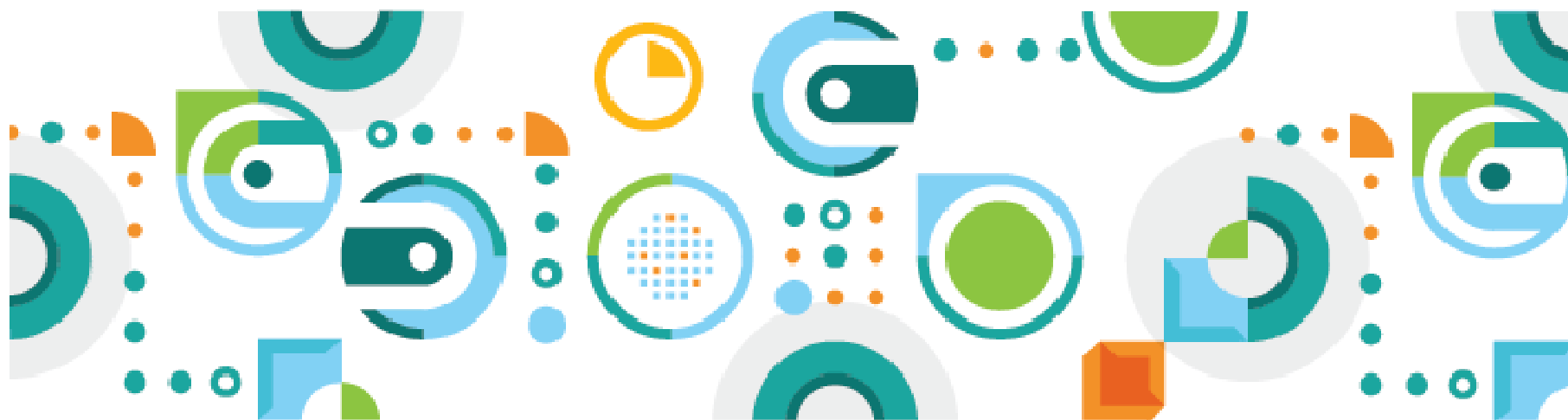


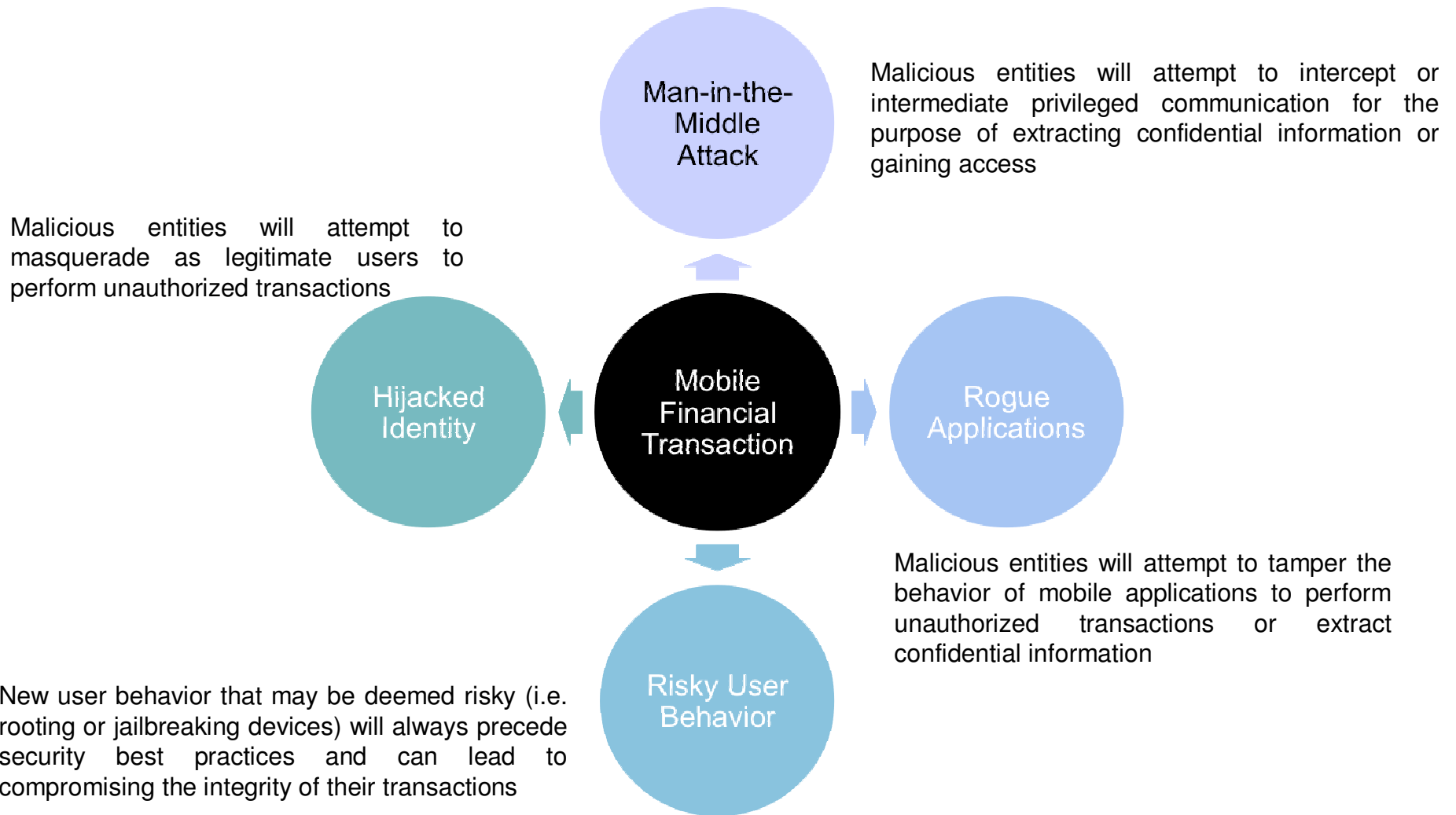
IBM Mobile Security: How We Secure The Mobile Enterprise

