Microsoft

Protecting your agency from risk: a holistic approach to security and compliance for government

Microsoft 365 and government

Government agencies work hard to deliver value to society. Whether the mission is to transform policy into impact, to implement programs, or deliver citizen services, the demands on government are increasing. As modern technology shifts societal behavior, citizens expect their governments to adapt accordingly. They expect you to move faster, all the while being more transparent in how you're protecting public data.

All of this is taking place in the context of eroding trust. That is, throughout much of the world, the ability to trust information has been challenged. This has resulted in declining trust in public institutions and in official information. In a context where the trustworthiness of official information and its sources is increasingly questioned, public officials have additional pressure to double down on their good stewardship of sensitive information. Additionally, the requirement to do more with a smaller budget can be a hurdle to delivering on your commitments. Providing effective services and increasing citizen confidence means managing these expectations alongside your organization's finances.

This e-book provides insight into Microsoft security and compliance solutions for government organizations to help protect your agency against cybersecurity risks associated with the sensitive information that you are stewards of.

How do you deliver the best services while protecting the sensitive data required to operate?

Are you guiding your organization to think more proactively about security—to instill trust with citizens, help ensure privacy and compliance, and help protect your agency and infrastructure against cyberattacks?

The current government landscape is complex

Being proactive in an ever-changing world while managing agency standards and public expectations

Successful governments around the world are embracing digital transformation to enhance government services, modernize the workplace, improve critical infrastructure, and engage with citizens. Program and policy implementation require communication and coordination across departments, agencies, and jurisdictions. As information travels across entities, exposure to cybersecurity threats grows.

The exponential growth of digital data has increased the surface area of vulnerability. As this data flows more freely and information is exchanged between citizens and government and across government entities, the imperative to protect data grows.

In this complex environment, government leaders themselves are being held accountable for ensuring the security and safety of sensitive information. It’s no longer sufficient to rely on IT leaders alone when agency executives are sharing the responsibility and accountability for cybersecurity publicly. Executives across the organization should become stakeholders in safeguarding their agency’s information and assets.

Security and compliance is a shared responsibility for government leaders

Understanding risks when handling sensitive data

Governments manage large volumes of data including personally identifiable information (for example, names, birthdates, driver's license records, tax information, and business filings) and top secret, confidential information that's critical for national security. This information is valuable on the black market and can be held for ransom. The disclosure or loss of personal information or attacks on government operations can have serious impacts on employees' or citizens' lives. It can erode confidence in government institutions and public trust.

Public sector organizations face a growing number of threats from increasingly sophisticated cyberattacks that often outpace their IT resources. Governments are amongst the most targeted sectors. In fact, according to a report by Verizon on 2019 Data Breach Investigations, the public sector has the highest number of incidents compared to other sectors.[1] While a majority of these incidents involve external actors in the form of cyber espionage, insiders—those with approved access—also account for a number of incidents resulting from misuse of their access or unintended errors.

While government leaders agree that security is a top priority, the cumulative effect of reactive spending on security can leave public sector agencies with trailing technology and systems that are often older and more vulnerable. Attackers are prepared to manipulate these vulnerabilities. Consider alternatively that unplanned spend on short- and long-term costs to respond to each breach can also cost you—impacting budgets and taxpayers.

The average cost of a data breach is $3.62 million.[2]

[1] Verizon. 2019 Data Breach Investigations Report.
[2] Ponemon Institute and IBM. 2017 Cost of a Data Breach Study: Global Overview. June 2017.

Proactively plan for potential risks.

New expectations for government leaders in a changing landscape

As more government employees need flexibility to work remotely, strong authentication measures are required to verify identity as work moves across devices and locations. These measures are necessary to ensure only an authorized user can access sensitive information. Additionally, controls need to be in place to automatically require additional authentication, password reset, or to limit or even block access to resources in case credentials are compromised.

Police officers, for example, are more reliant on technology to work remotely and communicate, so that they can prioritize time spent on the streets protecting citizens rather than traveling back and forth to the station. However, if an officer misplaces her device in the field, it's important that the sensitive data in her device is protected.

