Microsoft Identity-Driven Security

A holistic and innovative approach to mobility and security

Security landscape has changed

If you're like most companies today, then you've probably adopted some form of mobility and cloud services into your IT environment. Even if you haven't, chances are your employees have. In doing so, they've changed how they interact with their devices, apps, and your data. While they have become more productive, they've also created new security gaps for IT to handle. As the number of cyber-security attacks and data breaches increases worldwide, these issues only become more pronounced.

Introducing Microsoft Identity-Driven Security

Traditional security solutions used to be enough to protect your business. But that was before the attack landscape grew more sophisticated and the transition to mobility and the cloud made employees interactions with other users, devices, apps, and data more complex. To truly protect your business now, you need to take a more holistic and innovative approach to security, one that can protect, detect, and respond to threats of all kinds on-premises as well as in the cloud.

Microsoft Identity-Driven Security addresses the security challenges of today and tomorrow across users, devices, apps, data, and platforms. Each of your employees receive a single protected common identity for secure, risk-based conditional access to thousands of apps—on-premises and in the cloud. Innovative technologies safeguard your network at the front door. Deep visibility into apps, devices, and data activity uncovers suspicious activities, user mistakes, and potential threats before they become real ones. And with behavioral analytics, machine learning, and unique Microsoft security intelligence, you can secure your corporate files and data while freeing your employees to get their work done on the go.

Holistic. Innovative. Intelligent.

Protect at the front door

Safeguard your resources at the front door with innovative and advanced risk-based conditional accesses.

Protect your data against user mistakes

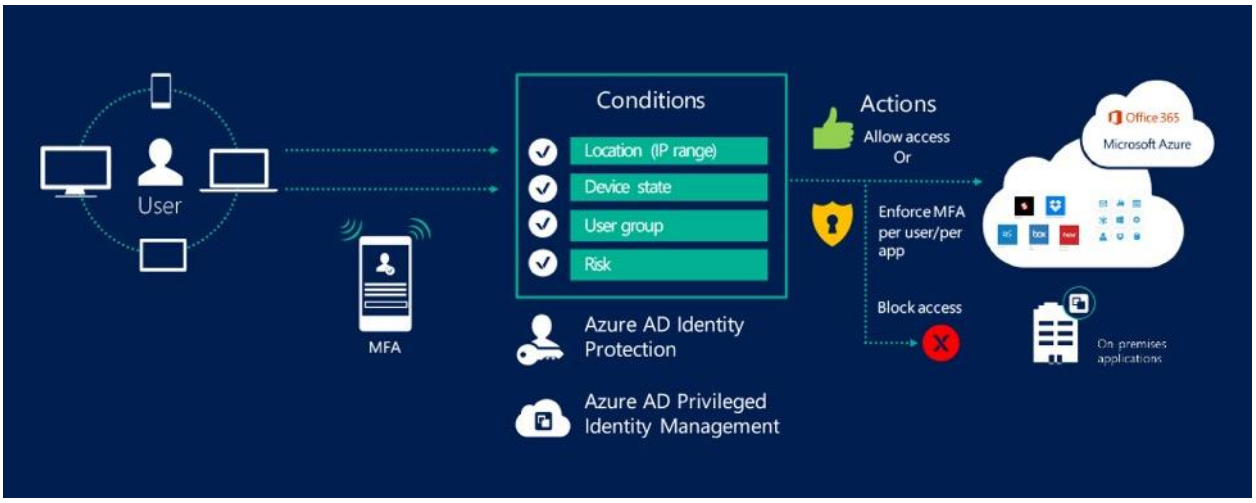
Gain deep visibility into user, device, and data activity on-premises and in the cloud.

Detect attacks before they cause damage

Uncover suspicious activity and pinpoint threats with deep visibility and ongoing behavioral analytics.

Protect at the front door

In more than 63 percent of data breaches, attackers gain corporate network access through weak, default, or stolen user credentials. Microsoft Identity-Driven Security focuses on user credentials, protecting your organization at the front door by managing and protecting your identities—including your privileged and non-privileged identities.