Giancarlo V. Marchesi
Manager, Security Worldwide A-Team (SWAT)



Mobile Security Challenges

Do You Have Visibility & Control Of The Mobile Devices & Transactions?



How Can We Achieve This?

Context Influences Risk

➤ The context of an interaction needs to be analyzed so appropriate security measures can be employed to counter plausible threats.

Interaction Interface is Critical

➤ Mobile apps are the primary interaction interface whose integrity needs to be safeguarded and validated.

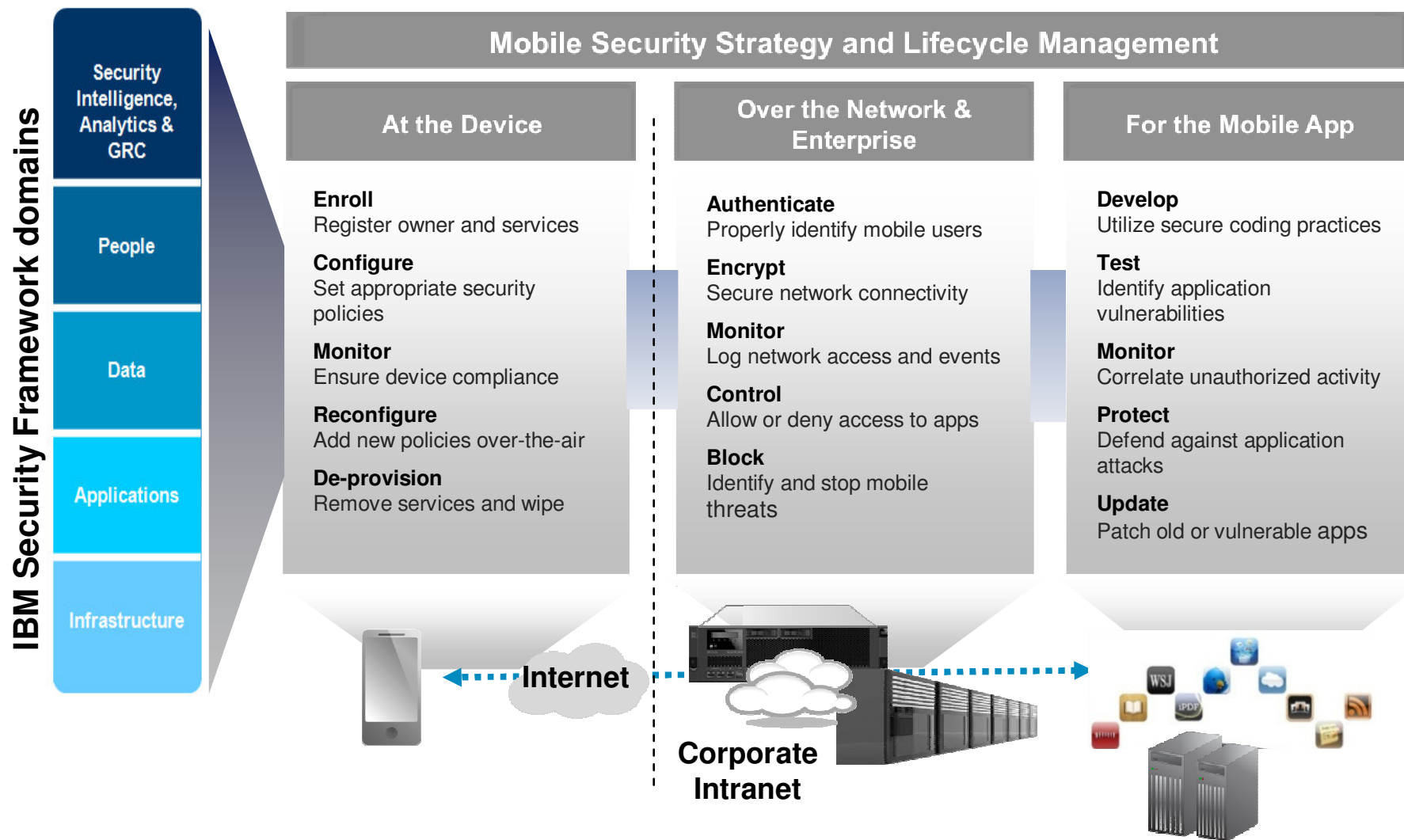
Vigilance is a Necessity

➤ Monitoring security events allows the ability to assess the completeness of the security posture as well as detect intentional and unintentional actions that may compromise it.

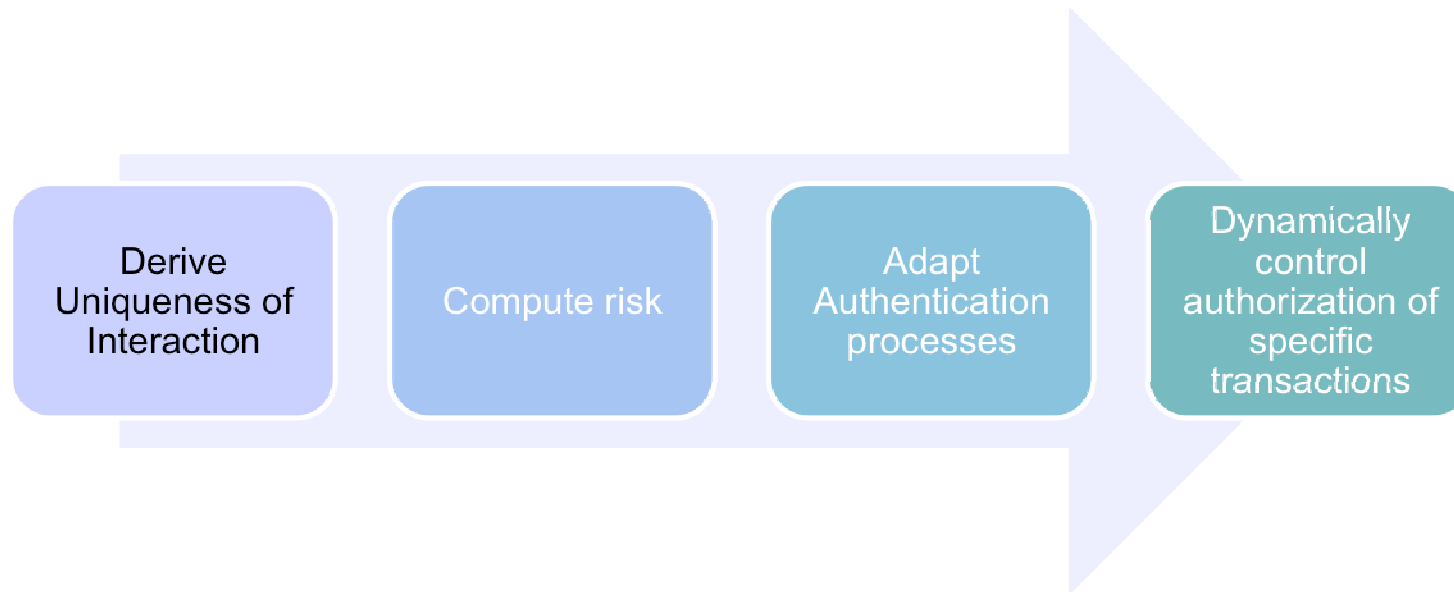
Oversee Devices in an Enterprise Context

➤ For certain segments of employees or business partners having visibility and control over the device will mitigate risk exposure.

