A crash course in security management: learning the keys to a better security posture

An evolving cyberthreat landscape combined with shifting security challenges can have a real impact on your business.

It's important to have intelligent management of your security solutions for better visibility into your security, control over your policies, and guidance on hardening your security posture.

Introduction

How can companies protect a growing number of attack surfaces from increasing—and increasingly sophisticated—threats? As organizations find themselves managing resources that are distributed across multiple environments, they're facing many security challenges, including increased complexity, lack of visibility, and ineffective response.

In an effort to keep up, many organizations deploy more solutions, often ending up with multiple point solutions addressing specific security concerns, within a single workload. This leads to the loss of full visibility into the end-to-end security state—and that can have an impact on the overall security of the organization.

The management of so many individual controls, point solutions, and vendors for security—coupled with the increasing "noise" caused by their diverse and usually siloed data sets—can become a burden and a security vulnerability. In addition, disparate point solutions are often difficult to integrate with each other, making it harder to gain visibility and insight into your security posture, let alone respond effectively to threats.

In this eBook, we'll show you how to achieve intelligent security management using the following three key principles:

Full **visibility** that helps you understand the security state and risks across resources

Built-in security **controls** to help you define consistent security policies

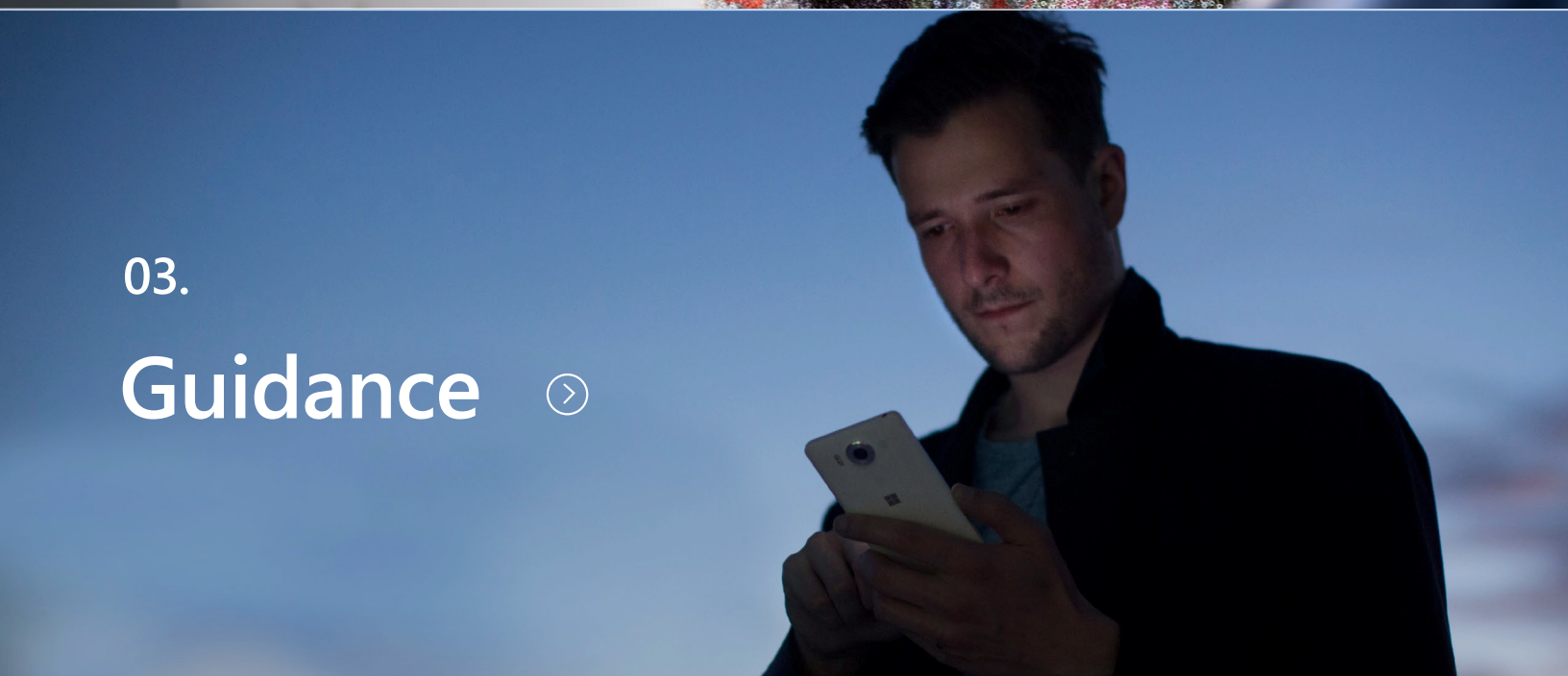
Effective **guidance** to help elevate your security through actionable intelligence and recommendations

