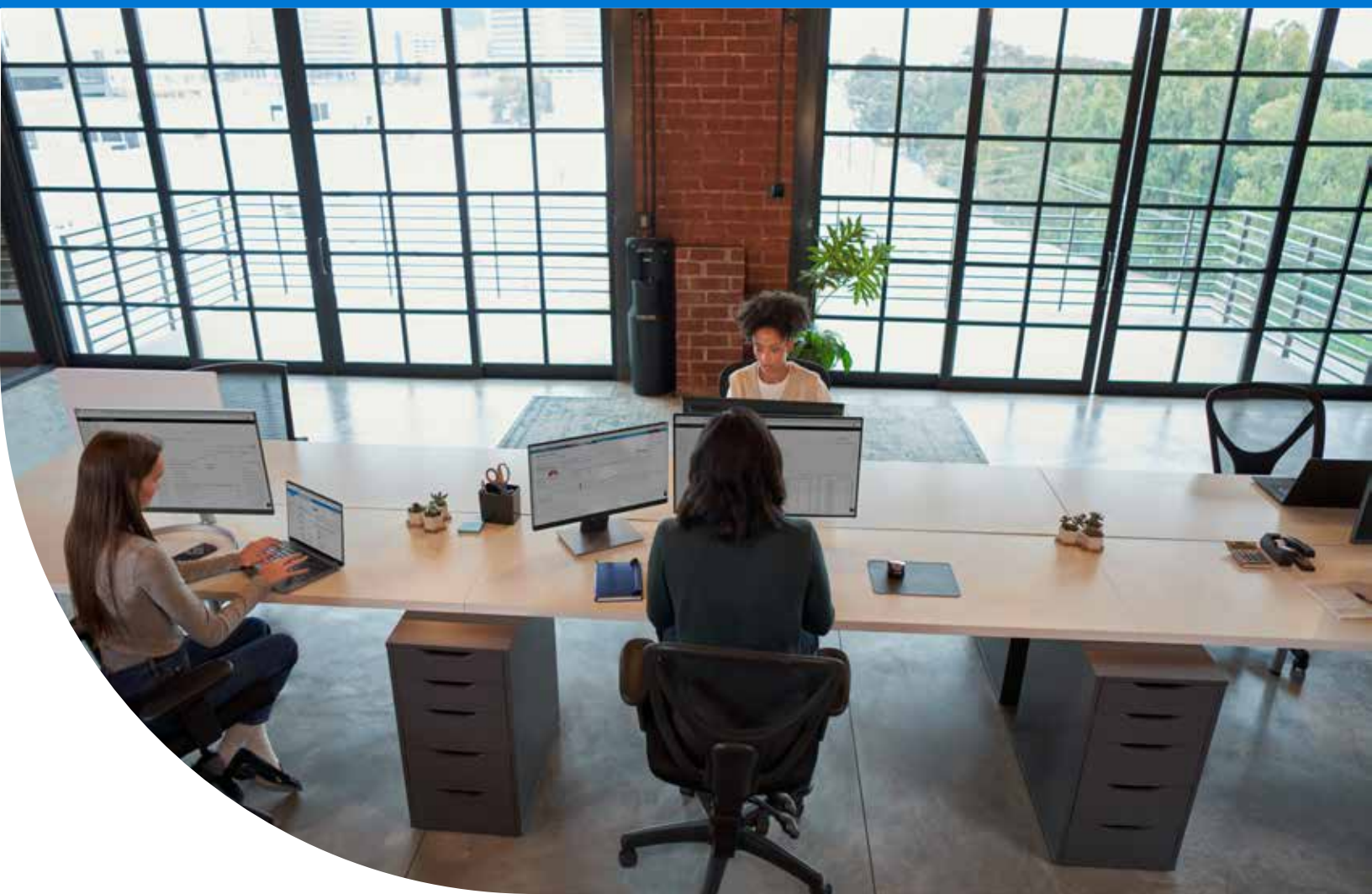
E-book Series

Microsoft Security

Safeguard your most critical assets

Ensure that you protect identities and sensitive business data



Importance of information protection and governance

Not only has digital transformation led organizations to deal with increasing volumes of data, much of that data is accessed outside the corporate network and shared with external collaborators such as partners, vendors, and customers. This shift has created a complex data landscape, especially when considering the proliferation of hybrid workforces and cloud migrations, growing cyberthreats, evolving security, and changing regulatory requirements around how data is governed and protected.

Reducing exposure and managing risk is easier when you efficiently manage the lifecycle and flow of sensitive data as part of your organization's business operations. For your security teams, the process starts with identifying critical assets, sensitive data, and who has access to it, so you're more aware of vulnerabilities and potential data exposure.

But how can you successfully monitor potential vulnerabilities when your data is used outside the traditional

On average, 78 GB of data is uploaded monthly to risky apps by enterprise organizations.

