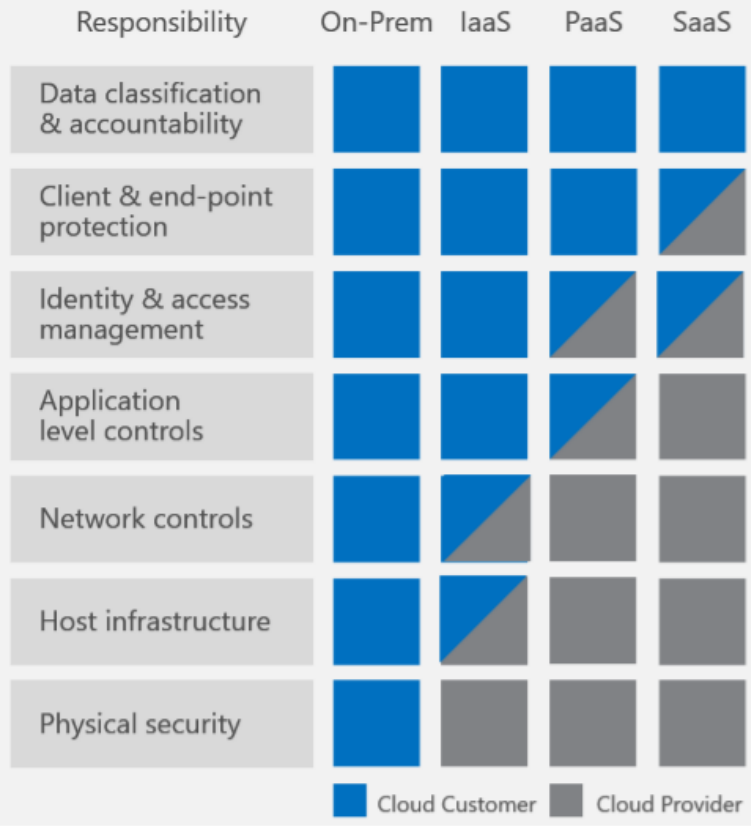
To this end, Microsoft 365 already provides capabilities that can help you identify what personal data you have and where it resides; govern how personal data is used and accessed; establish security controls to prevent, detect, and respond to vulnerabilities and data breaches; and will be extending those capabilities to enable organizations to better manage their own data subject requests, address data breaches, and provide regulators with necessary compliance documentation.

Within your organization, you will need to assign multiple roles and responsibilities to address all aspects of the GDPR. Regardless of how your organization's governance program is structured, it will be necessary for every team to understand the part it plays in maintaining compliance. For example:

- Users must be trained to handle data in appropriate ways
- Security must protect the data
- Compliance must ensure the controls are in place
- IT needs to implement and manage the systems
- Business needs to set policies and objectives

Shared Responsibility

Because your IT landscape may reside in various environments ranging from on-premises, to mobile devices, and on to cloud services, you may find that you need to share responsibilities in key areas such as: Client & Endpoint Protection, Identity & Access Management, and Application Level Controls. These environments and shared responsibilities are shown graphically here.



Software as a Service (i.e., SaaS) solutions such as Office 365, Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) platforms such as Azure, and On-Premises solutions such as Windows Server should be viewed and managed as holistically as you consider your GDPR responsibilities.

Microsoft is the only vendor to offer customers real "hybrid Cloud" configurations of Client, Server and Online Services across the most complete productivity portfolio. In our whitepaper titled, "Shared Responsibilities for Cloud Computing," we use the NIST definition of service models to define our responsibilities across SaaS, PaaS, IaaS and On-Premises software across 7 control areas shown graphically, above.`.

Microsoft is responsible for the platform including services offered, and seeks to provide a cloud service that can meet the security, privacy, and compliance needs of your organization.

As a customer, you are responsible for the environment once the service has been provisioned. You need to identify which controls apply to your business, and understand how to implement and configure them to manage security and compliance with applicable regulatory requirements.

GDPR is one of many regulations, as well as industry standards, that your organization may be required to meet and why Microsoft has a long history been investing more in security and compliance. There are ISO standards for information security management (ISO/IEC 27001) and for cloud privacy (ISO/IEC 27018) We implemented a security standard designed to prevent fraud through increased control of credit card data (PCI DSS) and supported a US healthcare law that establishes requirements for the use, disclosure, and safeguarding of individually identifiable health information (HIPAA).

Compliance Controls

Many organizations will choose to demonstrate their compliance with the GDPR, as well as other regulations and standards, by documenting and implementing a set of Controls that define specific steps the organization takes to address each aspect of a given regulation. These Controls cover all aspects of compliance including people, process and technology, although in the content of Shared Responsibility, they can be divided up into different types with regards to their responsibilities.

- Customer owned and implemented: Generally, concern the roles & responsibilities, such as assigning a Data Protection Officer that not technology-related.
- Customer owned, implemented with vendor: These relate to customer responsibilities such as data classification and access conrol that are implemented through a technology solution such as Azure Information Protection and Azure Active Directory.
- CSP owned and implemented: These relate to managing and protecting the underlying infrastructure through Roles Based Access Controls and the physical security of our datacenters. Microsoft provides records of our audits for these services here: https://aka.ms/auditreports

Demonstrating compliance means creating, implementing and maintaining an audit record of the controls in each of these three tiers once in a way that allows you to map them to any standards and regulations you need to address without the inefficiencies creating separate efforts for every new regulation that your organization may become subject to. The GDPR, given its security and privacy breadth is a good foundation for the establishment of these enterprise controls.

Of importance related to the GDPR are the responsibilities associated with compliance obligation, data classification & accountability. This paper is written from the perspective of a customer taking advantage of all Microsoft 365 Enterprise services, both as a cloud service provider as well as vendor of specific technologies and could be used as a framework of best practices for how you would approach incorporating supported Hybrid and On-Premises configurations into your overall GDRP governance program. In both on-premises and cloud models, you are accountable to ensure data is securely identified, labeled, and correctly classified to meet any compliance obligation. Distinguishing between customer data that is sensitive and/or contains personal data must be done by you.

A data classification approach as outlined in the Data Classification for Cloud Readiness white paper can be used as a starting point. SaaS solutions such as Office 365 offer capabilities to protect your data, such as encryption and Data Loss Prevention, but ultimately you must manage, classify, and configure the solutions to address their unique security and compliance requirements.