01.

Visibility

02.

Control



03.

Guidance

01.
Visibility

Understand your security state

Menu
For users
For devices
For apps and data

Visibility is the first step in achieving intelligent security management. You need insight into your security state to identify risks across resources in your organization, so you can effectively detect and respond to threats.

Here's how Microsoft 365 security management solutions help you understand the security state of your users, devices, apps, and data:

Menu
For users
For devices
For apps and data

With users now connecting and demanding access anytime, anywhere, on any device, identity has become the new security perimeter. This makes securing user identities—without negatively impacting the user experience—one of the most important aspects of modern cybersecurity.

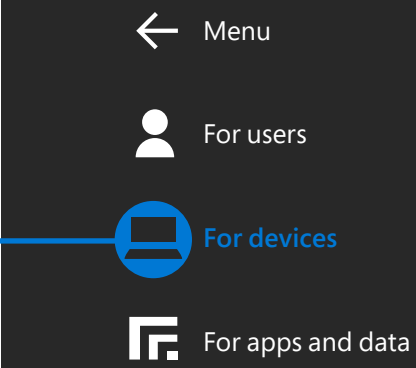
Microsoft's Identity and Access Management service, Azure Active Directory (Azure AD), provides access, usage, and security reports to gain visibility into the integrity and security of your organization's directory. With this information, a directory administrator can better identify and mitigate possible security risks.

With Azure AD, you can review and analyze:

- User-specific reports that display device and sign-in activity data for a specific user
- Activity logs that contain a record of all audited events within the last 24 hours, 7 days, or 30 days, as well as group activity changes and password reset and registration activity

---

In addition, Azure AD provides deep visibility into privileged identities to help you manage privileged accounts and monitor their activities, because of the risk associated with their misuse. Azure AD Privileged Identity Management can help you identify any administrator roles that are being misused, giving you the ability to discover, restrict, and monitor administrators and their access to resources. Users who need administrative access can get it for a preconfigured limited time (with just-in-time access) after they have proven their identity with multifactor authentication.



With always-connected users, device security becomes paramount. Therefore, security teams also need a solution that gives them visibility into their endpoint security, the ability to quickly assess the scope and root causes of incidents, and a rich toolset for investigation and remediation.

Windows Defender Advanced Threat Protection (ATP) includes Windows Secure Score. For both security management and security operations teams, Windows Secure Score provides real-time visibility into the security state of their endpoints and how well they are protected against the latest threats, while enabling them to address configuration issues proactively to reduce their organization's attack surface. It recommends steps to improve the overall security posture without the need to manually gather different reports from IT teams.

The Windows Secure Score dashboard provides a detailed view of security control configuration, as well as:

- Your current Microsoft Secure Score
- Your Windows Secure Score over time
- Windows Defender security controls
- Improvement opportunities, including recommended actions for each security control

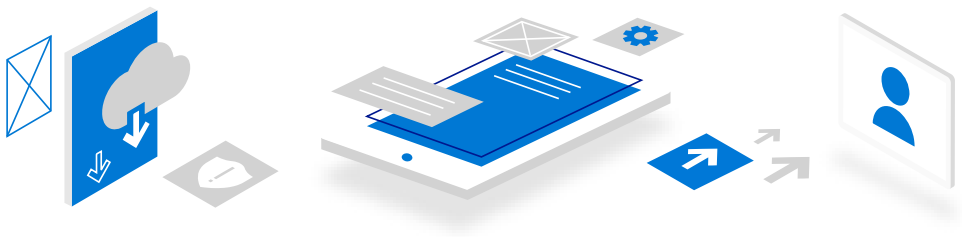
Menu
For users
For devices
For apps and data

Because of the sophistication and breadth of the cyberthreats that modern enterprises now face, they need to secure their apps and data at all times: at rest, in transit, and during processing. And with the introduction of regulations such as the GDPR, data security and usage transparency are now more important than ever.