Sometimes the risk comes from within—from suboptimal data management. This risk is amplified with the growing requests for public records and expectations of open government. To accommodate this trend and balance the risk of unintentionally divulging sensitive data along with public records, proper data classification and governance are required. Organizations need to identify, classify, and protect sensitive information when that information is created or altered. With an appropriate inventory of data by sensitivity, data requests can be managed with confidence and agility.

The private sector in the digital economy also requires access to aggregate public information to deliver innovative services. Whether it's traffic flow sensors or new business filings, agencies need modern tools to effectively store and securely share access to these databases with authorized persons only. Transparency is important to innovation, as is the good governance of sensitive information. Governments must therefore balance the imperative to spur innovation while upholding privacy and security.

> "To support this modern, cloud-based workplace, we need to protect our environment in a new way. The move to a solid, highly secure IT environment was a big factor in our decision to adopt Microsoft 365. We feel that Microsoft meets the complex security and compliance needs of a national police service."[3]
>
> - Wim Liekens, Director of Police Information and ICT (CIO) at Belgian Federal Police

Microsoft 365: uniquely positioned to help with government

Microsoft 365 brings together productivity, security, and mobility cloud software with Office 365, Windows 10, and Enterprise Mobility + Security, empowering your employees to work together securely and productively in the modern government workplace.

Microsoft 365 helps address the needs of a modern government.
It helps enable you to:

- **Securely share information**, helping to ensure that the right people have access to the right information and that the wrong people don't accidentally leak it.
- **Protect your agency against cyberattacks.**
- Support your journey to **meet regulatory and compliance requirements.**

Microsoft is committed to building trust into all we do. That means delivering intelligent security, offering the most comprehensive set of compliance offerings, and vigorously protecting the privacy of our customers and your data to meet your expectations and needs.

Security services from Microsoft 365 are powered by the Intelligent Security Graph. To combat cyber threats, the Intelligent Security Graph uses advanced analytics to link threat intelligence and security signals from Microsoft and partners. Microsoft operates global services at a massive scale with billions of security signals that power protection layers across the stack. Machine learning models reason over all this intelligence, and the signal and threat insights are widely shared across our products and services. This allows Microsoft to detect and respond to threats more quickly, and bring actionable alerts and information to our customers for remediation. Microsoft machine learning models are continuously trained and updated with new insights, helping us build more secure products and provide more proactive security.

[3] "Belgian police move into the digital age nationwide, solve crimes faster with Microsoft 365." Microsoft 365 Blog. December 2018.

Securely sharing information intra-agency or across agencies

The implementation of policies and programs seldom happens in isolation. Employees need to exchange information with each other and outside organizations to collaborate and innovate on service delivery. This flow of information can introduce vulnerabilities. To support a new, modern workplace, you need to protect your information in new ways.

- Verify that only the right users have the right level of access to information, and automatically block or limit access if the user doesn't have the right permissions/if the identity isn't verified.
- Classify and label that data so that it can be appropriately assigned with protection policies depending on the classification. Encrypt, limit, or block access to certain pieces of information, and block or revoke access to apps or data.
- Maintain control of that information where it travels, inside and outside of your organization.

How can you securely share information and communicate effectively to move your mission forward?