Likewise, client & end-point protection is a responsibility that will fall to you as you look at protecting data under the requirements of the GDPR. As more diverse devices are used, it is also essential that clear boundaries be defined, and responsibilities identified for the devices that are used to connect with a cloud service. CSPs may facilitate capabilities to manage end-point devices. For example, Microsoft Intune provides secure device management, mobile application management, and PC management capabilities. However, using a mobile management solution will still require customer accountability for their users.

Accelerating your GDPR compliance journey with Microsoft 365

While the specific solutions and technologies that Microsoft 365 provides can assist in your compliance with the GDPR, there are elements of how we develop and deliver these technologies that are equally important. We start with an overview of what is Microsoft 365 and then go into the distinct elements that accelerate your GDPR compliance journey:

- Choosing a platform you can trust, and verify
- Simplifying your approach to information governance
- Using intelligent tools to help discover and control data
- Leveraging the expertise of our community

What is Microsoft 365?

Microsoft 365 Enterprise is a complete, intelligent solution, including Office 365, Windows 10 Enterprise, and Enterprise Mobility + Security, that empowers everyone to be creative and work together, securely. Even before the GDPR takes effect, information loss is already the most expensive consequence of cyber-crime, closely followed by business disruption and loss of employee productivity.

Sophisticated organizations are choosing Microsoft 365 Enterprise for unmatched security protection and unique intelligence that only we can offer. It keeps customer data secure, without impeding productivity, so people can focus on what's important. Complete details are available at https://www.microsoft.com/microsoft-365, here are some of the key capabilities within Microsoft 365 that make it the most complete, intelligent and secure platform for digital work:

- **Office 365**
    - **Office 365 Pro Plus**: offers enterprise users the broadest and deepest set of always up-to-date productivity tools across all their devices, including Word, Excel, PowerPoint, Outlook, and many more.
    - **Microsoft Teams**: is a hub for teamwork, built on chat for today's work force with video and calling
    - **Exchange Online**: provides a rich, business-class email experience on all devices with bigger and more reliable mailboxes, better collaboration with document sharing with enhanced archiving, security, and compliance features
    - **SharePoint Online**: empowers individuals and teams to intelligently discover, share, and collaborate on content from anywhere and on any device
    - **OneDrive for Business**: Secure file sharing and storage solution for all users
    - **Skype for Business Online**: Enterprise-ready unified communications platform
    - **Advanced Threat Protection:** Zero-day threat and malware protection
    - **Advanced Security Management:** Enhanced visibility and control

    - **Threat Intelligence:** Actionable insights to global attack threats
    - **Advanced Data Governance:** Automatically classifying sensitive data with labels
    - **Advanced eDiscovery:** Identifying the relevant data quickly
    - **Customer Lockbox:** enhanced customer data access controls
- Windows 10
    - **Enterprise Data Protection**: Prevent accidental leaks by separating business and non-business data.
    - **BitLocker:** Protects data at rest by encrypting the computer's storage volume.
    - **Windows Hello for Business**: Enterprise grade biometric and companion device login.
    - **Credential Guard**: Protects user access tokens in a hardware-isolated container.
    - **Device Guard and AppLocker:** Device locked down to only run apps deemed as trustworthy.
    - **Advanced Threat Protection**: Behavior-based, attack detection, built-in threat intelligence, forensic investigation and mitigation built into Windows.
- Enterprise Mobility + Security
    - **Azure Active Directory:** delivers multi-factor authentication; access control based on device health, user location; and, holistic security reports, audits, and alerts.
    - **Microsoft Advanced Threat Analytics**: Identify suspicious activities & advanced targeted attacks before they cause damage
    - **Microsoft Cloud App Security**: Bring enterprise-grade visibility, information protection, and threat protection to your cloud applications.
    - **Microsoft Intune**: Mobile device and app management to protect corporate apps and data on any device.
    - **Azure Information Protection**: Encryption for files across storage locations with cloud based file tracking, and intelligent classification, labeling and protection for sensitive information like personal data.

Choose a platform you can trust, and verify

The world we live in is increasingly complex. Technology has been an engine of change in our world for many, many years, enabling people to accomplish new goals and achieve new efficiencies. With this new technology comes new challenges and public debates. Digital technology has enabled us to innovate faster and more cost-effectively. And, all of this opportunity and enablement has created a complex new environment. The rules and regulations, like the GDPR, that we use to govern technology are also evolving , creating complicated requirements with sometimes blurry boundaries and outcomes.

Connected devices and services have provided organizations with valuable data on individuals, creating new opportunities to personalize service and drive new business models. This has simultaneously raised new security and privacy concerns which the GDPR is responding to. In many cases, this data collection evolved over years across multiple IT systems with variable levels of security and compliance. It doesn't matter whether data is created, processed, stored, managed and protected on desktops, mobile devices, on-premises servers, or in the cloud; the GDPR essentially holds your organization to the same standard across all of your IT environments.

The most direct way to simplify your GDPR compliance journey is to consolidate whatever multitude of independent technologies that provide your necessary business capabilities into as few platforms as possible – thus reducing the total cost and complexity of implementing appropriate security and compliance controls. Relying on a technology platform from data processor can also significantly reduce the effort required to demonstrate compliance. The GDPR expects data controllers that utilize processors to ensure they have the sufficient expert knowledge, reliability, and resources to implement the technical and organizational measures to meet the requirements of the GDPR. In other words, you need platforms that you can trust on your GDPR compliance journey, but also one that can help you verify that the appropriate controls are in place.

Trust Principles

The Microsoft 365 platform and all its applications been developed with privacy and now the GDPR in mind. The Microsoft Cloud, where you are trusting much of your data and getting the benefit of intelligent discovery and protection capabilities, is built on the following principles:

- **Security.** We take your security very seriously—we spend over a billion dollars a year on our security practices and technologies. Our comprehensive approach to security helps protect your data wherever it may be—in the datacenter, on a phone, on a desktop, or en route through the Internet. Get access to penetration testing results and technical security whitepapers at https://aka.ms/trustdocs
- **Privacy and control.** At Microsoft, we fundamentally believe that customers' data is their own data, whether it sits in our cloud or in their own datacenter. We invest heavily in technology development and practices to ensure we actively protect your privacy and provide the necessary tools to control both the privacy and administrative aspects of your data.
- **Compliance.** Our extensive experience working with the world's largest governments and enterprises in the most highly regulated industries has been transferred to our products. Since the law was introduced last year, we have been making GDPR-specific investments in compliance-related technology, resources, and staff to help our customers prepare for the enforcement milestone. We have a long history of partnering with regulators and standards bodies to increase digital privacy and safety. You can download audit reports and other compliance documents from our Service Trust Portal at https://aka.ms/auditreports
- **Transparency.** Transparency plays an important role in developing trust—we work tirelessly to increase not only our own transparency, but the transparency of the industry and its regulators. We publish reports detailing government requests for customer data. We notify individual customers when the government requests data from their data or applications when legally

allowed to do so. Finally, we submit to a set of third-party audits and publish the results for our customers.

