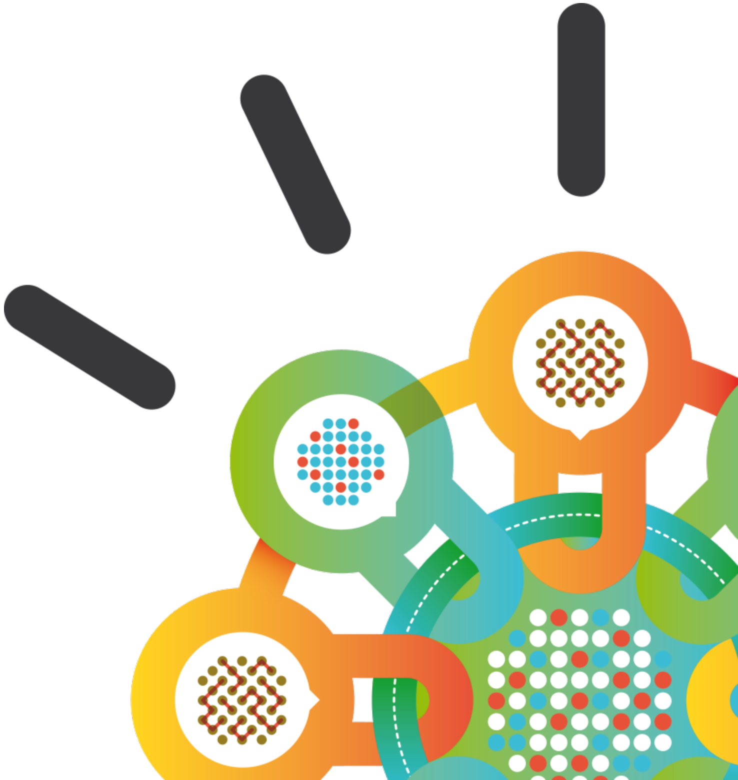
Security Intelligence.
Think Integrated.

Powering Security and Easy Authentication in a Multi-Channel World

Archit Lohokare
Global Product Manager
IBM Security Systems



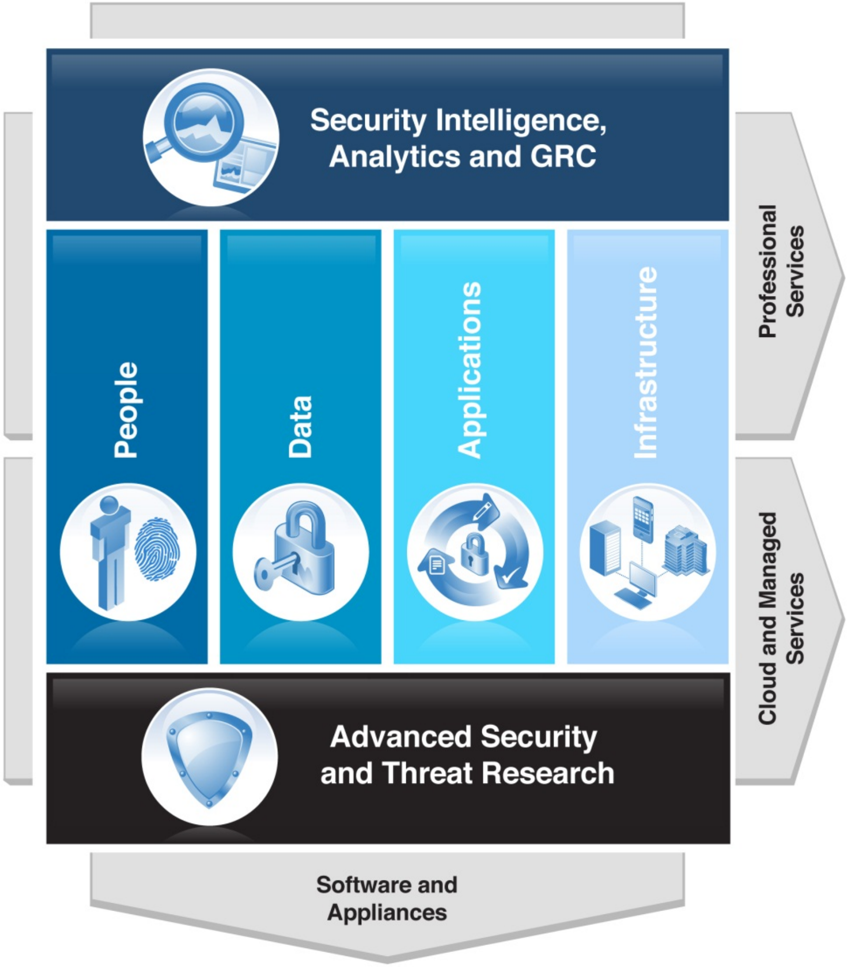
IBM Security Systems division is one of the largest security software focused vendors in the world

