Enterprise Mobility Management
Managed Mobility Solutions from AT&T

EMM & Collaboration Practice
AT&T Distribution & Channel Marketing

© 2016 AT&T Intellectual Property. All rights reserved. AT&T, Globe logo, Mobilizing Your World and DIRECTV are registered trademarks and service marks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks are the property of their respective owners.
Three of the top five strategic priorities for CIOs in 2015 are security related, according to the WSJ CIO Forum.¹

- Make security everyone’s business.
- Cyber risk = organization risk
- Anticipate a “cyber 9/11” event.
- Have a organization-centric vision.
- Be the change agent.
These priorities are being driven by technology trends. New endpoints, cloud computing, and advanced attacks are increasing the threat landscape.
As a result of these technology trends, the threat landscape is growing. Security breaches are becoming more and more common among large enterprises.

10x Increase in DDoS Attacks Since 2013
- Frequency has increased from 14 per month to 150+ per month
- Peak attack size increased from 2 Gbps to 300 Gbps

Increasing Security Risks and Threats
- 3.5 Billion Accounts Exposed

9.3x Increase in Mobile Attacks
- 9.3x year over year increase in attacks on mobile devices
- 175K new mobile malware programs detected in 1H2014

1B Digital Records Stolen Last Year
- Average cost of $3.5M/event, $145/user

$445B
annual cost to the global economy

1B
3.5B
9x
10x

© 2016 AT&T Intellectual Property. All rights reserved. AT&T, Globe logo, Mobilizing Your World and DIRECTV are registered trademarks and service marks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks are the property of their respective owners.
AT&T security solutions help protect our customers’ threat points.

Security solutions exist to help prevent, detect, and respond to threats.

**Customer Assets**
- Public Web Sites
- Corporate Email
- Network Access
- Mobile Endpoints
- Cloud Applications
- All Assets

**Prevent**
- AT&T Cloud Web Security Service
- AT&T Secure Email Gateway
- AT&T VPN
- Enterprise Mobility Management
- AT&T NetBond

**Detect & Respond**
- Response Consulting
- AT&T DDoS Defense
- AT&T DDoS Defense with Kona Site Defender
- AT&T Security Event & Threat Analysis
- AT&T Threat Manager - Advanced Log Management

© 2016 AT&T Intellectual Property. All rights reserved. AT&T, Globe logo, Mobilizing Your World and DIRECTV are registered trademarks and service marks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks are the property of their respective owners.
Protect enterprise data with multi-layer endpoint strategy.
AT&T Key Differentiators - EMM Platform Strategies
Working up the ‘Stack Attack’ - Targeting key Mobility Benefit Areas

- Corporate Devices
- Personal Devices

- BYOD

- CRU Devices/Plans
- BYOD Voice/Data Plans

- Mobile Application Mgt

- Mobile Content Collaboration Mgt (MCCM), ie, Box

- Enterprise Mobility Mgt (Mobile Device Management, BYOD)

Economics
- Mobility as a Service
  By running your EMM platform and deploying your devices, AT&T can free up your IT teams from having time consuming EMM administration activities

- Bundling
  AT&T can provide discounting when combining our rate plans with our EMM or MCCM Licenses

Governance
- Mobility/Application ‘Steering’ Committee
  Security Governance
  Security/Regulation alignment for EMM policies

Productivity
- BYOD policies, ie, Stipends
  User Group x User Group Application Enablement
  Content Collaboration
  Content Security Management

© 2016 AT&T Intellectual Property. All rights reserved. AT&T, Globe logo, Mobilizing Your World and DIRECTV are registered trademarks and service marks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks are the property of their respective owners.
Security has its own ROI/Benefits but the other Benefit areas can provide further ROI to support Critical/Enhanced security investment.
Mobile Security – Why is it Necessary?

Advanced Mobility Solutions from AT&T

Enterprise Mobility Management Value

Trusted Advisor: Economics, Governance, and Productivity
Top concerns of IT in mobile environment

- **58%** Mobile malware
- **56%** Malicious Apps
- **70%** Insecure or loosely-secured privacy setting on legitimate mobile apps

Source: IDC Whitepaper Sponsored by AT&T "Building Mobile Security Implementation at All Levels of the Organization" Doc #248005
A recent survey conducted by Enterprise Mobility Exchange found that 82% of companies allow their employees access to enterprise applications and contents—devoid of Mobile Security controls.