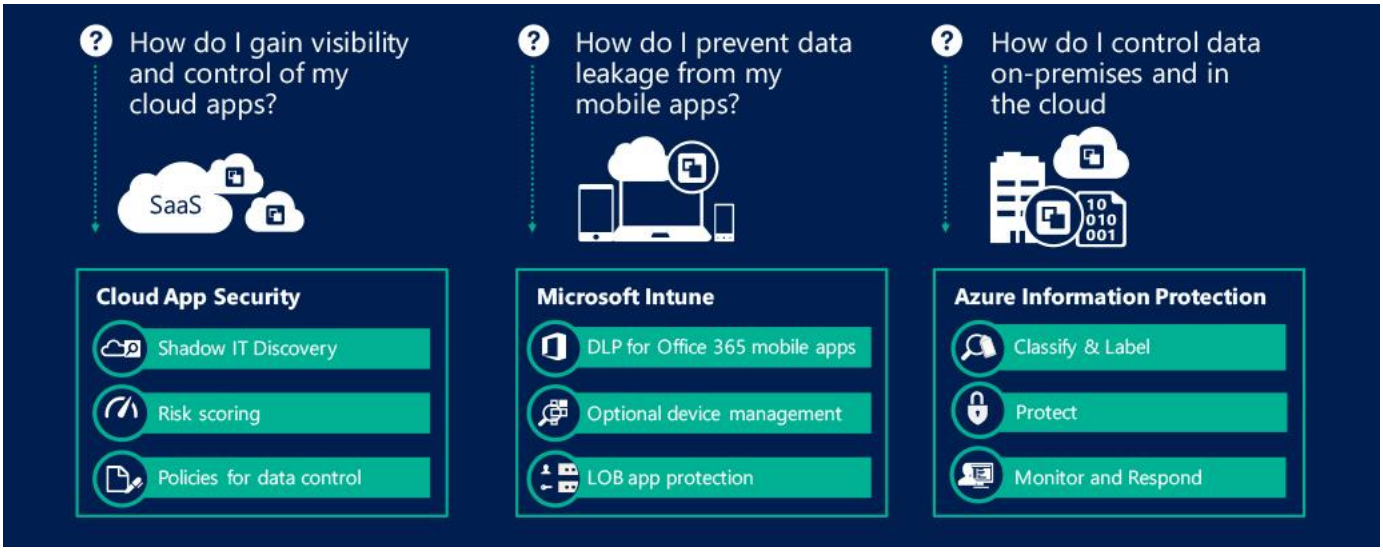


Azure Active Directory (AD) Premium

- **Secure single sign-on** and self-service identity management capabilities for 1000's of cloud and on-premises apps with a single identity managed and protected
- **Multi-Factor Authentication (MFA)** for user sign-ins and transactions to add an additional security layer
- Secure remote access for on-premises apps without using a virtual private network (VPN)
- Identity protection with machine learning-based threat detection and calculations of risk severity for every user and sign-in attempt
- **Risk-based conditional access** through an intelligent assessment of granting or blocking access and automatic protection from future threats
- **Discovery and restriction of privileged identities** and their access to resources (i.e. time limited "Just in Time" admin access) with Privileged Identity Management

Protect your data against user mistakes

The more visibility and control you have into your environment, the more you can keep it safely secured. Microsoft Identity-Driven Security offers deep visibility and strong data controls for the cloud apps your employees use, giving you complete context and granular-level policies. You gain the ability to classify and label files at creation, track their usage, and change permissions when necessary. And we help you prevent data loss on iOS and Android devices with an unparalleled ability to manage Office mobile apps.



Cloud App Security

- **Complete visibility** into employee cloud app usage and Shadow IT
- **Ongoing risk detection**, powerful reporting, and analytics on users, upload/download traffic, usage patterns, and transactions for discovered apps
- **Granular-level control** and data policies for on-going data protection in cloud apps

Microsoft Intune

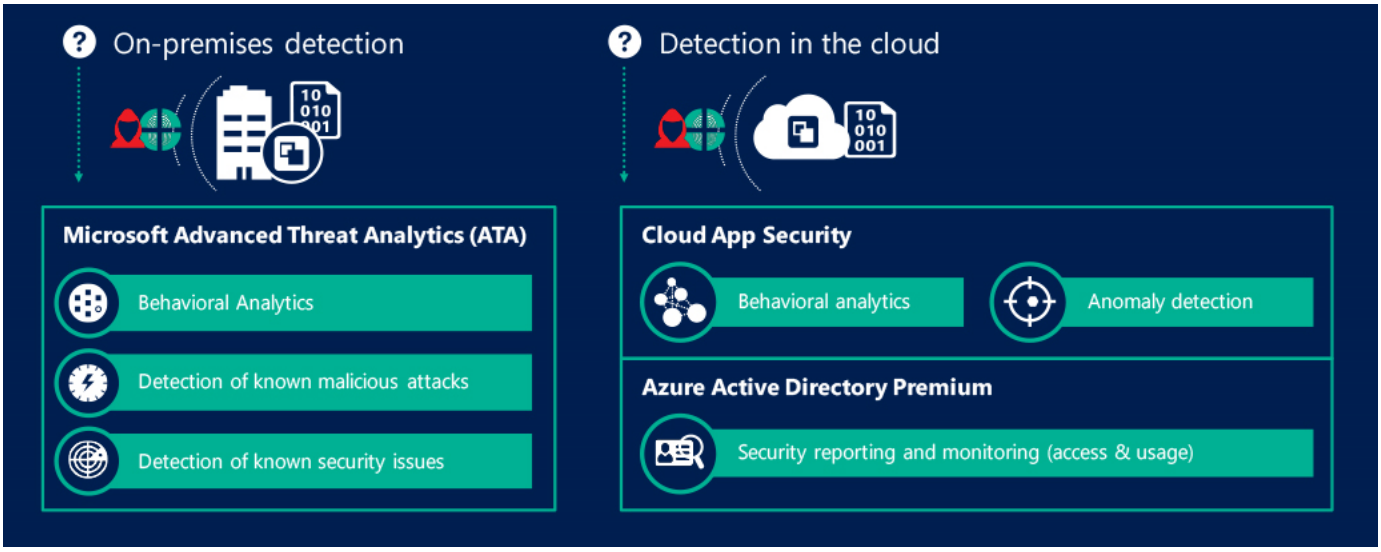
- **Unparalleled management of Office mobile apps** with or without device enrollment into MDM
- **Selective wipe of corporate data** (apps, email, data, management policies, and networking profiles) from user devices while leaving personal data intact
- **Security policy enforcement** for mobile devices, apps, and PCs