IBM Mobile Security



Context Influences Risk

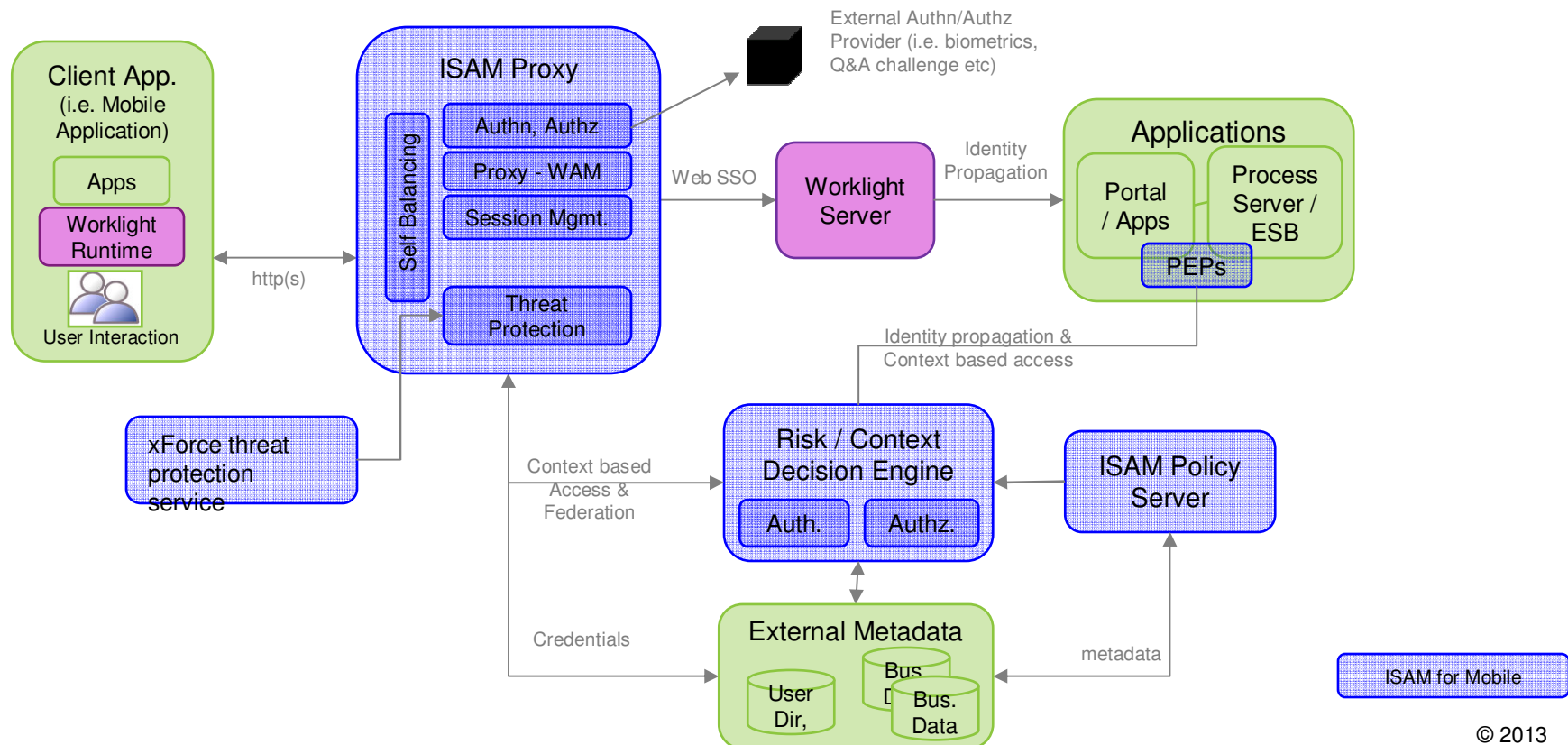


- Mobile affords many attributes that pertain to the user's context allowing for unique identification of a specific interaction (i.e. location, network, time, device properties etc)
- Risk of the unique interaction can be computed based on established policies
- The risk score can be utilized to select the authentication processes best suited for that interaction
- The risk score can also be employed to control authorization for specific transactions during that interaction and deliver education to the user on security best practices in context