IBM Security Systems

- Only vendor in the market with end-to-end coverage of the security foundation
- $1.8B investment in innovative technologies
- 6K+ security engineers and consultants
- Award-winning X-Force® research
- Largest vulnerability database in the industry

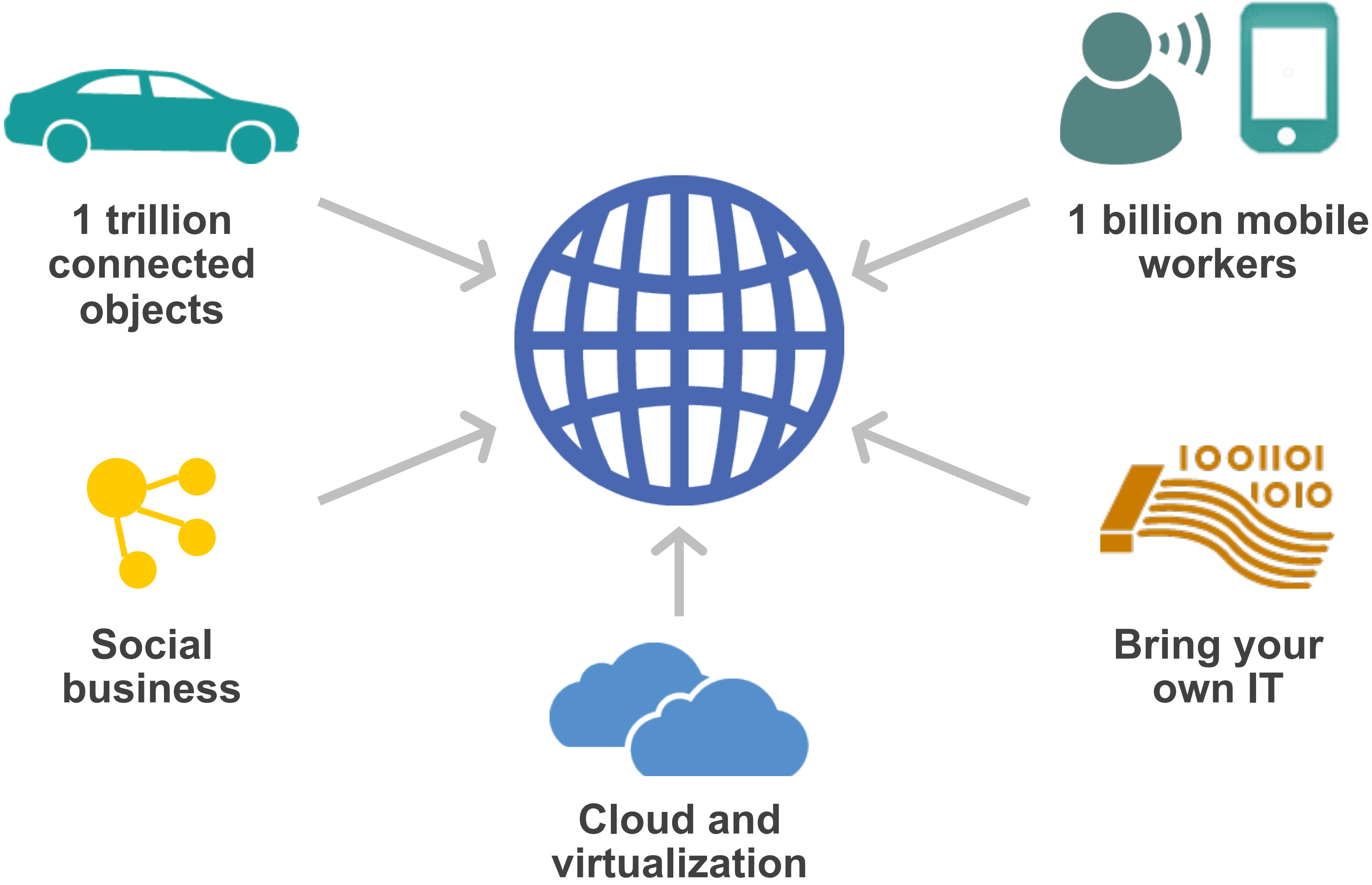
Intelligence • Integration • Expertise

IBM Security Framework


Security Intelligence, Analytics and GRC
People
Data
Applications
Infrastructure
Advanced Security and Threat Research
Professional Services
Cloud and Managed Services
Software and Appliances