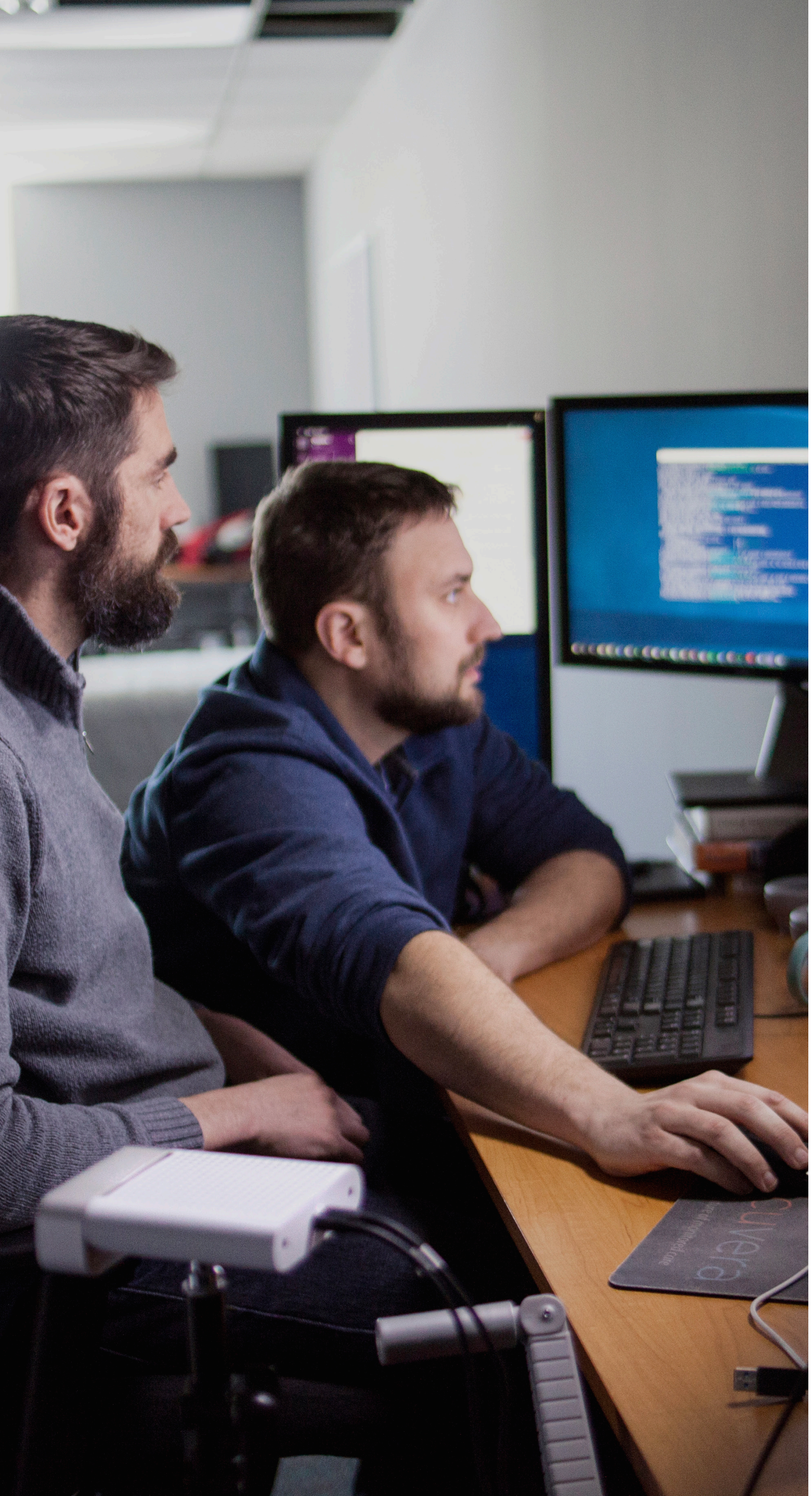
Identity and access management

Today, rather than computer and network infrastructure, end-user identity is the new security perimeter to control who has access to sensitive data; it can help verify that users are authorized before they gain access to apps and data.

Azure Active Directory (Azure AD), Microsoft's identity and access management solution, is designed to help organizations manage users and access privileges to specific systems and data sets. With Azure AD, you can set policies based on the user, location, device, and application, and risk signals to determine whether the user should be allowed, limited, or blocked from accessing resources.

Azure AD features:

- **Azure Multi-Factor Authentication.** Two-step verification to safeguard access to data and apps.
- **Passwordless authentication.** Multi-factor authentication to allow a user to sign in with a password alternative. The credential is tied to a device that uses biometric authentication (such as facial recognition or fingerprint), non-field communication, or personal identification numbers.
- **Password protection.** A safeguard against using common, compromised passwords through banned password lists and smart lockout features.
- **Conditional Access.** Manage access to apps based on status and risk level for the user, device, location, or app and apply the appropriate policies and controls.
- **Identity protection.** Calculate the risk level of users and sign-in attempts based on behavior and threat signals, analyze security logs, and get alerts on risk events.
- **Privileged identity management.** Minimize the attack surface by limiting access for privileged roles to critical operations and monitoring administrator access rights.