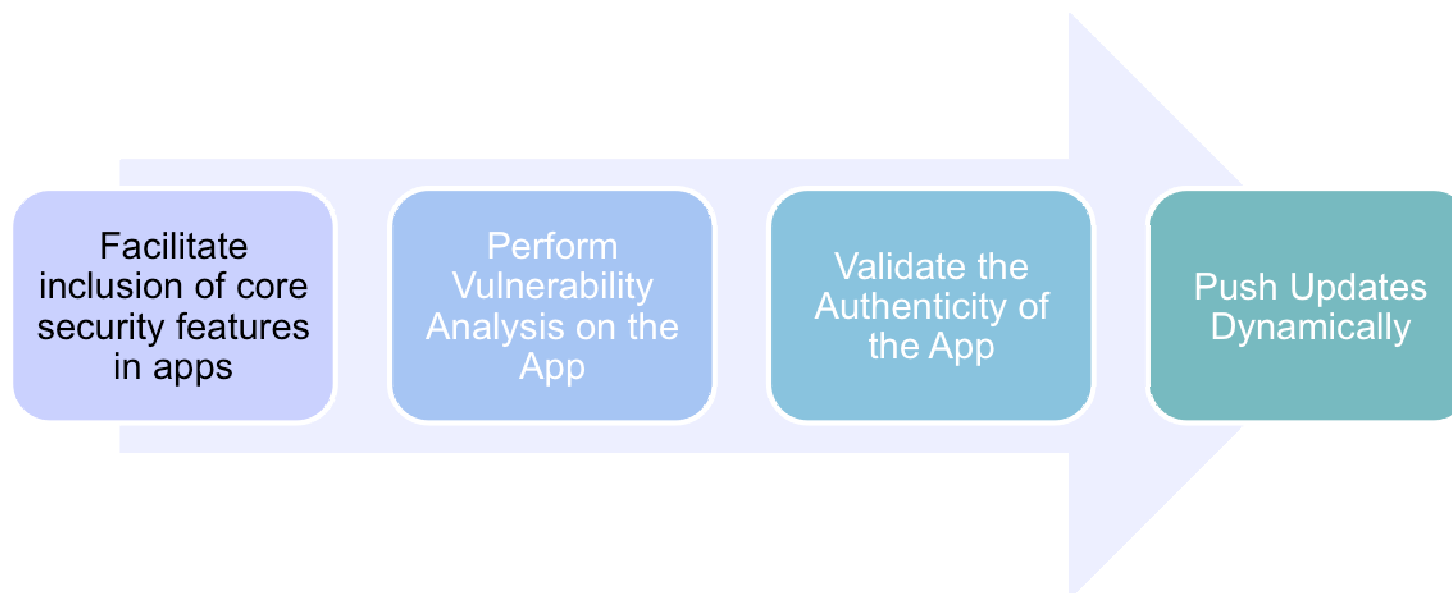
Context-Aware Risk Mitigation With IBM Mobile Security



- ❖ IBM Security Access Manager (ISAM) for Mobile affords customers with the ability to compute risk for an interaction based on the context of the user and configure authentication processes
 - ISAM provides the infrastructure to customize the authentication and authorization of both the user and the device (i.e. certificate-based, biometrics etc).
- ❖ Mobile apps can employ the risk score generated by ISAM for Mobile to control authorization to various transactions during that interaction and ISAM also delivers enhanced session management support to mitigate the risk of man-in-the-middle attack.
- ❖ ISAM integrates with IBM WorkLight