“When you start the mobile security maturity discussion, you have to begin with the entry point—*the device.*”

--- Information Security Media Group ---
## Business Challenges

### Smartphone user behavior and expectations

<table>
<thead>
<tr>
<th>Percentage</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>89%</td>
<td>Business users accessing critical work data from their personal mobile device(^1)</td>
</tr>
<tr>
<td>41%</td>
<td>Business users using personal device for work without company permission/knowledge(^1)</td>
</tr>
<tr>
<td>30%</td>
<td>IT pros whose company has experienced security threat due to a personal mobile device(^1)</td>
</tr>
<tr>
<td>32%</td>
<td>IT Pros concerned personal mobile devices introducing malware(^1)</td>
</tr>
<tr>
<td>41%</td>
<td>IT pros concerned about security breaches due to lost or stolen mobile devices(^1)</td>
</tr>
<tr>
<td>614%</td>
<td>Mobile Malware increase from 2012 to 2013(^2)</td>
</tr>
</tbody>
</table>

**SOURCE:**

1. Juniper Networks’ Trusted Mobility Index
2. Juniper Networks’ 3rd Annual Mobile Threat Report

© 2016 AT&T Intellectual Property. All rights reserved. AT&T, Globe logo, Mobilizing Your World and DIRECTV are registered trademarks and service marks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks are the property of their respective owners.
Why consider mobile security?

The Risk

Personal mobile devices have simultaneously brought new productivity options to employees, new security policy decisions to employers, and put sensitive data, processes, and tools at risk.

Security Risks of an Unprotected Mobile Inventory

- Data Loss
- Mobile Threats
- Legal, Regulatory and Compliance Risks
Mobile Security Challenges

- **Malware**
  - Viruses, Worms, Trojans, Spyware

- **Loss and Theft**
  - Loss or inappropriate access of sensitive data

- **Data Communication Interception**
  - Sniffing data as it is transmitted and received

- **Exploitation and Misconduct**
  - Online predators, inappropriate sites and communications, data leakage

- **Direct Attacks**
  - Attacking device interfaces, Network DoS, Malicious SMS
Use Case: Managing Your Mobile Security
Advanced Protection Through Your Network

Customer Challenges

- **Sensitive Data** at risk of theft
- **Malware & Viruses** can attack any connected devices
- **Direct Attacks** through Denial of Service (DoS) and Malicious SMS can impact your business
- **Exploitation and Misconduct** can cause data leakage and access to inappropriate sites
- **Data Communication Intercept** by sniffing data and communicating it to those looking to exploit your business

Customer Focused Security Solutions

A mobile device app that includes network-based, carrier-grade protection even if you aren’t an AT&T wireless customer

- **Customized**
  - Designed with the customers’ security requirements in mind
  - Experts can partner with you to design the right approach
  - Will work in any mobile environment

- **Integrated**
  - Solution will integrate with your wireline and wireless network
  - Web-Based portal will allow you to manage your security policies from anywhere

- **Managed**
  - AT&T will manage infrastructure, licenses, patches & support
  - You focus on running your business while we focus on your security

Customer Benefits

- **Reduce Risk** of sensitive data getting out in the open
- **Prevent Threats** from multiple sources
- **Centralized Management** of wireline & wireless security policies and enforcement
- **Remote wipe** any device to prevent data theft or loss
- **Enables device management & control** from a remote location

"The steady double digit growth of threats to smartphones makes security awareness and action imperative. Recognizing the seriousness of these threats and the ubiquitous, business-critical nature of mobile applications used by enterprises today,“

— Ed Amoroso
AT&T Chief Security Officer

© 2016 AT&T Intellectual Property. All rights reserved. AT&T, Globe logo, Mobilizing Your World and DIRECTV are registered trademarks and service marks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks are the property of their respective owners.
Simplifies the complexity of mobility for customers

MDM
Mobile Device Management

MWM
Mobile Workspace Management (BYOD)

MCCM
Mobile Content Collaboration Management

MAM
Mobile Application Management
EMM Platform Strategies - Working the ‘Stack Attack’

**1- Bring ROI and Productivity beyond Security and Email to fully access value**

2 – BYOD transitions can be Secure, Productive and minimize Reimbursement headaches

3- Focus on ROI with ‘Wireline’ projects
Better secure & control your end-points thru Enterprise Mobility Management

Comprehensive Cross-Platform EMM
Gain better control over your increasingly mobile workforce

End-to-End Security
Protect enterprise data at key endpoints

Mobile Device Management (MDM)
Manage your device inventory regardless of size

Mobile App Management (MAM)
Distribute apps more securely across multiple platforms

Mobile Content Management (MCM)
Connect employees to resources virtually anytime, anywhere

Archiving and Auditing
Ensure sensitive data is handled with strict requirements

Deployment Flexibility
Multiple options including cloud, on-premise & hybrid

Scalable Architecture
Customizable EMM solutions based on your EMM needs
Fully mobilized endpoints, securely connected to your CSP’s

Performance
Low-latency, On-Net

Security
Avoids Internet/DDoS threats

Agility
API controlled

Elasticity
Dynamic capacity

Cost
Baseline commitment with overage charges

Functionality
e.g. the Box platform unchanged
Security has its own ROI/Benefits but the other Benefit areas can provide further ROI to support Critical/Enhanced security investment.
Enterprise Mobility Challenges
The rapid pace of change poses complex business challenges

How do I support mobile users across the globe, 24x7?