Information protection

Microsoft 365 information protection and governance solutions can help classify, label, and protect sensitive information to ensure that important information is only accessible by those who are authorized to receive and view the information and that critical data is not accidentally released or deleted.

Data classification based on automatic analysis
Automatically classify, protect, and govern sensitive data. Data classification and protection controls are integrated into Microsoft Office and other common applications, with one-click options that make it easy to label and classify data. Use over 90 predefined sensitive information definitions and customize your own classification and labeling templates to help ensure information protection remains persistent and travels with the data.

There are a range of protection actions you can apply to your sensitive data and define your policy to treat data with different levels of sensitivity with a different level of protection. Both Azure and Office 365 have data encryption built into the service—for both data at rest and data in transit. You can adopt a multi-layered strategy to protect sensitive data. For example, to protect individual files, you can apply rights-based permissions so that only intended recipients can access and view the information, enable policy tips that notify users of sensitive information in documents, automatically apply a visual marking, and automatically retain, expire, or delete documents based on data governance policies defined by your organization.

This means your data are identifiable and protected—regardless of where it's stored or with whom it's shared. Microsoft tools and services support information protection and governance, including **Azure Information Protection, Advanced Data Governance, Office 365 Message Encryption**, and encryption capabilities such as BitLocker.

Azure Information Protection

Azure Information Protection is a solution that enables you to discover, classify, and protect sensitive information. Azure Information Protection policy can be applied and enforced across several apps and services, including Office apps, on-premises file servers, and across cloud storage services (via its integration with Microsoft Cloud App Security).

You can use Azure Information Protection to discover and classify sensitive information using any of the 90+ out-of-the-box sensitive information definitions, such as financial data, personally identifiable information (PII), or health-related information. Policies can automatically apply sensitivity labels to documents and emails (such as "Highly Confidential") or you can empower end users to manually apply sensitivity labels to their files. Depending on your label policies, protection actions can be applied to your information, such as encryption, rights restrictions, or visual markings.

Data loss prevention

To comply with business standards, industry regulations, and consumer expectations, organizations need to protect sensitive information and prevent its inadvertent disclosure. Data loss prevention (DLP) is a compliance feature of Microsoft 365 that's designed to help you prevent the intentional or accidental exposure of sensitive information—such as date of birth, citizen identification numbers, or other sensitive data—to unwanted parties.

Email and document encryption

Office 365 Message Encryption can send encrypted emails to others—both inside and outside of the organization, to help ensure only the recipients can view the information. You can also encrypt sensitive information in Office documents via password protection or enforce additional control access rights to specific groups or individuals. This helps ensure only the right people (including employees, partners, and citizens) can access sensitive or private data.

Data encrypted at rest and in transit

Microsoft products and services use industry-standard encryption to protect critical organization data, whether it's being accessed by employees or stored at rest. Microsoft uses some of the strongest, most secure encryption methods, protocols, and algorithms across our products and services to help provide a secure path for data to travel through the infrastructure.

- **Microsoft 365 managed encryption.** Microsoft uses multiple encryption methods, protocols, and ciphers to help provide a secure path for your agency's data to travel across Microsoft 365 services—and to help protect the confidentiality of sensitive data stored within Microsoft 365 services. Service-side technologies encrypt data at rest and in transit. In Microsoft 365, service-side encryption is used by default—you don't have to configure anything.

- **Customer-managed encryption.** By adding content-level encryption, you can protect data to help ensure that only authorized users can view the protected content. To further mitigate data loss and leakage, you can apply both rights protection and encryption for emails and files in SharePoint Online.

> Microsoft uses some of the strongest, most secure encryption methods, protocols, and algorithms across our products and services to help provide a secure path for data to travel through the infrastructure.

Protecting government services against cyber threats

Security breaches and ransomware are two of the top risks for government organizations. Cybercriminals are targeting agencies by exploiting security vulnerabilities, affecting availability of services, and compromising sensitive employee, citizen, and mission data.

