UniCredit Țiriac Bank

Enterprise Mobility Management for Financial Sector

Conferința Ziarul Financiar:

Scurgeri de informații, furt de date confidențiale, hackeri. Pot fi o realitate?
Principalele riscuri de securitate și strategii de gestionare a lor.

Bogdan-Mihai Zamfir, CISM, C|CISO, COBIT-F,
Head of ICT Security & Compliance, UniCredit Tiriac Bank
bogdan.zamfir@unicredit.ro

Bucharest, 18 September 2014

ABOUT UNICREDIT TIRIAC BANK

- UniCredit Tiriac Bank is part of UniCredit, leading European financial group with the largest CEE presence.
- In Romania, UniCredit Tiriac Bank is one of the main financial institutions, offering high quality services and products for 580.000 clients.
- The bank strives to have a client centric policy, to be an easy to deal with partner and also an active part of the communities in which it operates.
- UniCredit Group is also present in Romania through UniCredit Consumer Financing (UCFIN), UniCredit Leasing Corporation (UCLC), UniCredit Insurance Broker, UniCredit Leasing Fleet Management, UniCredit Leasing Romania, Allib ROM, Debo Leasing, UCTAM, Pioneer Asset Management and UniCredit Business Integrated Solutions (UBIS).
- UniCredit Tiriac Bank is a pioneer in implementing latest security technologies, a leader on the local market from this perspective.

AGENDA

- Introduction
- Cybercrime in the mobile world
- From MDM to EMM
- Getting the Enterprise Mobile: the Executive Checklist
- Common RFP model
- Core features of an EMM
- Particularities for the Financial Sector
- Final points to check
- Conclusion