- **Reliability.** Microsoft invests in state of the art hardware and infrastructure to meet customers' immediate needs and anticipate future requirements. We provide world-class availability, recovery and backup capabilities for organizations around the world with industry-leading, financially-backed uptime commitment. We proactively publish service health information for increased access to key availability information.

The GDPR is nothing new to Microsoft as we already offer the most comprehensive set of compliance offerings of any cloud service provider and can help your organization comply with many national, regional, and industry-specific requirements governing the collection and use of customer data,

Microsoft cloud services operate with a cloud control framework, which aligns controls with multiple regulatory standards. We design and build our cloud services using a common set of controls, which streamlines compliance across a range of regulations not only for today, but for tomorrow as well. Then we engage independent auditors to perform in-depth audits of the implementation and effectiveness of these controls. Visit the Service Trust Portal at https://aka.ms/trustdocs to find further resources.

Operational Security

Microsoft 365 is a security-hardened service, designed following the Microsoft Security Development Lifecycle. We bring together the best practices from two decades of building enterprise software and managing online services to give you an integrated software-as-a-service solution.

At the service level, Microsoft 365 uses the defense-in-depth approach to provide physical, logical, and data layers of security features and operational best practices. In addition, Microsoft 365 gives you enterprise-grade user and admin controls to further secure your environment. The (5) five areas outlined below provide you with the highlights of operational security underpinning Microsoft 365.

Physical security

- 24-hour monitoring of datacenters.
- Multi-factor authentication, including biometric scanning for datacenter access.
- Internal datacenter network is segregated from the external network.
- Role separation renders location of specific customer data unintelligible to the personnel that have physical access.
- Faulty drives and hardware are demagnetized and destroyed.

Logical security

- Lockbox processes for a strictly supervised escalation process greatly limit human access to your data. Learn how to activate Lockbox.
- Servers run only processes that are whitelisted, minimizing risk from malicious code.
- Dedicated threat management teams proactively anticipate, prevent, and mitigate malicious access.

- Port scanning, perimeter vulnerability scanning, and intrusion detection prevent or detect any malicious access.

Data security

- Encryption at rest protects your data on our servers.
- Encryption in transit with SSL/TLS protects your data when it's transmitted between you and Microsoft.
- Threat management, security monitoring, and file/data integrity prevent or detect any tampering of data.
- Exchange Online Protection provides advanced security and reliability against spam and malware to help protect your information and access to email.

User controls

- The new Office 365 Message Encryption capabilities allow users to send encrypted and rights protected emails to anyone, whatever email service recipients may use.
- Data loss prevention can be combined with Rights Management and Office 365 Message Encryption to give greater controls to your admins to apply appropriate policies to protect sensitive data.
- S/MIME provides message security with certificate-based email access.
- Azure Rights Management prevents file-level access without the right user credentials

Admin controls

- Multi-factor authentication protects access to the service with a second factor such as phone.
- Data loss prevention prevents sensitive data from leaking either inside or outside the organization while providing user education and empowerment.
- Built-in mobile device management capabilities allow you to manage access to corporate data.
- Mobile application management within Office mobile apps powered by Intune provides granular controls to secure data contained in these apps.
- Built in antivirus and antispam protection along with advanced threat protection safeguard against external threats.
- Office 365 Advanced Security Management provides enhanced visibility and control into your Office 365 environment.

Operational security also rests on a set of principles, including data protection by design and by default, that are specially cited in the GDPR (Article 25). Find information about this and our other principles on the Microsoft Trust Center at https://Microsoft.com/Trust.

When you entrust your data to Office 365, you remain the sole owner of that data: you retain the rights, title, and interest in the data you store in Office 365. It's our policy to not mine your data for advertising purposes or use your data except for purposes consistent with providing you cloud productivity services. That means that you are the owner of the data; Microsoft is the custodian or processor of your data. It's

your data, so if you ever choose to leave the service, you can take your data with you. This helps address data portability requirements within the GDPR. And, we do not mine your data for advertising purposes.

As a processor within the definitions outlined in the GDPR (Article 4), we use your data only for purposes consistent with providing you services you pay us for. Microsoft Engineers do not have standing access to any service operation. As a cloud services provider, we recognize that organizations understandably want to have full control over access to their content stored in cloud services. With Customer Lockbox for Office 365, you have unprecedented control over the content in your service.

The privacy controls built into Office 365 enable you to configure who in your organization has access and what they can access. Further, the design elements of Office 365 prevent mingling of your data with that of other organizations using Office 365.There is also extensive auditing and supervision to prevent administrators from getting unauthorized access to your data.

Data Resiliency and Residency

Given the complex nature of cloud computing, Microsoft is mindful that it's not a case of *if* things will go wrong, but rather *when*. We design our Microsoft 365 cloud services to maximize reliability and minimize the negative effects on customers when things do go wrong. We have moved beyond the traditional strategy of relying on complex physical infrastructure, and we have built redundancy directly into our cloud services.

We use a combination of less complex physical infrastructure and more intelligent software that builds data resiliency into our services and delivers high availability to your organization. This type of resiliency is critical to your ability to meet the requirements of the GDPR.

Resiliency refers to the ability of cloud-based services, such as Microsoft 365, to withstand certain types of failures and yet remain fully-functional from the customers' perspective. Data resiliency means that no matter what failures occur within Microsoft 365, your customer data, including any personal information, remains intact and unaffected. To that end, Microsoft 365 services have been designed around five specific resiliency principles:

- There is critical and non-critical data. Non-critical data (for example, whether a message was read) can be dropped in rare failure scenarios. Critical data (for example, customer data such as e-mail messages) should be protected at extreme cost. As a design goal, delivered mail messages are always critical, and things like whether a message has been read is non-critical.
- Copies of customer data must be separated into different fault zones or as many fault domains as possible (e.g., datacenters, accessible by single credentials (process, server, or operator)) to provide failure isolation.
- Critical customer data must be monitored for failing any part of Atomicity, Consistency, Isolation, Durability (ACID).
- Customer data must be protected from corruption. It must be actively scanned or monitored, repairable, and recoverable. Data security capabilities such as these are important elements contained in the GDPR.