One of the primary ways Microsoft 365 gives you visibility into your apps and data is through audit logs and reports to help you understand what users are doing. Logs can be easily accessed and searched via the Office 365 security and compliance center. Built-in reports help you visualize the log data. For example, they can show you how many people are violating data loss prevention (DLP) policies across SharePoint Online, One Drive for Business, and Exchange Online, or how many malicious attachments are being stopped by Office 365 Advanced Threat Protection.

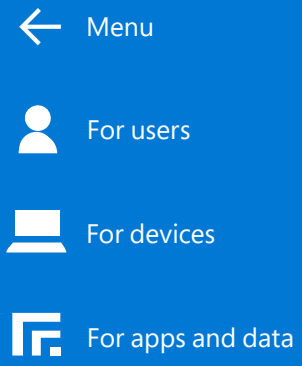
Microsoft Cloud App Security helps you gain additional visibility into all cloud use in your organization, including Shadow IT reporting and control and risk assessment. In addition, it parses the data from the Office 365 Management Activity API to create alerts on anomalous activity—such as someone logging in from a new location, logging in at unusual intervals, or using an ISP that they normally don't use.

These alerts can also be on specific activities, such as uploading or syncing files to OneDrive with known ransomware extensions or downloading a large amount of content from a SharePoint site that has sensitive HR data.



02.
Control

Define the data protection you need



After you've gained visibility into your security state, ongoing control over your security posture is the next step. You need to create and customize consistent security policies and enable the controls that are crucial to intelligent security management.

Here's how Microsoft 365 security management solutions help you define policies and enable controls for users, devices, and apps and data:

Menu
For users
For devices
For apps and data

Microsoft 365 helps you defend your organization at the front door by using conditional access and by controlling and protecting privileged identities.

Azure AD is Microsoft's Identity and Access Management solution, and it's designed to help organizations manage user identities and associated access privileges. Azure AD can help you secure and restrict data access with capabilities such as conditional access, user and sign-in risk calculation, multifactor authentication, and privileged identity management.

Azure AD Conditional Access provides a powerful framework for regulating access in governance, risk, and compliance scenarios. Conditional access policies can be applied based on device state, application sensitivity, location, and user rules.

