

ENTERPRISE MOBILITY + SECURITY





KEEP YOUR EMPLOYEES PRODUCTIVE AND SECURE ON THEIR FAVORITE APPS AND DEVICES

Employees today are on the move, and they're using their mobile devices wherever they go. Whether in a conference room, in line for a cup of coffee, or using Wi-Fi on a flight, the modern employee wants full access to the apps and software that make them productive – from Office 365 or Salesforce, to custom applications running on Microsoft Azure or other cloud platforms. There are a couple of mega trends that have been changing the world of work as we know it. The place where people actually get their work done is no longer exclusively a traditional office or workplace, we are in an era where mobility really is the new normal.



So many different devices in our company (domain joined, non-domain joined, Servers, Smartphones, ...)



What is the best way to deploy Line Of Business Apps to different types of devices and platforms?



Increase of external Software as a Service („SaaS“) applications ... is there a Single Sign On solution?



Many different Credentials cause more forgotten passwords



We want to protect certain systems (SharePoint, Exchange, ...) with a multi-level method



Microsoft Enterprise Mobility + Security (EMS) provides an identity-driven security solution that offers a holistic approach to the security challenges in this mobile-first, cloud-first era. Not only help you protect organizations but also identify breaches before they cause damage.

Protect at the “front door”

EMS security approach starts with one protected common identity for secure access to all corporate resources on-premises and in the cloud with risk-based conditional access. Provides one protected common identity for accessing thousands of apps



Protect your data from user mistakes

EMS enables IT to gain deeper visibility into user, device, and data activity on-premises and in the cloud. With EMS, IT can protect corporate data from user mistakes with stronger controls and enforcement.



Detect attacks before they cause damage

EMS enables IT to identify attackers in your organization using innovative behavioral analytics and anomaly detection technologies, on-premises and in the cloud. It will assist IT to detect known malicious attacks and known security vulnerabilities in their systems.







BASIC PACKAGE

One user. One identity.
Everywhere

8 000,00 €



PROFESSIONAL PACKAGE

Hybrid Identity with advanced
protection

11 000,00 €



PREMIUM PACKAGE

Hybrid Identity with advanced
protection, Analytics and control

19 000,00 €



BASIC PACKAGE



- 3 week form completion
- Hybrid Identity Enablement
- Single Sign On to 2 SaaS Applications
- Device Management and 2 Application Management publishing
- Multi Factor Authentication on Cloud Identity

PROFESSIONAL PACKAGE



- 4 week form completion
- Privileged Identity Management
- Single Sign On to 2 On premises Applications to cloud identities
- Advance Security Reporting
- Document tracking and revocation
- All Features from Basic Package

PREMIUM PACKAGE



- 8 week form completion
- Microsoft Cloud App Security
- Microsoft Advanced Threat Protection
- All features from professional package



BASIC PACKAGE



- Azure AD Activation
- Simplified access management and security
- Multi-factor authentication
- Mobile Device and Application Management
- Azure Information Protection to cloud files

PROFESSIONAL PACKAGE



- Advanced protection for users and privileged Identities
- Advanced security reporting
- Intelligent Classification and Encryption for files inside and out of organization
- Embrace GDPR
- All features from Basic Package

PREMIUM PACKAGE



- Cloud App Security – Discover and secure cloud application
- Protection from advanced targeted attacks leveraging behavioral analytics
- All features from Professional Package



BASIC PACKAGE



- Self-service password hybrid model
- Multi-factor authentication
- Single sign-on for of SaaS apps
- Robust sync capabilities across cloud and on-premises directories
- Mobile device and application management across devices
- Information protection from the cloud or in a

PROFESSIONAL PACKAGE



- Self-service password data for greater security
- Multi-factor authentication • Information protection from the cloud or in a hybrid model with your existing on-premises infrastructure
- Conditional Access
- Group-based provisioning and single sign-on of SaaS apps
- Robust sync capabilities across cloud and on-premises directories
- Mobile device and application management across devices
- Advanced Reporting
- Broad device support for iOS, Android
- Selective wipe of apps and

PREMIUM PACKAGE



- Self-service password on-premises infrastructure
- Multi-factor authentication • Cloud App Discover
- Conditional Access • Secure Cloud Apps Organization
- Group-based provisioning and single sign-on of SaaS apps • Behavioural analytics for advanced threat detection
- Robust sync capabilities across cloud and on-premises directories • Detection for known malicious attacks and security issues
- Mobile application management across devices • Integration with your existing Security Information and Event Management (SIEM) systems
- Advanced Reporting
- Information protection from the cloud or in a hybrid model with your existing



ARMIS

[+351] 226 002 295

Rua do Freixo, n° 725-B,
4300-217 Porto

info@armisgroup.com