- Most data loss results from customer actions, so allow customers to recover on their own using a GUI that enables them to restore accidentally deleted items. And, how you manage this access through Microsoft 365 is important to your ability to comply with the GDPR.

Through the building of our cloud services to these principles, coupled with robust testing and validation, Microsoft 365 is able meet and exceed the requirements of customers while ensuring a platform for continuous innovation and improvement. Coupled with data resiliency is data residency where you can control where your data, including any personal data, is stored.

In answer to the question, "where is my data located?", you can view a set of interactive data maps that provide specific geographic details about where your organization's data is stored in Microsoft Office 365 and Microsoft Dynamics 365. Among the questions that you will find answers to on the data location page are the following, providing transparency regarding your organization's data:

- Does Office 365 disclose information about where data is stored?
- Where might customer data be transferred to, processed, and/or stored?
- Why would Microsoft move data to a different geo from my own?
- Will Microsoft give notice when customer data is transferred to a new country?
- Where are Office 365 datacenters located?

New Multi-Geo Capabilities in Office 365 enable a single tenant to span multiple Office 365 datacenter geographies (geos) to store data at-rest and on a per-user basis in customer specified geos. Multi-Geo helps customers address organizational, regional, and local data residency requirements and enables modern collaboration experiences for their globally dispersed employees. Learn more about Multi-Geo here.

In addition to our global network of datacenters, Microsoft cloud services are available in three separate national clouds. These national cloud versions are physical and logical network-isolated instances of Microsoft enterprise cloud services, which are confined within the geographic borders of specific countries and operated by local personnel. Compliance offerings for national clouds may be audited and maintained separately from global public cloud services.

Microsoft makes these services available in the national clouds:

- Microsoft Azure in-scope services offer hyperscale computing, storage, networking, and identity management. Azure safeguards data in the cloud at the government-required level of security, privacy, control, compliance, and transparency.
- Microsoft Dynamics 365 is a cloud-based customer relationship management (CRM) solution that equips government employees with data reporting, modeling, and workflows, while offering security features that can limit access to sensitive data.
- Microsoft Office 365 combines a defense-in-depth approach to security, rich data-protection tools, and an enterprise-grade compliance framework to provide a secure cloud-based productivity experience for government employees.

Simplify your approach to information governance

The amount of electronic data being created by organizations is growing exponentially. This growth is being driven by an ever-increasing number of sources and the data being generated now is more complex than ever. As your business grows, staying compliant in a sea of new global regulations adds new layers of complexity. The nexus of these two forces has made data governance, regulatory compliance and eDiscovery some of the most essential business priorities in IT.

Many organizations are exposing themselves to unnecessary risk because they don't have a good grasp on all the data they have. For example, many organizations continue to retain the personal information of former employees who left the company long ago. Were this data to be compromised in a breach, the company could be liable for costly remediation, such as lifetime credit monitoring for these former employees.

While following compliance, legal and overall governance requirements, organizations must still get business done. Ensuring that users can quickly access the appropriate information, when and how they need it, is paramount to staying in business. The ability to actively find information quickly, share knowledge, and make informed decisions can determine an organizations ability to remain agile.

Finally, it is essential to consider how you protect content from global cyber threats, and the very visible impact of leaks and breaches.

Ultimately, your compliance with the GDPR will be determined by how effective your data governance program is. Your enterprise needs to protect its content and be prepared for internal audits, external litigation, regulatory data requests, and e-discovery. Human beings, using manual processes, just cannot keep up with this given the likely explosion of personal data across the organization.

Microsoft offers a unique approach with in-place solutions that don't require additional steps and risk to meet the various requirements of different teams. With our advanced processing capabilities, we can draw correlations and take actions within the data in a way that an individual would not be able to. We have brought these together in a single place, called the Office 365 Security and Compliance Center, to help you meet your organization's data governance needs.

Illustration of the Office 365 Security & Compliance Center

To help you address the challenges of today's complex compliance landscape, including the GDPR, Microsoft 365, provides built in capabilities that give increase your ability to discover and govern the data necessary to meet your compliance needs.

Microsoft Information Protection

Data is travelling between users, devices, apps and services more than ever before. Protecting your perimeter, users or devices does not guarantee protection of your data as it travels outside of corporate boundaries. You need a unified approach and streamlined process to detect personal data, and apply the right controls. All while ensuring that end user productivity is not negatively impacted. For you, the GDPR may well be the most important compliance matter facing you over the next year or so. There are certain steps that you can take to protect your sensitive information, such as the personal data of individuals, and accelerate your compliance with your internal requirements as well as regulatory bodies or the GDPR.

We can make the information protection lifecycle a little more concrete by following the journey of a typical document or file.

It all starts with **data creation** or origination. This can occur at any number of locations, device types or services. For example, a user in your organization may create an Excel spreadsheet in Office 365 while on their Surface pro. If you are just getting started storing data in a cloud service, your user may be importing a bulk of data into the service from another location.

For this data creation phase, it's important to consider what kind of baseline encryption is offered by the service you are using – for both data at rest and data in transit. If the data resides on a device or drive, it's also important to consider if that device requires full-disk encryption to protect in that event that the device is lost or stolen.

After data is created or originated, the next natural step is to scan and **detect** sensitive data as it moves across devices, apps and services. In most environments, only a small percentage of the entire corpus of data contains sensitive information. The key is to be able to identify and detect the data that contains the sensitive or important information you care about.

Once sensitive data is detected and identified, you want to be able to **classify and label** that data in a manner that reflects its sensitivity. Even if the data is considered sensitive, they are typically different levels of sensitivity, and you may want different actions to be applied based on the level of sensitivity.

For example, getting back to the example Excel file, if it contains employee ID numbers it may be labeled as Confidential, whereas if it contained Social Security Numbers, it may be labelled as Highly Confidential. It's important that you have the granularity you need to detect and label the different kinds of documents in your environment based on the varying degrees of sensitivity.

Once the data has been stamped with a sensitivity label, your company can have the desired **policy** automatically applied to the document. Based on the policy defined by your company, any number of protective actions can be taken, such as encryption, restricting access rights, applying visual markings or a watermark, applying a retention or deletion policy, OR a DLP action such as blocking sharing. A critical step in the overall information protection strategy is defining the policies and actions to take, while also ensuring end-users can get their jobs done.