How can I control operational and labor investments related to mobility?

How do I manage changes to my organization’s Mobile Device Management environment?

How do I quickly gain the expertise and infrastructure needed to support and manage mobility?
Managed Mobility Services

Mobile Device
- Feature Phones, Smart Phones or Tablets
- Premium Device Deployment & Extended Warranty Service

Voice & Data Plan
- AT&T Mobile Select or your pre-negotiated rate plan

EMM Deployment and Support
- Mobile Device Selection & Configuration
- Stage, Kit, Provision & Ship at Scale
- Advanced Exchange & Extended Warranty
- Legacy Device Salvage & Recycle

Deployment - AMLS
- Configuration
- Training
- 24x7 Support
- Remote Admin Adv.

Tailored Support
- Mobile Device Selection & Configuration
- Stage, Kit, Provision & Ship at Scale
- Advanced Exchange & Extended Warranty
- Legacy Device Salvage & Recycle
Enterprise Managed Mobility Lifecycle

& Mobility Consulting

& Enterprise Mobility Management

& Mobile Deployment, Support Solutions
EMM Implementation Services
EMM Remote Administration
EMM Application Service Desk
Project Management
Gold Image Creation
Tier 1 Help Desk

& Advanced Mobile Lifecycle Services
Custom Configuration
ACAP Self Service Client Asset Portal
System Administration, Asset Tagging
Platform Consulting
EMM Support and Remote Administration

A full set of solutions that provide resources to help customers design, install, configure and run their EMM infrastructure

EMM Platform Technical Support
- Single Point of Contact to resolve service issues and support requests
- Addresses interoperability between multi-carrier mobile devices, network, platform, mobile applications and hosted infrastructure
- 9x5 business hours or 24x7 options

EMM Platform Remote Administration
- Full platform administration and release change management.
- Implements ongoing security policies and user group administration for platform as well as day to day MACD activities
- Consults on release feature enhancements

Service is designed in modular increments allowing customers to select the amount of support that best fits their needs
Save time, scale resources, and increase productivity by offloading the full scope of mobile device deployment and lifecycle support to AT&T’s world-class delivery team.

Nearly 1 Million Devices Deployed and Managed – meeting enterprises needs today.
# Mobile Security & Compliance – Becoming Mobile First

## Increasing device value-add in corporate environments

### What’s Required?
- **Employee Experience**
- **Productivity**
- **Applications**

### Separation of work and personal content & apps
- Privacy
- Access to Content anytime, anywhere from any device
- Access to Cloud Services
- Enterprise Procurement
- Ease of Access
- Shared Devices

---

© 2016 AT&T Intellectual Property. All rights reserved. AT&T, Globe logo, Mobilizing Your World and DIRECTV are registered trademarks and service marks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks are the property of their respective owners.
Survey for AT&T Education Executive Advisory Council

• Top 3 BYOD Concerns
  1. Data Security/Loss – 33%
  2. Access Security – 20%
  3. Device Management – 20%

• Other Concerns
  1. How can BYOD work without a solid VDI or virtual infrastructure behind it. Don’t currently have the resources to build and support our workforce.

• Top Applications/Types to Enable
  1. ERP
  2. Degree Audit
Faculty and staff are increasingly using their own devices for work related activities
IT leaders predict that in 2014 about 60% of faculty, staff and administrators will use their own device for work related purposes

Students grew up with technology and demand anytime, anywhere access
According to EDUCAUSE Center for Analysis and Research, the top student requests are “accessing course websites or syllabi” (66%) and “using course or learning management systems” (64%)

Mobile Device and OS proliferation is constraining campus resources
Administrators need a secure method to consolidate a variety of different mobile services. Device and operating system proliferation is driving high administrative, infrastructure and cost burdens

How has BYOD manifested in your institution?

