



Enterprise Mobility + Security

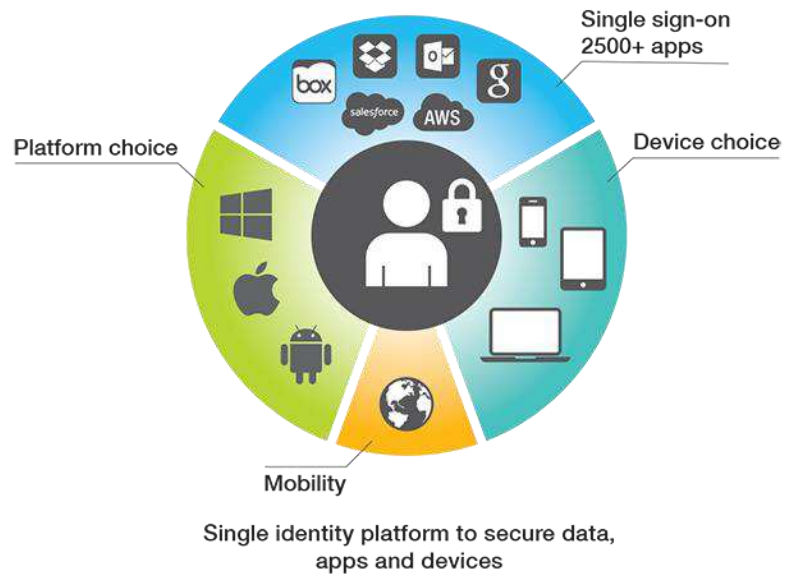
Simplify security, stay productive

Secured access to government data

The Pentagon reports **10 million cyber attacks daily**. The State of Utah averages **20 million a day**. Federal, state, or local government agencies need to safeguard information and maintain control when addressing internal mandates for cloud migration.

Microsoft Enterprise Mobility + Security (EMS) helps reduce security risk and enable workers to be more productive with features like:

- Identity and access management
- Information protection
- Device and application management
- Cyber intrusion detection



Government security needs

Provide all workers with simple, secure access to 2,500+ apps

Control access to confidential data

Lock down devices to make remote workers more efficient

Avoid legal or disciplinary actions for non-compliant data security

Prevent data theft

EMS can help...

Enable **single sign-on (SSO)** so workers only need one password or biometric/PIN combination to access all the applications they need.

Implement **multi-factor authentication (MFA)** to help prevent unauthorized access. **Secure information** across file servers, email, and collaboration platforms with **document tracking and encryption**.

Enforce security policies on government-owned or personal devices to help protect data even if devices are lost or stolen. Remote workers like road crews, health inspectors, and park rangers can access the information they need anywhere, anytime.

Centrally manage and secure devices, applications, and data to help comply with government regulations for information security. **Quickly provision and deprovision identities and access** for new, temporary, or exiting employees.

Identify cyber attacks before data is compromised **using behavior-based analytics** that leverage Machine Learning to inspect all network traffic.

“The Enterprise Mobility Suite provides the tools we need to configure, secure, and manage mobile devices as well as protect data. It’s absolutely key to achieving our mobility strategy.”

– Local Government Customer

Why EMS is right for government

EMS includes Azure Active Directory, Azure Rights Management, Microsoft Intune, and Advanced Threat Analytics to provide organizations with cost-effective, comprehensive security for users, devices, applications, and data.



Secured, flexible access to government resources

- Single sign-on to any application on your favorite device.
- Corporate policy enforcement for accessing resources from corporate or personal devices.
- Managed access to more than 2,500 pre-integrated SaaS applications, as well as your own custom cloud or on-premises hosted web applications.



Layered protection against data theft

- Data encryption that follows documents everywhere.
- Behavioral analytics to pinpoint cyber attacks before information can be compromised.
- Trusted multi-factor authentication engine that processes billions of requests every week.



Low licensing and implementation costs

- Comprehensive security coverage for nearly half the price of third-party solutions.
- Self-service password reset can reduce Help Desk calls by an average of 25%.
- Simple set-up, always up to date, and connects to your on-premises datacenter.

Act Now

- ✓ **Learn more about EMS in a Demo Session** – See all the tools and security tips applied in action. [Register Now](#)
- ✓ **Is your Data Secure?** – Let us help you Assess the Security of your Environment. [Engage Our Experts Now](#)
- ✓ **Get a Free Trial** – [Contact US](#)



For more information on EMS, visit www.communicationsquare.com/enterprise-mobility-security/