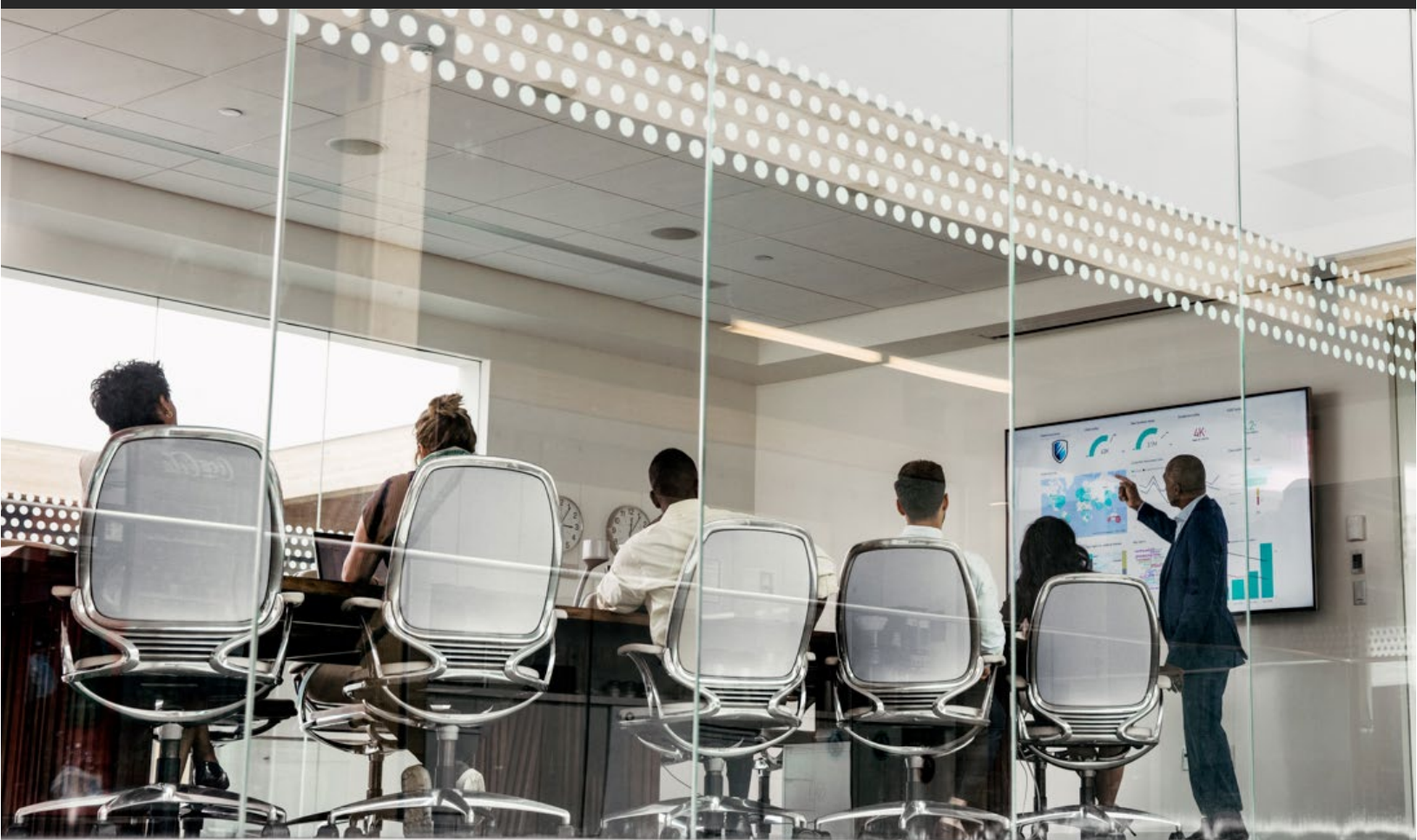
Additionally, Microsoft Enterprise Mobility + Security can protect your data in real time from the most advanced threats using identity protection capabilities that calculate the risk of every access request and user, then apply automated remediation actions as needed.

While any compromised account is bad, a compromised admin account is catastrophic. It's critical to minimize the probability and number of accounts with admin privileges. Azure AD Privileged Identity Management enables you to have the smallest possible number of admin-privileged users by helping you set policies to grant admin access only when needed, for only as long as needed, and only in compliance with your elevation policies.

Menu
For users
For devices
For apps and data

One of the most important security management practices is the ability to quickly enable the full Windows Security stack and configure it in a way that is compliant with your security policies. Microsoft provides a centralized tool for managing all Windows Defender ATP components.

Your security administrators can use System Center Configuration Manager or Microsoft Intune as their single, unified IT and security configuration tool, which they can use to enable and configure all Windows Security controls in one place. This is also very effective for organizations that use role-based security to limit access and control to the right people.