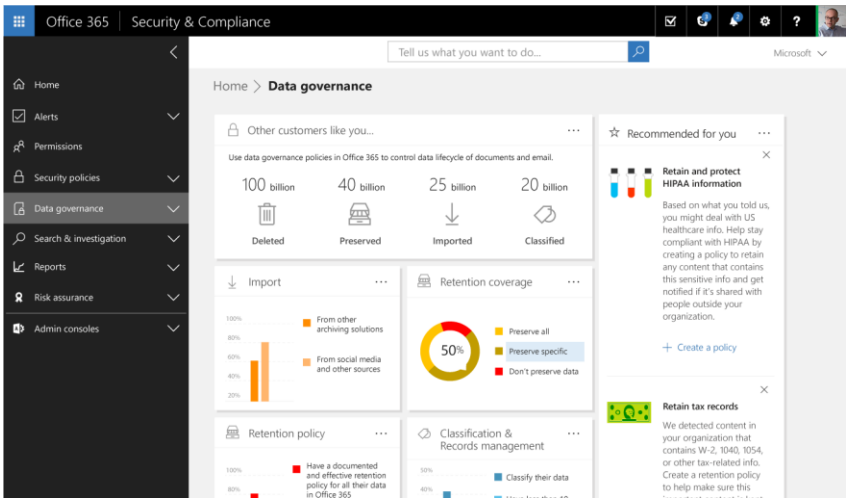
Of course, files and data often don't stay in one location. Users may need to share the information with others, both inside and outside of the organization, in order to collaborate and get their work done. For example, information may be emailed, access to the file may be shared or the information may be moved to another service. It's important in the information protection lifecycle that protection persists with the data, no matter where it travels. If the Excel file has a classification of "Highly Confidential" and sharing is restricted, and lives in SharePoint Online, that label and protection should persists if a user happens to move the file to Box, for example.

Whether the data stays or one place or moves around, it's critical that IT has the ability to **monitor** data access and sharing, usage and respond quickly to potential abuse or threats. This can be in the form of real time alerts, emails or reporting dashboard.

Finally, depending on the sensitivity of data and corporate defined policy, as the data ages it is subject to **expiration, retention and deletion**. This is an important aspect of overall information protection, because if sensitive data persists in the environment longer than necessary, it can pose a potential risk if discovered and compromised.

This is a brief view of the overall information protection lifecycle using the life of a file as an example. As you can see, there are key considerations to evaluate at each step.

Advanced Data Governance applies machine learning to help customers find and retain important data while eliminating trivial, redundant and obsolete data that could cause risk if compromised.



Advanced Data Governance delivers the following capabilities:

- Proactive policy recommendations and automatic data classifications that allow you take actions on data—such as retention and deletion—throughout its lifecycle.
- System default alerts to identify data governance risks, such as "Unusual volume of file deletion," as well as the ability to create custom alerts by specifying alert matching conditions and threshold.
- The ability to apply compliance controls to on-premises data by intelligently filtering and migrating that data to Office 365.

If you are a data controller as defined by the GDPR, you are responsible to determine the purposes, conditions and means of the processing of personal data, and that extends to your oversight of any data processors you may have engaged. With growing number of Software as a Service (SaaS) apps used in your environment, you may have personal data stored and processed in both sanctioned and non-sanctioned cloud apps. Discovering data stored in the cloud may be complex.

More than 80 percent of employees admit using "non-approved" SaaS apps and less than half are concerned that their use of unapproved software could lead to data loss[1]. But you are still responsible for personal data that may be created, processed, managed, and stored in apps obtained by what is often called "shadow IT". The more visibility and control you have into your environment, the more you can keep it safely secured and the better you can meet the security requirements of the GDPR.

Service encryption with Customer Key – We recently announced the availability of service encryption with Customer Key, which can help regulated customers demonstrate additional compliance controls by managing the encryption keys for their Office 365 data. Here is an example of how Customer Key works in SharePoint Online.

Microsoft Cloud App Security is a comprehensive service providing deep visibility, granular controls and enhanced threat protection for your cloud apps. It identifies more than 15,000 cloud applications in your network—from all devices—and provides risk scoring and ongoing risk assessment and analytics. No

[1] *The Hidden Truth Behind Shadow IT*, published in November 2013 by Stratecast, a branch of Frost & Sullivan.

agents required: information is collected from your firewalls and proxies to give you complete visibility and context for cloud usage and shadow IT.

To better understand your cloud environment, Cloud App Security investigate feature provides deep visibility into all activities, files and accounts for sanctioned and managed apps. You can gain detailed information on a file level and discover where data travels in the cloud apps.

Use intelligent tools to better discover and control your data

With the explosion of data and its increasing value – many organizations cannot adequately manage their assets with traditional manual processes. You organization needs tools to track where personal data is stored and who has access to it. As we said previously, it becomes much simpler to implement and maintain adequate control over personal data when that data is consolidated into as few technology platforms as necessary.

Unfortunately, even once you know where all the data is and how it should be managed, you must constantly ensure it is protected from threats. The GDPR requires organizations take appropriate measures to prevent unauthorized access or disclosure and to notify stakeholders in the case of breach. Today, on average attacks exist for over 90 days in an environment prior to detection. Microsoft continues to invest in tools that help detect attacks sooner and then remediate, as well as in pre-breach attack prevention tools. We are making significant investments into capabilities to better manage and protect data stored with Microsoft 365.

To meet the various requirements of the GDPR, regardless of your business processes, you will need a technology platform that has these inherent capabilities, otherwise you will need to account for the add cost and complexity of integration and maintenance:

- eDiscovery
- Identity & Access Management
- Threat Protection
- Security Management

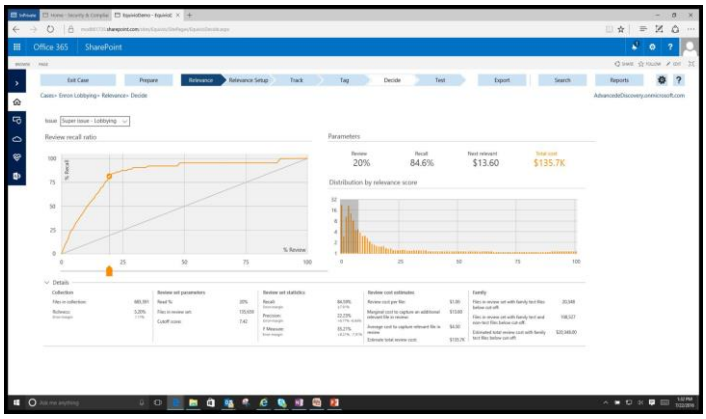
eDiscovery & Advanced eDiscovery

As organizations migrate to the cloud, they need solutions designed for the cloud from the start, not simply older tools that have been shoe-horned into this new environment. That's why our cloud first strategy requires that we build new solutions that give our customers increased efficiencies, cost savings, and security in the cloud. eDiscovery has traditionally been on premises where information is manually collected from various sources and processed to find the most relevant data. Our Office 365 eDiscovery solution brings eDiscovery to the cloud in a scalable, efficient, up to date, and secure environment.