Source: Microsoft Tech Community, August 2021

Protect assets anywhere with a Zero Trust security model

With hybrid work models, corporate assets and data are on the move. Your organization needs to control wherever the data transfers—on devices, inside apps, and with partners.

In traditional networks, critical data access is governed by network perimeter control, not based on data sensitivity. Labels on sensitive data are applied manually, which results in inconsistent data classification.

For modern-day security, however, you can no longer rely on these traditional network protection controls. What you need is a Zero Trust security model to protect sensitive data where it lives while ensuring that applications work quickly and seamlessly.

An effective Zero Trust architecture reduces risk across your digital estate at every opportunity by adhering to the following principles:

Verify explicitly

Always make security decisions using all available data points, including verifying every identity, location, resource, and data classification while identifying device health and anomalies.

Use least-privilege access

Limit access with just-in-time/just-enough-access (JIT/JEA) and risk-based adaptive policies. Capture and analyze telemetry to better understand and secure your digital environment, ensuring you can discover and secure unmanaged endpoints and network devices.

Assume breach

Minimize blast radius with micro-segmentation, end-to-end encryption, continuous monitoring, and automated threat detection and response.

A Zero Trust model is a proactive, integrated approach to security across all layers of the digital estate that explicitly and continuously verifies every transaction; asserts least-privilege access; and relies on intelligence, advanced detection, and real-time response to threats.

Zero Trust principles for unified data governance and protection

A Zero Trust model helps you implement unified data protection and governance best practices to ensure proper storage, access, flow, and lifecycle. In turn, these practices support better management of your sensitive data, so it doesn't persist or propagate beyond your control. As a baseline, you need to discover sensitive data, apply and monitor the use of appropriate labels, and put into effect data loss prevention policies to protect data with more confidence.

The Zero Trust security model includes the following core elements of data governance and protection:

Know your sensitive data

Understand your data landscape and identify critical and sensitive data across your cloud and on-premises environment. Classify all data by sensitivity level.

Govern your data

Only keep and govern data that has value for your organization. Apply governance practices such as deduplicating and centralizing data with proper archival and masking for protection.

Protect your data

Protect your sensitive data throughout its lifecycle by applying sensitivity labels. Employ actions like encryption, access restrictions, visual markings, tokenizing, and more.

Prevent data loss

Apply a consistent and unified set of data loss prevention policies across your environments and endpoints to monitor, prevent, and remediate risky activities with sensitive data.

Use least privilege access

Before a user attempts to access sensitive data, verify the identity with strong authentication to ensure access is compliant and typical for that identity. Follow least-privilege access principles and apply minimal permissions regarding who can access sensitive data and what they can do with it.

Monitor and act

Continuously monitor sensitive data to detect and control unauthorized data usage and movement, policy violations, and risky user behavior. Take appropriate action based on policy violations, such as revoking access, blocking users, creating alerts, encrypting data, or refining your protection policies.

When sensitive data is recognized, labeled, and classified, you can enforce policies to block or remove data from being shared and encrypt it with sensitivity labels on device endpoints. You can also auto-classify content with sensitivity labels through security solution policy and machine learning. Your security and governance teams can track and monitor sensitive data using corporate policies as the data moves inside and outside your organization.

Benefits of enabling work from anywhere with a Zero Trust approach

The Zero Trust approach for data protection and governance can maximize the business value of your data while helping you minimize the security and compliance risk of that data.

Boundaryless collaboration

Share data and information safely with partners, vendors, and customers. Help eliminate external collaboration barriers for employees, who can seamlessly coauthor and collaborate on sensitive data with partners outside the organization. Ensure that only authenticated and authorized individuals and devices have access to sensitive data. Provide greater control and help mitigate data breaches through network segmentation.

Identify exposure and risks to sensitive data and guide policy configuration

Understand the volume, location, and inventory of sensitive data and associated risks. Discover risk vectors and rank their severity to manage sensitive data's risk effectively. Give your security team greater control of sensitive data by monitoring which users interact with content and how they do so. Plus, allow your security team to apply real-time policies based on the context to protect sensitive data, such as encryption or limiting access, restricting third-party apps and services, and more.

Enforcing strong governance

Validate business claims, assess security posture, and understand the impact of your security culture on sensitive corporate data. Ensure the integrity of your sensitive data, driving continuous assessment and improvement for more robust data governance.

Data classification and security

Classify, inventory, and label sensitive data, automatically ensuring that sensitive information is protected and secured in a structured, predictable manner. Overcome the impact of human error on security measures by automating the data classification and labeling processes needed to achieve compliance.

Access and identity control

With data encryption and access management, gain additional protections by limiting which data can be accessed and the required actions taken with the sensitive data even if access was allowed. Create micro-segmentation around data, limiting cyberattackers' ability to access sensitive data or otherwise spread it.

Start your journey with Zero Trust security

With a Zero Trust strategy, you can deliver on improved and modernized security while driving tangible business results.

To learn more, visit aka.ms/zerotrust