Interaction Interface is Critical



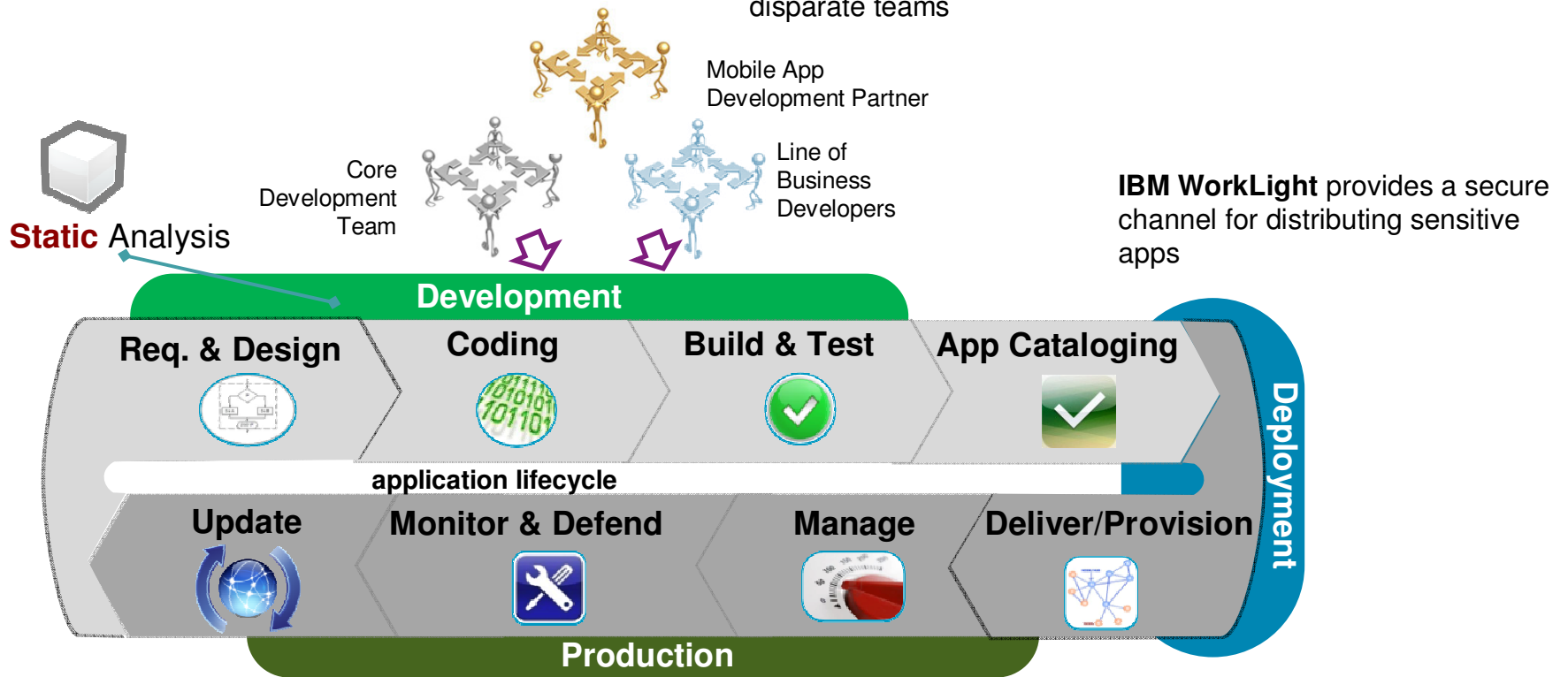
- Mobile developers need to be assisted with standardized proven techniques to quickly incorporate core security features in their apps (i.e. encryption of locally stored data)
- Vulnerability analysis on the app can significantly mitigate the exploitation of the app and its chances of going rogue
- During each interaction validate that the app has not been modified in any way to improve confidence in the integrity of the interaction
- Dynamically update the app in the event the app has been compromised or new vulnerabilities were identified