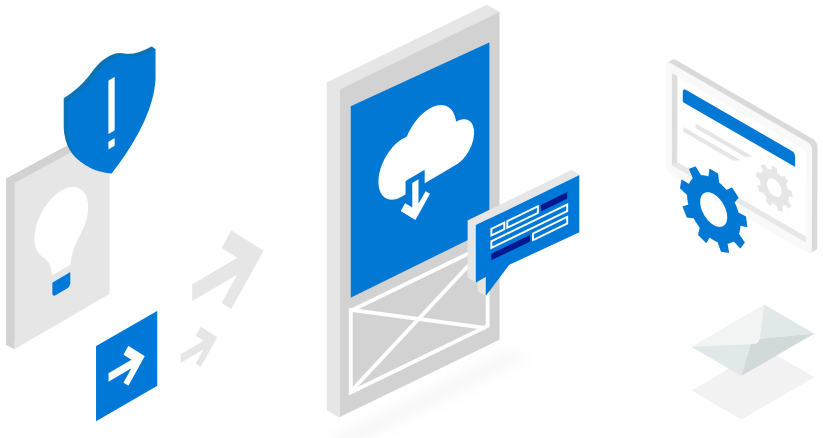


Menu
For users
For devices
For apps and data

You can better control the security of your apps and data through the Office 365 security and compliance center, a customizable, centralized portal for important security and compliance features. For example, you can easily set up DLP and data retention policies, configure how malware and spam are handled, and review threat intelligence data.

The security and compliance center also makes it easy to configure role-based security groups, giving people access to just the security and compliance features they need, versus global administration rights. This helps restrict access to administrative functions such as billing, assigning licenses, and creating new users.

Another important new security analytics tool is Microsoft Secure Score, which provides a single number to represent how your configurations compare to best security practices. Secure Score makes finding and enabling core security controls easier, including enabling multifactor authentication, auditing, and security features from the various Microsoft workloads. Secure Score also keeps historical data of what controls you've enabled, so you can track and share your progress and score with other members of your organization.



03.

Guidance

Keep current with security intelligence

Menu
For users
For devices
For apps and data

Once you have controls in place that define your optimal security policies, you need to follow up with ongoing intelligence and recommendations that will enable you to harden your security posture.

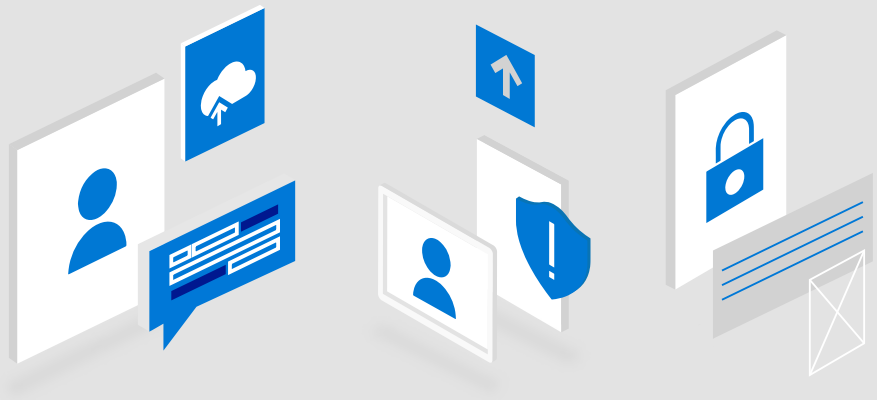
Here's how Microsoft 365 security management solutions deliver built-in intelligence and recommendations for users, devices, and apps and data:

Menu
For users
For devices
For apps and data

Azure AD provides the first line of defense with risk-based conditional access. With Azure AD, you get security reports in three broad categories:

- Cases where a login is anomalous and associated with some level of risk that the login is an attempt at unauthorized access
- Cases with significant indication that a user's credentials have been compromised, either because they are showing up frequently in risky logins or because they have been discovered in unauthorized hands
- Cases where your security posture could be improved, meaning there are vulnerabilities in your defenses that configuration changes can mitigate

Azure AD Identity Protection Security Reports provide you this information, either in the Azure AD Portal or programmatically, so you can integrate it into your SIEM or ticketing system.



Menu
For users
For devices
For apps and data

Windows Secure Score gives your security teams better insight into what security controls are available and which configurations can help you achieve a better security posture for your organization.