Microsoft Threat Protection

With Microsoft 365, you can implement a comprehensive solution to protect your organization by helping employees secure identities, emails, apps, data, and devices. You can apply analytics and intelligence to prevent threats like phishing and zero-day attacks (from unknown threats).

Microsoft recently launched the Microsoft Threat Protection solution, which is designed to secure the modern organization from the evolving threat landscape. The solution offers comprehensive, integrated security across multiple attack vectors.

- **Office 365 Advanced Threat Protection.** Safeguard your organization against malicious threats posed by email messages, links, and collaboration tools. Additionally, Advanced Threat Protection anti-phishing protection can help protect your organization from malicious impersonation-based phishing and other attacks.

- **Microsoft Cloud App Security.** Detect unusual behavior across Microsoft and third-party cloud apps to identify ransomware, compromised users, or rogue apps; analyze high-risk usage; and remediate automatically to limit the risk to your organization.

.

- **Azure Advanced Threat Protection.** Detect, identify, and investigate advanced threats, compromised identities, and malicious insider actions and generate alerts for the IT team so they can investigate further and remediate.

- **Azure Active Directory Identity Protection.** Configure risk-based policies that automatically respond to detected issues when a specified risk level has been reached.

- **Microsoft Defender Advanced Threat Protection (ATP).** Built-in and cloud-powered technology includes preventative protection, post-breach detection, automated investigation, and response. Microsoft Defender ATP protects endpoints from cyber threats, detects advanced attacks and data breaches, automates security incidents, and improves security posture.

- **Microsoft Intune.** Enables comprehensive remote management of mobile devices including remote data wipe and deployment of a user’s applications and configuration to a replacement device. Intune is integrated with Microsoft Defender ATP and other mobile threat defense partners to define an acceptable level of risk on a device and block connections from anything that exceeds that level.

- **Azure Sentinel.** See and stop threats before they cause harm, with SIEM reinvented for a modern world. Azure Sentinel is your birds-eye view across the enterprise. Put the cloud and large-scale intelligence from decades of Microsoft security experience to work. Make your threat detection and response smarter and faster with artificial intelligence (AI). Eliminate security infrastructure setup and maintenance, and elastically scale to meet your security needs—while reducing IT costs.

- **Azure Security Center.** Microsoft uses a wide variety of physical, infrastructure, and operational controls to help secure Azure—but there are additional actions you need to take to help safeguard your workloads. Turn on Security Center to quickly strengthen your security posture and protect against threats.

Control access and proactively protect against cyber threats.

Visibility into security posture

With Microsoft Secure Score in the Microsoft 365 security center, you get increased visibility and control over your organization’s security posture.

A centralized, real-time dashboard helps you monitor the protection state of data, apps, devices, and infrastructure. It delivers a numerical summary of your organizational security posture based on system configuration, user behavior, and other security-related measurements. To improve the score, this dashboard recommends prioritized improvement actions such as enabling multi-factor authentication, turning on auditing, designating less than five global administrators, and much more.

Note: Secure Score is not an absolute measure of how likely you are to experience a breach. Rather, it indicates the extent to which you have adopted controls that can offset the risk of being breached. No service can guarantee that an organization will not be breached. Secure Score shouldn’t be interpreted as a guarantee.

Get increased visibility and control over your organization’s security posture.

Meeting regulatory requirements and compliance

Adhering to regulatory compliance is paramount. This is where Microsoft can help. Our vision is centered around the idea of "built-in" compliance. Our capabilities allow you to better assess your risk, govern, and protect sensitive and mission critical data, and respond to regulatory requests with intelligence and efficiency. Furthermore, Microsoft 365 provides ongoing assessment of your compliance posture—including actionable insights to help your organization stay current. Microsoft 365 helps you assess and manage compliance risk in several ways.

Proactive tools to help you demonstrate compliance

To help ensure that organization records and citizen data remain safe and compliant, you need to continuously assess how your organization complies with changing regulatory requirements. When you move your agency's data to a cloud service, it becomes a shared responsibility between your organization and the cloud service provider to protect data and meet compliance obligations. Performing comprehensive, prioritized risk assessments spanning common workflow scenarios with awareness of organization-specific and common vulnerabilities is crucial to gain an understanding about the effectiveness of security, compliance, and privacy controls managed by your organization and cloud provider.