Azure Information Protection

- **Persistent data classification and protection** that ensures data is protected at all times—regardless of where its stored or with whom its shared
- **Safe sharing** with people inside and outside of your organization
- **Simple, intuitive controls** for data classification and protection
- **Deep visibility and control** of shared data for users and IT

Detect attacks before they cause damage

Our comprehensive threat intelligence uses cutting-edge behavioral analytics and anomaly detection technologies to uncover suspicious activity and pinpoint threats—on-premises and in the cloud. That includes known malicious attacks (i.e. Pass the Hash, Pass the Ticket) and security vulnerabilities in your system.



Microsoft Advanced Threat Analytics (ATA)

- **Identification of advanced persistent threats (APTs)** on-premises by detecting suspicious user and entity behavior using machine learning and event logs
- **Detection of known malicious attacks** almost as instantly as they occur
- **A simple attack timeline** with clear and relevant attack information so you can quickly focus on what is important

Cloud App Security

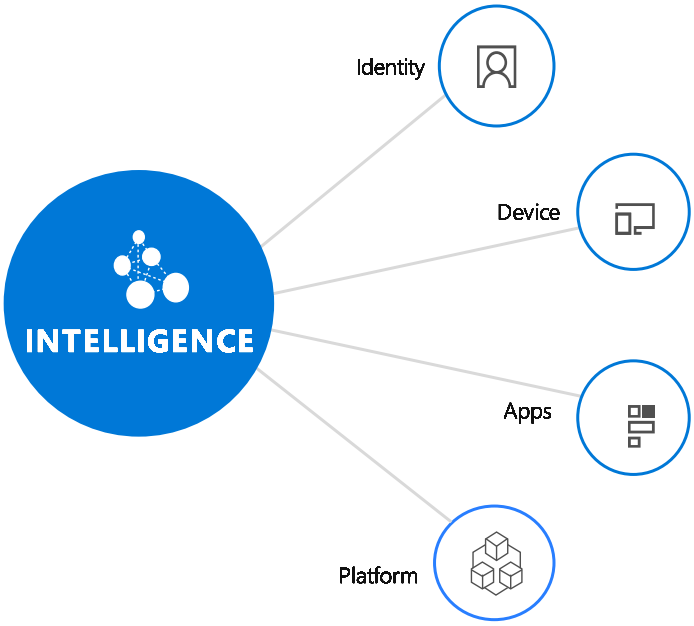
- **Behavioral analytics** that assess risk and identify attackers targeting your cloud apps
- **Identification of anomalies and policy violations** that may be indicative of a security breach

Azure Active Directory Premium

- **Identity protection** that provides a consolidated view of all the risky events and possible configuration vulnerabilities with notifications, analysis, and recommended remediation based on 10 TB of cloud data processed daily
- **Advanced security reporting** to protect against suspicious behaviors and advanced attacks
- **Access and usage reports** that give visibility into the integrity and security of your organization's directory with access and usage reports

Enhanced with the Microsoft Intelligent Security Graph

We continue to evolve our security intelligence with real-time insights and predictive intelligence—across our network—that help you stay a step ahead of threats. With our Intelligent Security Graph, formed by trillions of signals from billions of sources, you can better detect attacks, accelerate responses, and prevent modern day threats. The graph uses input we receive across our endpoints, consumer services, commercial services, and on-premises technologies. These and other enhancements help your IT staff enable rapid innovations while protecting corporate data and assets.



Microsoft

You can learn more about Microsoft Identity-Driven Security at www.microsoft.com/ems