Discussion Question

## Value of Advanced Mobility for Students

<table>
<thead>
<tr>
<th>User Story</th>
<th>Value of Advanced Mobility</th>
</tr>
</thead>
<tbody>
<tr>
<td>As a student I need access to course websites and syllabi – on the go</td>
<td>Access university websites and content on mobile devices through Advanced Mobility Secure Browsers</td>
</tr>
<tr>
<td>As a university student I want to be able us my mobile device but not my personal data allotment on school related applications</td>
<td>Send rich content to devices and provide faculty, staff and students data subsidies for school related activities</td>
</tr>
<tr>
<td>As a college student I want access to mobile applications both for fun and for school work without having to worry about personal privacy</td>
<td>Maintain personal privacy and ensure network security through personal and school profile segregation – all on one device</td>
</tr>
<tr>
<td>As a student I work with my classmates on group projects and need to communicate with my professors using email and other collaboration tools</td>
<td>Collaborate with other students and teachers using permitted mobile collaboration tools that allow you to easily create, edit and share</td>
</tr>
</tbody>
</table>
## Value of Advanced Mobility for Faculty and Staff

<table>
<thead>
<tr>
<th>User Story</th>
<th>Value of Advanced Mobility</th>
</tr>
</thead>
<tbody>
<tr>
<td>As a faculty member I use my personal device to distribute content and to</td>
<td>Email, call and distribute content to students on both personal and university owned</td>
</tr>
<tr>
<td>communicate with students by voice and email outside of office hours</td>
<td>devices in a secure and consistent manner</td>
</tr>
<tr>
<td>As a university professor I collaborate with grad/post-grad students and</td>
<td>Collaborate with trusted colleagues by leveraging applications that are secured through</td>
</tr>
<tr>
<td>my constituents on R&amp;D projects both on and off campus</td>
<td>app level VPN over secure or public Wi-Fi and cellular</td>
</tr>
<tr>
<td>As a mobile admissions officer I want access to university resources on</td>
<td>Use secured productivity and collaboration tools to manage a busy schedule, store and share</td>
</tr>
<tr>
<td>both my personal tablet as well as my university issued smartphone</td>
<td>prospective student information</td>
</tr>
<tr>
<td>As a university CIO I need to ensure the integrity of the school network</td>
<td>Provide highly secure access to university resources using Secure Browser, unique policy</td>
</tr>
<tr>
<td>while allowing use by a growing number of devices and applications</td>
<td>settings and app level VPN</td>
</tr>
</tbody>
</table>

© 2016 AT&T Intellectual Property. All rights reserved. AT&T, Globe logo, Mobilizing Your World and DIRECTV are registered trademarks and service marks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks are the property of their respective owners.
How does your organization distribute information?

Cloud or on-premise model?

Deliver apps or content?

Work or personal devices?

Domestic or international?
<table>
<thead>
<tr>
<th>Basic Sync &amp; Share</th>
<th>Features</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Features</td>
<td>Description</td>
</tr>
<tr>
<td>Basic Sync &amp; Share</td>
<td>Use Box for content storage and sharing, replacing a personal or corporate drive, accessible on any device</td>
<td></td>
</tr>
<tr>
<td>Mobile Productivity</td>
<td>Use Box to access corporate content from a mobile device</td>
<td></td>
</tr>
<tr>
<td>Team Collaboration &amp; Project Management</td>
<td>Use Box to store, share, and collaborate on documents and critical projects with team members</td>
<td></td>
</tr>
<tr>
<td>Cross-Department Collaboration</td>
<td>Use Box to store documents between different internal teams</td>
<td></td>
</tr>
<tr>
<td>External Collaboration</td>
<td>Use Box to store and manage the transfer of content with external parties</td>
<td></td>
</tr>
<tr>
<td>Process Management</td>
<td>Use the Box platform to build custom apps for business processes, integrate with existing business applications, or to sell as independent app</td>
<td></td>
</tr>
<tr>
<td>Platform</td>
<td>Use the Box platform to build custom apps for business processes, integrate with existing business applications, or to sell as independent app</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Description</th>
<th>Features</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Features</td>
<td>Description</td>
</tr>
<tr>
<td>Basic Sync &amp; Share</td>
<td>Use Box for content storage and sharing, replacing a personal or corporate drive, accessible on any device</td>
<td></td>
</tr>
<tr>
<td>Mobile Productivity</td>
<td>Use Box to access corporate content from a mobile device</td>
<td></td>
</tr>
<tr>
<td>Team Collaboration &amp; Project Management</td>
<td>Use Box to store, share, and collaborate on documents and critical projects with team members</td>
<td></td>
</tr>
<tr>
<td>Cross-Department Collaboration</td>
<td>Use Box to store documents between different internal teams</td>
<td></td>
</tr>
<tr>
<td>External Collaboration</td>
<td>Use Box to store and manage the transfer of content with external parties</td>
<td></td>
</tr>
<tr>
<td>Process Management</td>
<td>Use the Box platform to build custom apps for business processes, integrate with existing business applications, or to sell as independent app</td>
<td></td>
</tr>
<tr>
<td>Platform</td>
<td>Use the Box platform to build custom apps for business processes, integrate with existing business applications, or to sell as independent app</td>
<td></td>
</tr>
</tbody>
</table>
VMO (Value Management Office) Model Assumptions

- Staff – 250 users
- Field staff – 50 users, maintenance
- Students – 1000 users
- Faculty – 200 users