Respond to citizen and organization requests efficiently.

- Included with Microsoft 365, **Compliance Manager** provides an intelligent score that reflects your performance against data protection regulatory requirements. And it provides built-in collaboration tools to streamline workflows across teams and richly detailed reports of pertinent data.

- With capabilities to discover, classify, protect, and monitor, **Microsoft Information Protection** helps to better protect and govern data, in addition to responding to regulatory requests with intelligence and efficiency. Good compliance with regulations begins with proper data classification and labeling. That becomes the building block against which you and your team applies governance to manage the data according to its sensitivity. Protecting, retaining, or reporting on sensitive data follow more seamlessly when you start with good classification. This also adds agility and accuracy as you respond to citizen requests or your team needs to make data available to regulators.

- With growing demand to respond to regulatory, litigation, and data requests (such as GDPR, PDPA, and FOIA), **the Microsoft 365 e-Discovery and Data Subject Requests** capability allows you to quickly search through relevant data, produce reports, and respond to and comply with discovery or other data and documentation requests.

- **Advanced Data Governance** helps organizations identify and classify important information. It also helps create retention or deletion policies for your compliance needs.

- Advanced Data Governance includes **Records Management** to modernize records management by providing capabilities that help ensure core business records are properly declared and stored immutability with full audit visibility to meet regulatory obligations.

- As agency data is shared, tracking its flow is important. **Audit log and alerts** in Microsoft 365 can help. It includes several auditing and reporting features that customers can use to track certain activity such as changes made to documents and other items. Organizations also need to examine whether instances of sensitive data may be leaking through new communications networks. **Supervision** in Microsoft 365 can help organizations monitor employee communications channels to manage compliance and reduce reputation risk.

- **Microsoft Cloud App Security** is a cloud access security broker solution that helps detect use of native and third-party cloud applications. It helps discover cloud apps that are accessed by users, evaluates their risk level, and allows you to manage access based on organizational requirements. Microsoft Cloud App Security can help identify cloud apps for your organization that comply with regulations relevant to you, to help meet your compliance goals. More than 16,000 cloud apps have been assessed against more than 75 risk factors, including compliance and industry regulations, which will allow you to govern access accordingly.

- **Customer Lockbox** can help support compliance needs by demonstrating that you have procedures in place for explicit data-access authorization. Customer Lockbox allows you as the customer to be an active participant in any request Microsoft engineers may have to access your content while resolving an issue. With Customer Lockbox, you have control. You’re fully able to approve or reject the access request and be a part of the resolution process.

- Microsoft has built **the Service Trust Portal (STP)** as a public site for publishing audit reports and other compliance related information related to Microsoft cloud services. STP users can download audit reports produced by external auditors and gain insight from Microsoft-authored white papers that provide details on how Microsoft builds and operates our cloud services.

Partnering with Microsoft on security and compliance

As the digital landscape changes, government organizations have an opportunity to enhance government services, modernize the workplace, and improve engagement with citizens all while remaining trusted stewards of sensitive information.

Microsoft's commitment to you and your organization

Microsoft invests over $1 billion annually in developing comprehensive security and compliance solutions that unlock the potential of the intelligent cloud. We're committed to empowering organizations to digitally transform with confidence.

Keeping up with organizational security and compliance is a collective responsibility that sits not only with IT but also with leaders across the organization. To enlist everyone as stakeholders in the security and compliance journey, you need a solution that's easy to follow as you go about your daily duties.

Microsoft has invested in four areas critical to a secure digital estate: Identity and Access Management, Information Protection, Threat Protection, and Security Management. With Microsoft 365, your organization gets end-to-end, intelligent, and integrated security without impacting user productivity.

Additionally, the built-in compliance features in Microsoft 365 help you assess your compliance posture, protect and govern sensitive data, and efficiently respond to regulatory data requests.

Experience more

Learn more about Microsoft 365 and government
Learn more about Microsoft 365 security solutions
Discover ways to simplify your compliance journey through the Microsoft Trust Center

Microsoft