Protecting Mobile App Interaction With IBM Mobile Security

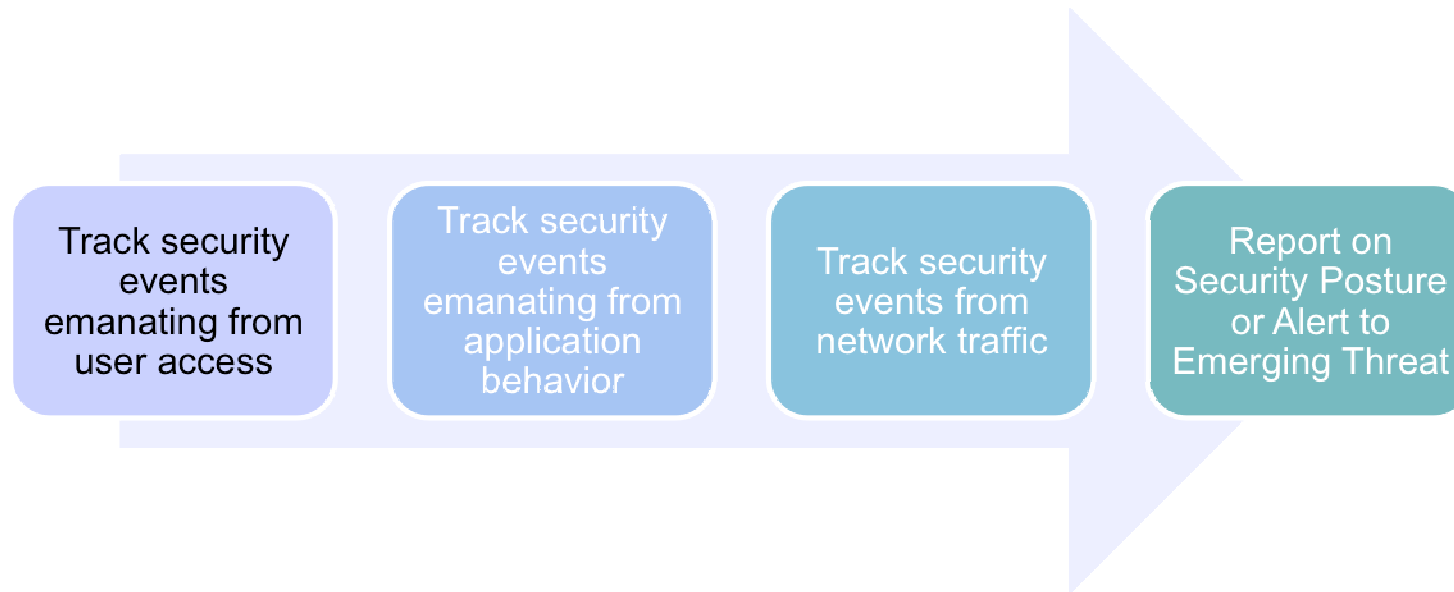


IBM AppScan enable static vulnerability testing with full-trace analysis to facilitate developer development and minimizes false positives to improve productivity

IBM WorkLight offers a consistent development environment which offers core security features developers can embed in their development standardizing the security posture of apps built by disparate teams

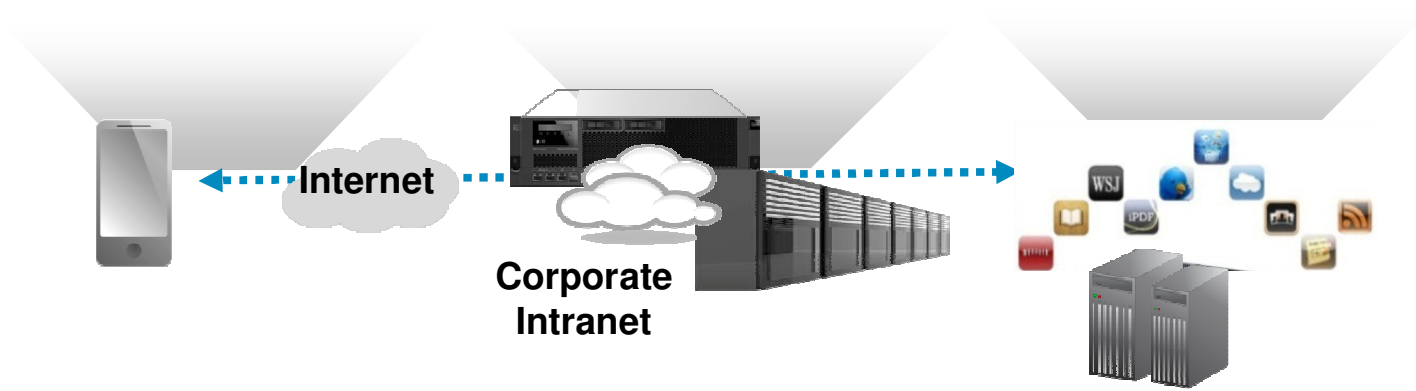
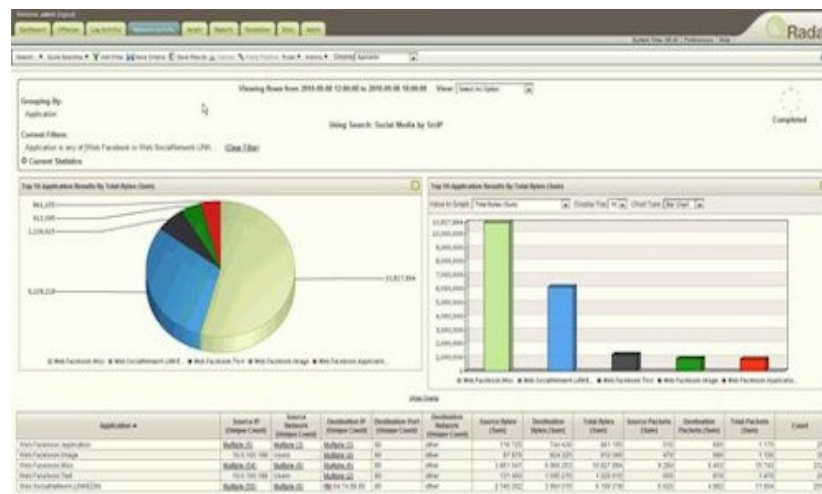


Vigilance is a Necessity



- Mobile user access needs to be monitored to potentially identify abnormal behavior
- End-to-end visibility of mobile app behavior is needed to identify malicious or rogue apps
- Constant awareness of network traffic allows an organization to identify threats and take appropriate response
- Reporting for compliance as well as proactive action to improve response time to an emerging threat will reduce exposure

IBM Qradar SIEM delivers mobile security intelligence by monitoring data collected from other mobile security solutions (i.e. IBM Security Access Manager, AppScan etc) – visibility, reporting and threat detection.



