

Enterprise Mobility + Security
Simplify security,
stay productive

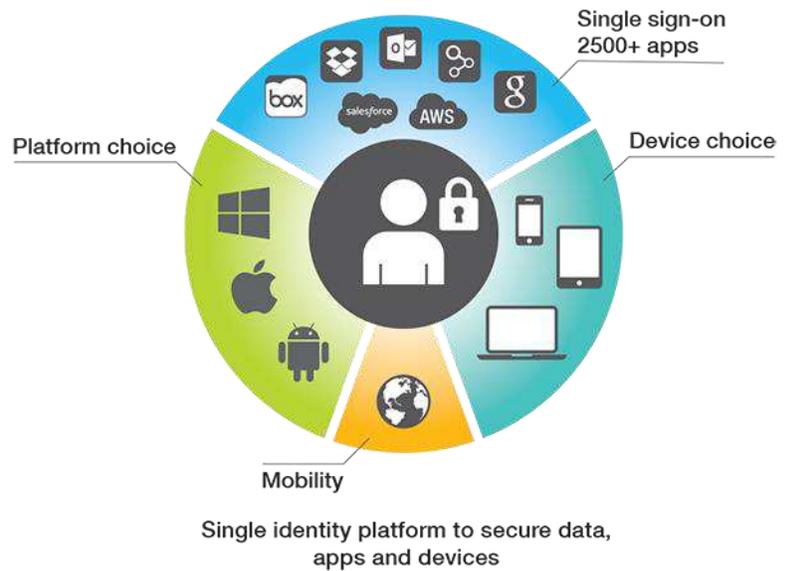


Better care through secure,
anywhere access

The average profit from a stolen medical record is \$20,000 – 10 times more than regular identity theft.* Security breaches cost healthcare organizations \$37 billion in 2015 – an average of \$398 per stolen record.**

Microsoft Enterprise Mobility + Security (EMS) helps secure patient health information (PHI) and allows workers to provide excellent care with features like:

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



Healthcare security needs

Control access to patient data

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

Expedite patient care with mobile devices

Prevent negative brand exposure and litigation costs

Avoid HIPAA fines

EMS can help...

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

Enable single sign-on (SSO) so workers only need one password to access all their applications. Use **mobile device management and cloud-based identity** to quickly provision and deprovision new, temporary, or exiting workers.

Provide secure access to patient data on corporate-owned or personal devices to provide faster, more comprehensive care.

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

Enforce security policies to keep workers from inappropriately downloading PHI to unsecured personal devices via DropBox or email.

*World Privacy Forum

**Poneman Institute, *Fifth Annual Benchmark Study on Privacy and Security of Healthcare Data, May 2015*

“With Microsoft EMS, we can be sure who is accessing and sharing content, such as medical lab protocols or procedural documents, and enable our clinicians and support staff to make better decisions.”

– Brett Taylor, Information Technology Director, St. Luke's Health System

Why EMS is right for healthcare

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 company 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 PHI 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/