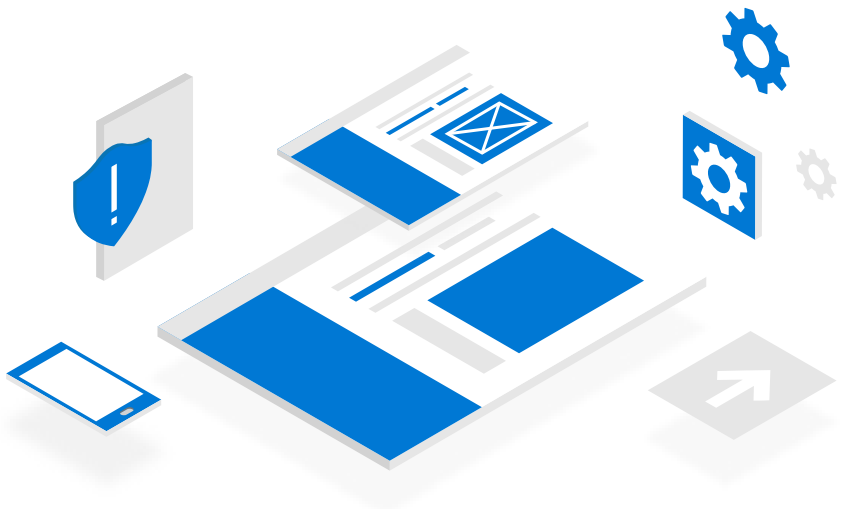
The Windows Secure Score dashboard recommends actions for each Windows Defender security control. It lists all available configuration options for each control and shows which ones are applied to which machines, and a number next to each configuration shows how much this additional configuration would contribute to your overall score. If a threat gets detected, the associated alert also comes with recommendations for containment and mitigation.

Menu
For users
For devices
For apps and data

Microsoft 365 provides recommendations to help you harden your security posture in two primary ways: through the Office 365 security and compliance center and through Microsoft Secure Score.

The security and compliance center shows you what recommendations the service has for your organization. Leveraging machine learning, Office 365 interprets signals from your usage to make recommendations on protecting data. For example, if you're not protecting tax documents, it might recommend that you create a data retention policy to hold that content for seven years. If you don't have a data loss prevention policy for personally identifiable information (PII), it can help you easily create one. The service can even leverage information specific to your industry for more customized recommendations.

Microsoft Secure Score helps you balance productivity and security. Based on our best practices and data from customer support, you receive recommendations on what security controls to enable to better protect against threats such as data exfiltration, account breaches, and elevation of privilege.



Powered by the Microsoft Intelligent Security Graph

Microsoft's security management solutions—including those referenced in this eBook—are powered by the **Microsoft Intelligent Security Graph**. The insights provided by the Intelligent Security Graph are generated from a massive amount of threat intelligence and security data from a range of Microsoft products and partners across devices and cloud services.

To defend against attacks that are fast and complex, the **Intelligent Security Graph** utilizes machine learning and artificial intelligence to detect and rapidly respond to threats. The system collects, correlates, and learns from the constant stream of data and updates continuously with the newest threat information. This anonymized data is coming from the hundreds of global cloud services we operate, and from the more than 1 billion PCs worldwide that we update every month. Human threat hunters, researchers, analysts, and engineers fine-tune models and add further insight and context. The data is also aggregated with external data points from extensive research, partnership with industry and law enforcement through our Digital Crimes Unit, and our Cyber Defense Operations Center.

Get started with intelligent security management

Microsoft 365 provides optimized security management for your organization's users, devices, and apps and data, while minimizing the need for multiple point security solutions and management consoles. Microsoft 365 security management solutions enable comprehensive visibility and control, and it provides you with built-in guidance and recommendations.

Here's how to get started:

1. Use Azure AD to secure identities in your environment.

2. Enable threat management for your devices through Windows Defender Security Center.

3. Manage and control apps and data for your SaaS apps with Office 365 security and compliance center, Microsoft Secure Score, and Microsoft Cloud App Security.

Ready to improve your organization's security posture?

Learn more about intelligent security management

Additional resources

Identity and Access Management

- Learn about Azure Active Directory

Security Management for Devices

- Learn about Windows Defender Security Center

Security Management for Apps & Data

- Learn about Office 365 security and compliance center
- Get an overview of Cloud App Security