Office 365 eDiscovery offers many benefits, including:

- **Global availability.** The Office 365 eDiscovery solution is available globally to use in any locale or situation where you need to find and access content to respond to legal and compliance needs or to an internal investigation.
- **Cost savings.** Office 365 eDiscovery helps you identify the most relevant content more quickly and easily, with far less manual review than previously possible. In legal matters, with less content to send to third-party reviewers, review costs are significantly reduced.
- **Faster responses to eDiscovery requests.** Content that you place on hold in Office 365 is preserved in place. You don't need to move it to another archive for preservation and then wait for it to be indexed before you can search it. Office 365 eDiscovery lets you quickly identify and export relevant content when you need it.
- **Less manual work.** Enhanced remediation in Advanced eDiscovery reduces the need to manually remediate unsearchable content. Also, the ability to port relevant content directly into third-party review tools eliminates the need for manual processing to enable ingestion.

Advanced eDiscovery leverages machine learning, predictive coding, and text analytics to intelligently reduce the costs and challenges of sorting through large quantities of unstructured data.



The eDiscovery process often involves sorting through thousands of email messages, documents, and other data to find the small number of files that may be relevant. Office 365 Advanced eDiscovery integrates machine learning to reduce the costs and challenges of sorting through large quantities of unstructured data.

Office 365 Advanced eDiscovery reduces the volume of data by finding near-duplicate files, reconstructing email threads, and identifying key themes and data relationships. You can also train the system to intelligently explore and analyze large, unstructured datasets and quickly zero in on what's relevant. Finally, you can export this data to third-party applications for review.

While the amount of data being generated and stored in Office 365 is growing at an exponential rate, many organizations still have data in legacy file shares and archives., Data is also being generated in other cloud services which may be relevant for an eDiscovery case surrounding a Data Subject Request. Analysis of non-Office 365 data allows organizations to import the case-specific copy of such data into a specifically assigned Azure container and analyze it using Office 365 Advanced eDiscovery. Having one eDiscovery workflow for both Office 365 and non-Office 365 data provides organizations with the consistency they need to make defensible decisions across the entire data set of a case.

Identity & Access Management

The GDPR requires organizations take appropriate measures to prevent unauthorized access or disclosure and to notify stakeholders in the case of breach. Let's start by focusing on why identity is important in the overall context of the GDPR.

Cybersecurity attacks have been a great headache for IT organizations. Even large organizations, reputable financial organizations and even governments are not immune to these threats. The nature of the cybersecurity attacks has been changing, attackers found an intelligent way to breach into the networks, by breaching into credentials. Rather than using virus or malware software, most of the time they hide under the identity of an innocent user. 81% of hacks and cybersecurity attacks are traced back to lost, weak or compromised user credentials.

Why are credentials so vulnerable? Because passwords are vulnerable. And passwords are not really the best form of access and authentication. Think about it. How many times you have used the same password to access a corporate account as well as a personal account? How old are your personal passwords? Do you use the same password for your social media and bank account? It is quite possible – because it is hard to remember several passwords when you're trying to get things done. Statistics prove this as well – 73% of passwords are duplicates. This means the users are using the same password for several accounts.

And why do we use this? Because they want to be productive, we want to get things done, wherever we are. As users, our first focus is productivity before security. 80% of employees admit using non-approved SaaS apps for work. 79% of employees work on virtual teams according to Forbes. The mobile work force has grown by 103% since 2005.

As organizations and their employees are moving to the cloud, the security strategy needs to start with a strong protected single identity at the center of the business. As we talk to customers who're moving to the cloud, we realize that they are still concerned about network security in their journey to the cloud. The reality is that as you move the cloud, the identity becomes your control plane, it is the new perimeter. As you can see the confines of the enterprise is no longer and can no longer be the perimeter of your organization. Having a strong identity and access strategy is critical to balancing security and productivity in the organization and for being the first line of defense.

A key element of the GDPR is the requirement to ensure that personal and sensitive data is adequately protected from inappropriate access. Microsoft's Identity and Access Management solution and technologies are designed to check users are authorized before granted access to data and apps. If identity is our new control plane and our perimeter, we need to protect that identities and protect our organization from identity breaches.

Here we focus on three key areas:

- **Protection at the "front door"**. No matter where you're accessing from, we will help you to protect your organization. No matter where you're coming in, we will be the first line of defense to protect your organization. So we build that security into your users experience.
- **Simplify access to devices and apps**. As we have seen the statistics earlier, users will bypass any protection if we don't make it simple. Passwords are not sustainable, they're weak and they're not the best form of authentication

- **Safeguard your credentials**. We also help you safeguard credentials, we help you protect credentials – privileged and non-privileged ones - in the first place.

Threat Protection

Whether driven by regulations such as the GDPR or not, cyber threats Cyber have become a CEO level issue. The statistics clearly indicate the adverse impact cyber threats have on today's businesses. In some instances, cyber attacks have the potential for destroying the business, so indeed, cyber security has become a CEO level issue. Even before potential fines from the GDPR are considered, look at the following statistics from Microsoft, McKinsey, Ponemon Institute and Verizon:

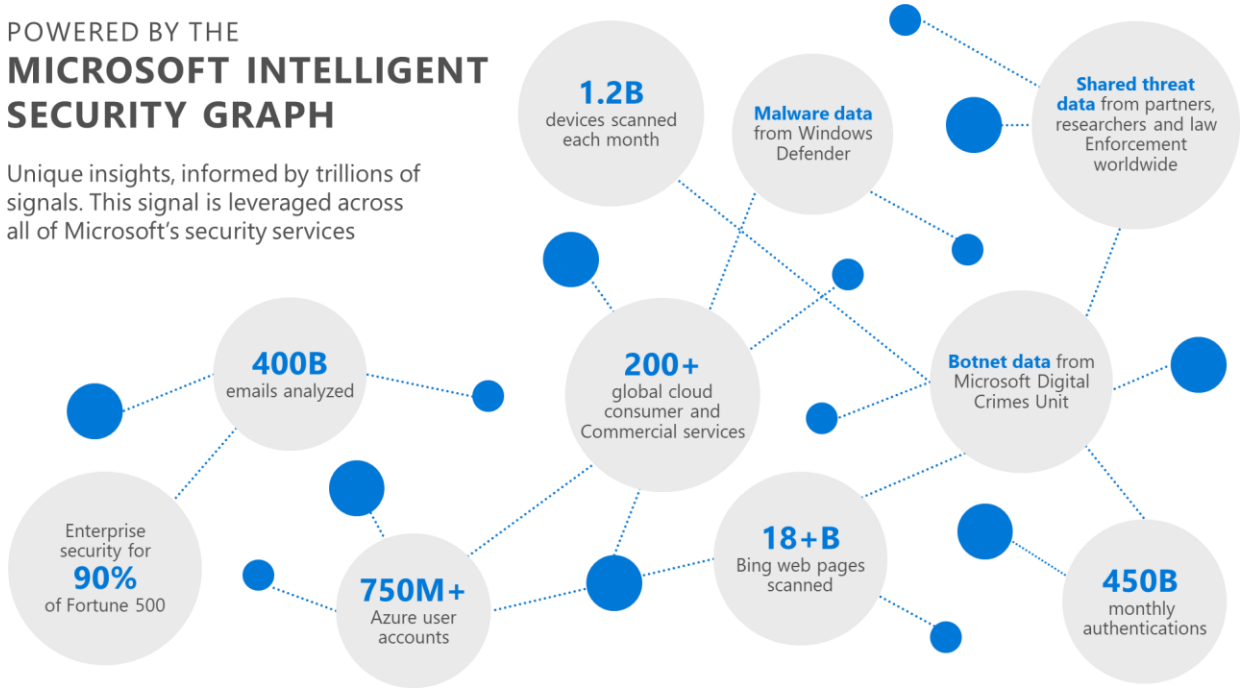
- **$4.0m** is the average cost of a data breach per incident.
- **81%** of breaches involve weak or stolen passwords.
- **>300K** new malware samples are created and spread every day.
- **87%** of senior managers have admitted to accidentally leaking business data.

As such, Microsoft has spent the last few years heavily investing in security to not only enable our you to mitigate the effects of the evolving threat landscape, but also empower you to succeed in the new norm of daily cyber-attacks.

We continue to think broadly across all the critical areas across an organization – building security into our platform as well as providing security tools and technologies to you. Acting on the Intelligence that comes from our security-related signals and insights – helps you and us to detect threats more quickly.

Fostering a vibrant ecosystem of partners who help us raise the bar across the industry – we know we're not your only security vendor, in fact you probably have 30-40 security companies you're working with. We want to work with the industry and take a holistic approach to technology.

One way that Microsoft detects cybersecurity activity in our datacenters is the Intelligent Security Graph. Microsoft has incredible breadth and depth of signal and information. We analyze from 450B authentications per month across our cloud services, 400B emails scanned for spam and malware, over a billion enterprise and consumer devices updated monthly, and 18B+ Bing scans per month.



This intelligence, enhanced by rich expertise of Microsoft's world class talent of security researchers, analysts, hunters, and engineers, is built into our products and our platform – enabling customers, and Microsoft, to detect and respond to threats more quickly.

Microsoft security teams use the graph to correlate large-scale critical security events, using innovative cloud-first machine learning and behaviour and anomaly-based search queries, to surface actionable intelligence. The graph enables teams to collaborate internally and apply preventive measures or mitigations in near real-time to counter cyber threats. This supports protection for users around the world and assures CISOs that Microsoft has the breadth and scale to monitor and protect users' identities, devices, apps and data, and infrastructure.

The massive scale of Microsoft's cloud enables us to gather an enormous amount of intelligence on malicious behaviour, which in turn allows us to prevent the compromise of accounts, and block the use of leaked or stolen credentials.

Let's look at Threat Protection using this approach and our strengths to help you be secure against advanced threats and recover quickly in the event you are attacked and to avoid the type of breaches that will result in notifications required under the GDPR. We believe the goal for threat protection should be:

- Enabling your organization to have the ability to protect yourself from advanced cyber-attacks.

- Providing you with solutions which can help detect suspicious behavior within your organization.
- Finally, since no security solution is ever 100% effective, there must be processes and tools to quickly respond to threats which enable damage control and limit the effects from an attack.

With these targeted solutions in mind, we have built threat protection security services which are ideal for today's business. To help protect organizations from advanced cyber-attacks, we have built solutions for the potential attack vectors.

- We can help secure your end-user identities where we leverage our machine learning and signal from the threat landscape to identify vulnerabilities to reduce the attack surface.
- To protect your apps and data, Microsoft has developed solutions to help secure email, data, and even your app ecosystem.
- Microsoft has solutions to help protect your devices to prevent encounters, isolate malicious threats, and to control execution of untrusted applications or code.
- We can also secure your cloud infrastructure by leveraging built-in controls across servers, apps, databases and networks

Security Management

Across industries, challenges in security management include ever increasing complexity of attack methods that ultimately leads to deployment of more solutions. You need to manage distributed resources across many environments. Given the constantly evolving threats, this means more attacks surfaces that need to be protected.

In some cases, you may end up having multiple point solutions even within a single workload to address specific security concerns. However, managing a growing number of individual security controls becomes a true nightmare. You lose full visibility into the security state of that workload, let alone the entire organizational security.

Managing many point solutions and vendors coupled with increasing 'noise' caused by diverse datasets adds to the complexity of security management and makes it even harder to gain optimal insight into end points and even less visibility to the security posture of your entire network.

Often, these point solutions don't share any information as they are not integrated, which leads to the most dangerous of these challenges: ineffective responses to threats that grow both in number and sophistication targeting your organization and your customers. More solutions to deploy, more vendors manage, with less insight and ineffective threat response ultimately manifests itself in higher costs of security for CISOs as well.

An effective security management solution is not about a single console. Effective security management integrates where it counts, but also offers specialized tools for different functions.

We can help you consolidate from many to few while ensuring that your specialized teams have the flexibility and freedom to manage their security as per the unique needs of that component, whether it is identity, devices, apps or infrastructure.

However, the key that makes Microsoft security management consoles much more effective is the intelligence sharing, which helps your organization maintain a consistent and robust security posture.

With Microsoft, intelligence is shared through the Microsoft Intelligent Security Graph. Harnessing the power of machine learning, processing trillions of pieces of data from billions of devices, we make the security management solutions work for you.