UniCredit Țiriac Bank

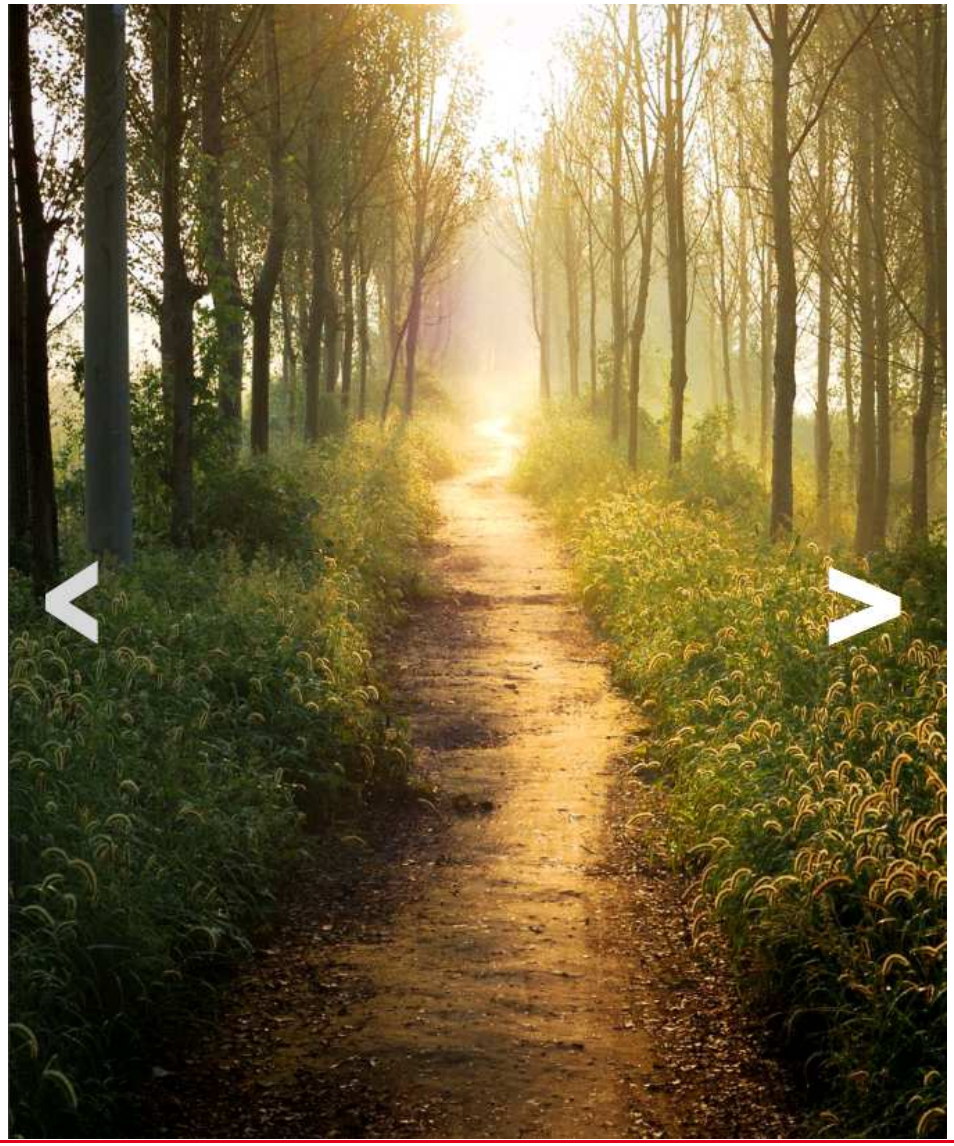
INTRODUCTION

CYBERCRIME IN MOBILE WORLD

- Crimes that can use either computers or mobile devices to advance other ends include:
  - Malware (ex.: addware, spyware, ransomware etc.)
  - Cyberstalking (espionage)
  - Fraud and identity theft
  - Information leakage
  - Phishing (smishing, vishing)
  - Spam
  - Device theft

THE JOURNEY

MDM



EMM

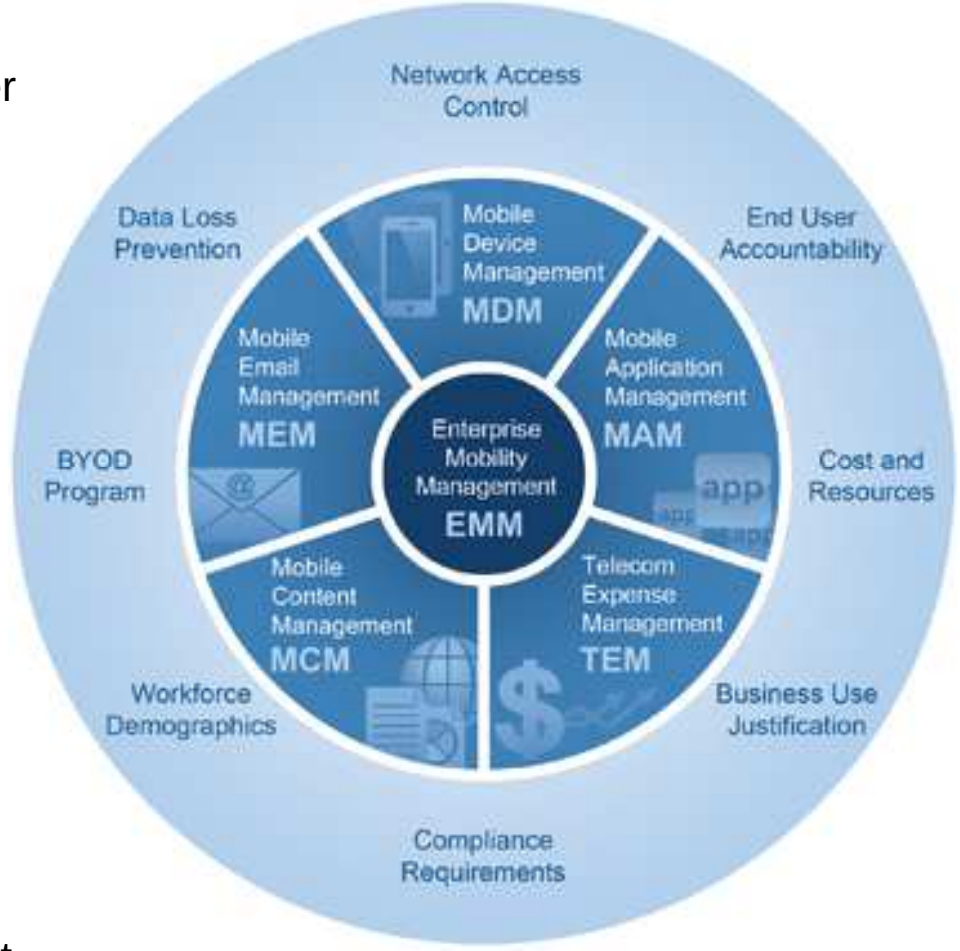
GARTNER PUTS FOCUS ON EMM

New 2014 “Magic Quadrant for Enterprise Mobility Management Suites” defines that EMM are expected to include the following functions:

- Hardware and application inventory
- OS configurations management
- Mobile app deployment, updating and removal
- Mobile app configuration and policy management
- Remote view and control for troubleshooting
- Execute remote actions such as remote wipe
- Mobile content management: secure container, content push and content access

EMM IS MORE THAN MDM

- Consolidation and governance of all mobility initiatives under IT management
- Enforcement of mobile device policy and user access configuration and compliance
- Streamlining new user enrollment, software updates, Help Desk troubleshooting, and device decommissioning for lower support costs per user
- Automated alerting and controls, preventing excessive charges through real-time cost management
- **Secure containerization** for email, calendar and attachments
- **Secure access** to intranet sites, line-of-business applications, internally published mobile apps, and internal document management systems
- **Protection of critical business data**, user authentication, and encryption for data at rest and data in motion.



Source: NotifyCorp

UniCredit Țiriac Bank

GETTING THE ENTERPRISE MOBILE: THE EXECUTIVE CHECKLIST

Consider:

- Device (freedom vs. consistency for type, company goals)
- User (enablement/eligibility, BYOD, no of. devices per user)
- App (allowed apps, securing apps, business opportunities)
- Data (prevent data leakage, facilitate collaboration, classification)
- Policy (minimum reqs., privacy considerations, stds. compliance)
- Security (data protection, device/user/app compliance, threat monitoring, decommissioning, SIEM integration)
- HA (uptime, scalability, redundancy and fault tolerance)
- Service (QoS, telecom expenses, remote support, self-service)

COMMON RFP MODEL

Things to check:

- Vendor/company background
- Local resellers and vendor support (SLA)
- Customer base, references, case studies
- Deployment time-frame
- Product network architecture and fit in your environment
- On premise or in cloud solution and data traffic routing
- Platform support (iOS, Android, Windows, BlackBerry)
- Core features

UniCredit Tiriac Bank

CORE FEATURES (I)

- Platform/device management (inventory, location, diagnostics etc.)
- Applications management (enterprise apps store, updates, white /blacklisting, web filtering etc.)
- Anti-malware, firewall, secure configuration profiles
- Wireless (WPA2) centrally manageable
- Control use of device if SIM is removed or disabled
- Media encryption
- User and device authentication, identity management
- Access restrictions/NAC support
- Enterprise VPN support

UniCredit Tiriac Bank

CORE FEATURES (II)

- Manage personal and corporate data separately
- Enforced complex passwords, inactivity timeout, audit trail
- Encryption, secure lock, selective wipe, jailbreak detection etc.
- Hardening for backup, user credentials, keys, policies
- Remote provisioning (centralized management) including account instantiation and personal certificates, remote update, unlock etc.
- Active Directory integration
- User self-service administration (device lock, location support etc.)
- Low battery consumption of the resident mobile agent
- Multiple users support (for apps or virtual machine, dual boot etc.)

PARTICULARITIES FOR THE FINANCIAL SECTOR

EMM financial applications:

- Mobile Banking app
- Mobile token (ex. RSA authentication)
- Other payment solutions (SMS Banking, NFC)
- Internal financial applications (BI, CRM, DWH etc.) – access and availability

Compliance:

- Customer data protection

Other:

- Complex environment
- Voice encryption

UniCredit Țiriac Bank

FINAL POINTS TO CHECK:

The EMM features that need to be closely checked:

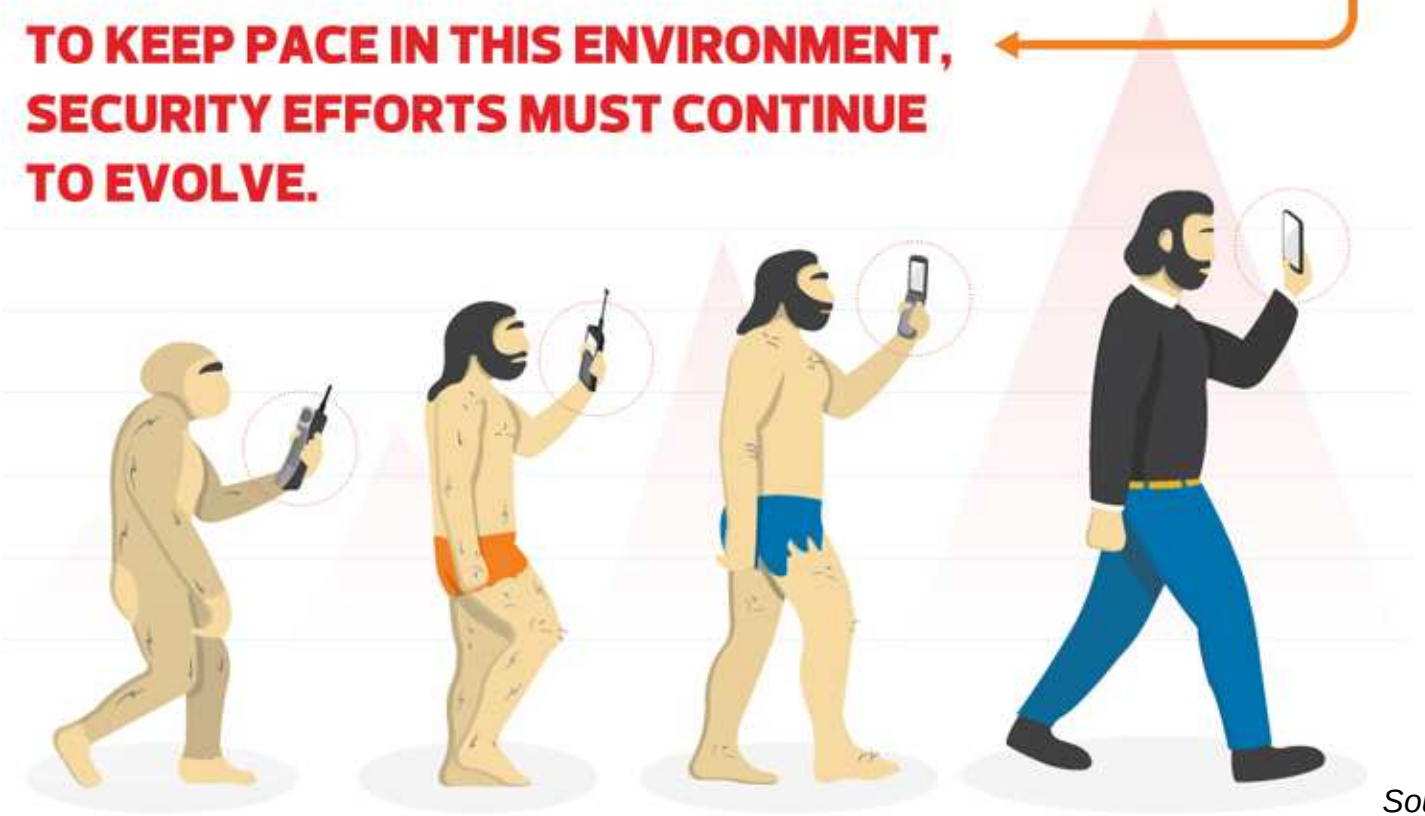
- Integration across apps, if needed apps are available on all devices
- Data/information classification support for containerized email and office suite, DLP integration
- Easy customization to different business needs
- Secure access, eSSO
- Swiftly access to Intranet portals (with NTLM/Kerberos integration)
- Automatic, self packaging for secured (container) apps + internal
- Architecture mapping on a multiple tier network design
- Productivity, efficiency and easy administration of the solution

CONCLUSIONS

Mobile technology is a critical tool for successful organizations, but the risks it faces are growing rapidly. Threats from mobile malware, hackers and other vectors are increasing in number and sophistication.

A recent survey found that IT security decision-makers consider mobile devices, such as smartphones and tablets, to be IT security's weakest link.

TO KEEP PACE IN THIS ENVIRONMENT, SECURITY EFFORTS MUST CONTINUE TO EVOLVE.



Source: cdw.com

UniCredit Țiriac Bank

Enterprise Mobility Management for Financial Sector

Conferința Ziarul Financiar:

Scurgeri de informații, furt de date confidențiale, hackeri. Pot fi o realitate?
Principalele riscuri de securitate și strategii de gestionare a lor.

Bogdan-Mihai Zamfir, CISM, C|CISO, COBIT-F,
Head of ICT Security & Compliance, UniCredit Tiriac Bank
bogdan.zamfir@unicredit.ro

Bucharest, 18 September 2014