IBM Mobile Security

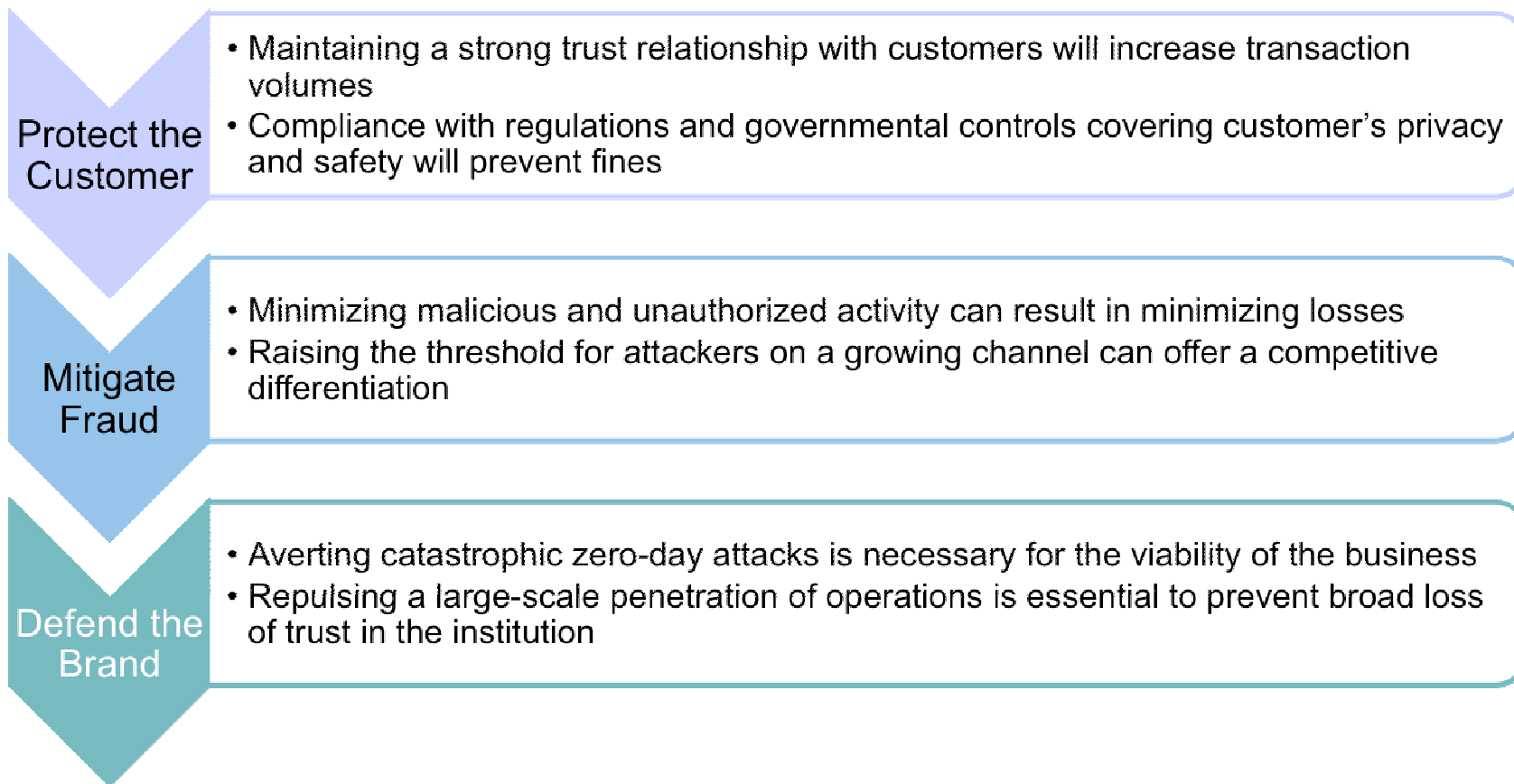


Device Management	Network, Data, and Access Security	Application Layer Security
Security for endpoint device and data	Achieve visibility and adaptive security policies	Develop and test applications

The Challenge

Mobile payments are set to increase 62% in value through 2012 to reach \$171.5bn (\$106bn in 2011). An average 42% annual growth will see total value of mobile transactions rise to \$617bn by 2016.

- Gartner





© Copyright IBM Corporation 2013. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software. References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in these materials may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. IBM, the IBM logo, Rational, the Rational logo, Telelogic, the Telelogic logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.