This shared intelligence is leveraged by the management consoles across Identity, Devices, Apps & Data and Infrastructure- helping security admins and operation center teams to get important information optimized for their workloads.

The key for a CISO's success in managing security is not about a single console across everything, but integration wherever it makes sense. You don't need all the point solutions to manage, data points to sift through to secure your end user devices and expanding networks.

With single vendor management, built-in controls that come with MS solutions and the unmatched intelligence, Microsoft becomes your trusted partner in achieving intelligent security management.

In short, Microsoft provides you intelligent security management with:

- Specialized Controls based on your security teams' needs;
- Visibility where needed;
- And Guidance on how to harden your organization's security posture based on unmatched intelligence.

Leverage the expertise of our community

Partner Ecosystem

In conjunction with the capabilities contained in Microsoft 365 to help you accelerate your journey to GDPR compliance, we have a professional services global ecosystem consisting of both Microsoft Services and partners. As five examples of the types of challenges these service organizations can address are the following[2]:

- Data Breach Notification - Many organizations that do business in the Europe market or with European customers will have to tackle privacy rules for the first time. Microsoft Services and other GDPR-related partners can be critical to putting these processes in place.
- Privacy-by-design - Partners can work closely with your security leaders to provide GDPR assessments and determine how Microsoft 365 and partner services can enable you to meet privacy-by-design requirements.

[2] Brief: You Need An Action Plan For The GDPR, Enza Iannopollo with Christopher McClean, Fatemeh Khatibloo, Bill Barringham, Andrew Reese, Oct 14, 2016

- Global Coverage - With 72-hour data breach notification, partners can utilize Microsoft 365 services to become an incident response (IR) orchestrator through managed services or professional services.
- Data Privacy Officer (DPO) - At least 75,000 DPOs will be required by 2018 WW[3]. Partners can provide DPO as a service to you.
- Evidence of Risk Mitigation - Per GDPR policy, organizations must demonstrate that they have implemented appropriate measures to mitigate privacy risks. Partners can help you use Microsoft 365 to build evidence of mitigation strategies and controls.

Many advanced compliance partners specialize in audit and risk governance programs, including advice regarding your responsibilities as a controller, and provide implementation assistance to deploy and fully ready your organization to utilize the various Microsoft 365 capabilities. They can work collaboratively with you to utilize many of the support materials we have developed and made available to do the following:

- Enables customer use of Microsoft controls to meet their obligation as a Data Controller
- Conducts additional assessments based on Compliance Dashboard and Compliance Companions
- Coordinates & leverages *definitive* legal advice provided by customer's or outside council
- Identifies applicable Governance, Risk, and Compliance (GRC) authority requirements
- Identifies customer data and processes requiring governance controls
- Establishes data classification taxonomy

Another group of partners specialize in the Security aspects of the GDPR and can help design, deploy and maintain solutions built with Microsoft 365. Finally, for very specific GDPR related workflow such as mapping data flows within your organization or managing all Data Privacy Impact Assessments across the organization, you can turn to ISVs who develop complementary solutions.

There are also many independent organizations, such as the International Association Of Privacy Professionals (http://IAPP.org), which provides resources to professionals responsible for implementing the GDPR. They offer multiple courses and events bringing together experts on the GDPR. Another example of their resources include a partnership with OneTrust to provide a tool that helps organizations operationalize data protection and privacy impact assessments (PIA or DPIA) in an agile, cross-jurisdictional, and GDPR compliant approach. Available at https://onetrust.com/iapp-pia/, this service is not associated with Microsoft.

Closing

The GDPR calls for enforcement to commence on April 25, 2018 and you should not delay evaluating your obligations under the regulation. Trust is central to Microsoft's mission to empower every person and every organization on the planet to achieve more. So that you can trust the Microsoft products and

[3] Study: GDPR's global reach to require at least 75,000 DPOs worldwide, Rita Heimes, CIPP/US, Sam Pfeifle, Nov 9, 2016

services you use, such as Microsoft 365, we take a principled approach with strong commitments to privacy, security, compliance and transparency. This approach includes helping you on your journey to meet the requirements of the European Union's General Data Protection regulation (GDPR).

If your organization collects, hosts or analyzes personal data of EU residents, GDPR provisions require you to use third-party data processors who guarantee their ability to implement the technical and organizational requirements of the GDPR. To further earn your trust, we are making contractual commitments available to you that provide key GDPR-related assurances about our services. Our contractual commitments guarantee that you can:

- Respond to data subject requests.
- Detect and report personal data breaches.
- Demonstrate your compliance with the GDPR.

Microsoft is the first global cloud services provider to publicly offer you these contractual commitments. We believe privacy is a fundamental right. The GDPR is an important step forward to further clarify and enable individual privacy rights and look forward to sharing additional updates how we can help you comply with this new regulation and, in the process, advance personal privacy protections.

Microsoft 365 provides the most complete, intelligent and secure solution for digital work. By bringing together the best of Office 365, Windows 10, and Enterprise Mobility + Security, we can help accelerate your journey to compliance with the GDPR by:

- Providing a platform you can trust and verify
- Simplifying your approach to information governance
- Offering intelligent tools to help discover and control data
- Leveraging the expertise of our community

Next Steps

In addition to understanding the capabilities provided to you in Microsoft 365, we recently released two new General Data Protection Regulation (GDPR) compliance assessment tools to further round out our GDPR resources already available on the Microsoft Trust Center.

Available to any business or organization, Microsoft's free GDPR benchmark assessment tool is now available online. Our interactive tool guides users through 26 questions and generates a downloadable report showing the organization's readiness to comply with the GDPR's provisions.

Available to customers through Microsoft's extensive Partner Network, our detailed GDPR readiness assessment tool provides an in-depth analysis of your organization's readiness and it offers actionable guidance on how to prepare for compliance, including how Microsoft 365 features can help simplify your journey. There are many links provided in this document that can provide details on the capabilities that Microsoft 365 can provide you as your organization moves toward GDPR compliance. Some of the key resources include the following:

There are many links provided in this document that can provide details on the capabilities that Microsoft 365 can provide you as your organization moves toward GDPR compliance. Some of the key resources include the following:

- Microsoft 365 Overview: https://www.microsoft.com/en-us/microsoft-365
- The GDPR Trust Center: https://www.microsoft.com/en-us/TrustCenter/Privacy/gdpr
- Information on the GDPR from the EU: http://ec.europa.eu/justice/data-protection/