IBM is ranked #1 by IDC in Identity and Access Management (IAM) and Security & Vulnerability Management (SVM)

New Technologies ➔ Multi-Perimeter World



1 trillion connected objects

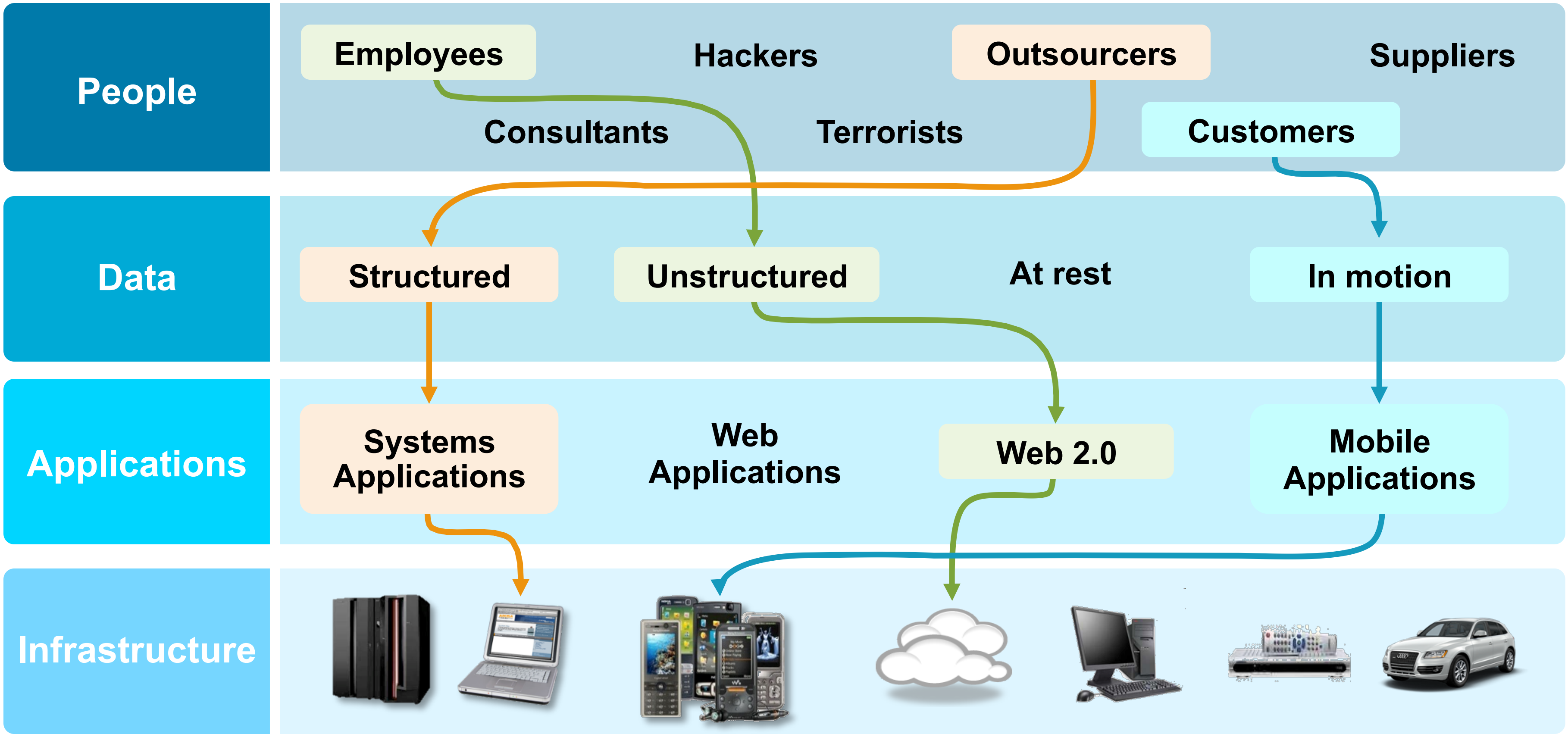
1 billion mobile workers

Social business

Bring your own IT

Cloud and virtualization

Solving security issues is a complex, four-dimensional puzzle



People

Employees Hackers Outsourcers Suppliers

Consultants Terrorists Customers

Data

Structured Unstructured At rest In motion

Applications

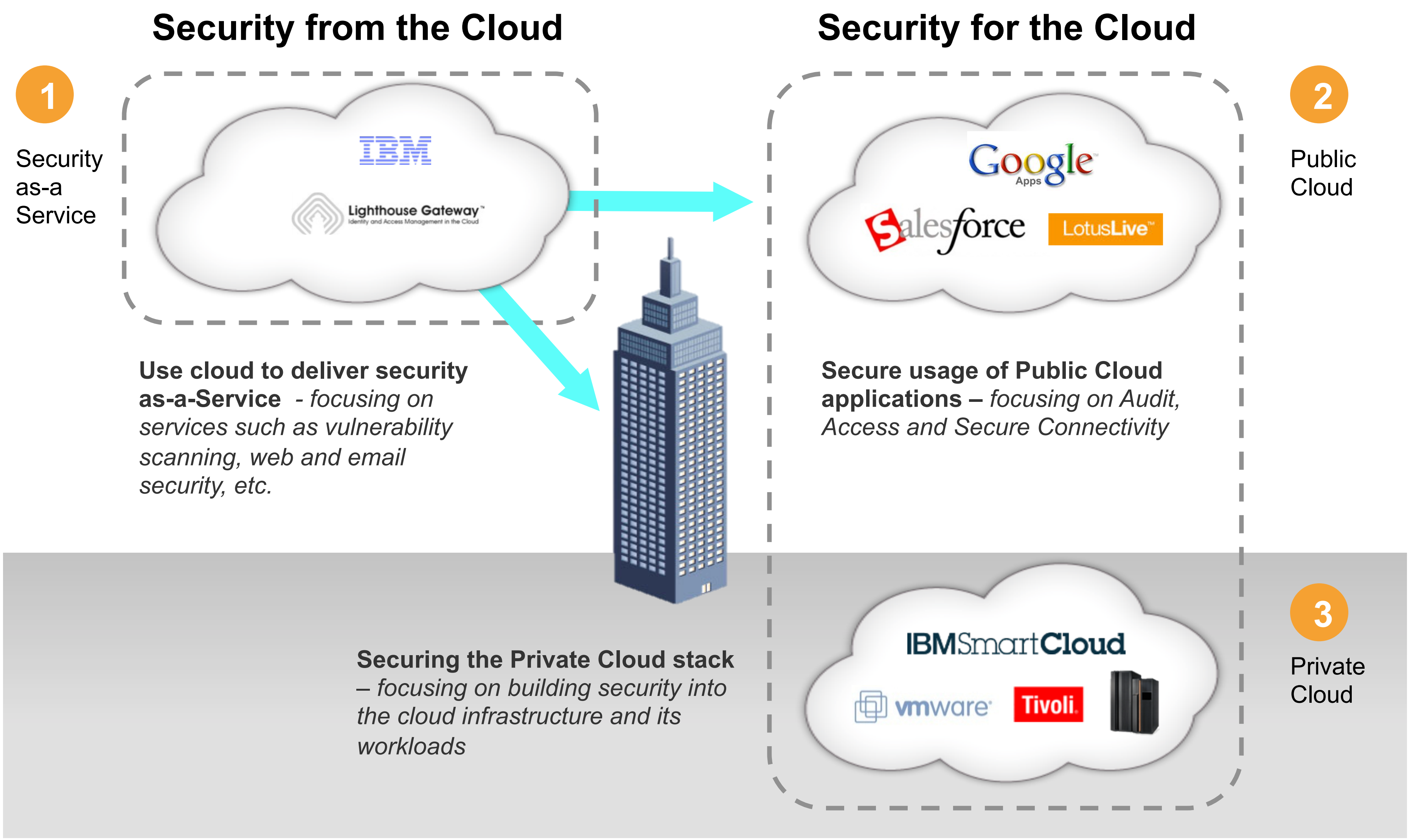
Systems Applications Web Applications Web 2.0 Mobile Applications

Infrastructure

Attempting to protect the perimeter is not enough – siloed point products and traditional defenses cannot adequately secure the enterprise

JK 2012-04-26

We see three prominent cloud security scenarios to help customers



Security from the Cloud

Security for the Cloud

1

Security as-a Service

Use cloud to deliver security as-a-Service - *focusing on services such as vulnerability scanning, web and email security, etc.*

2

Public Cloud

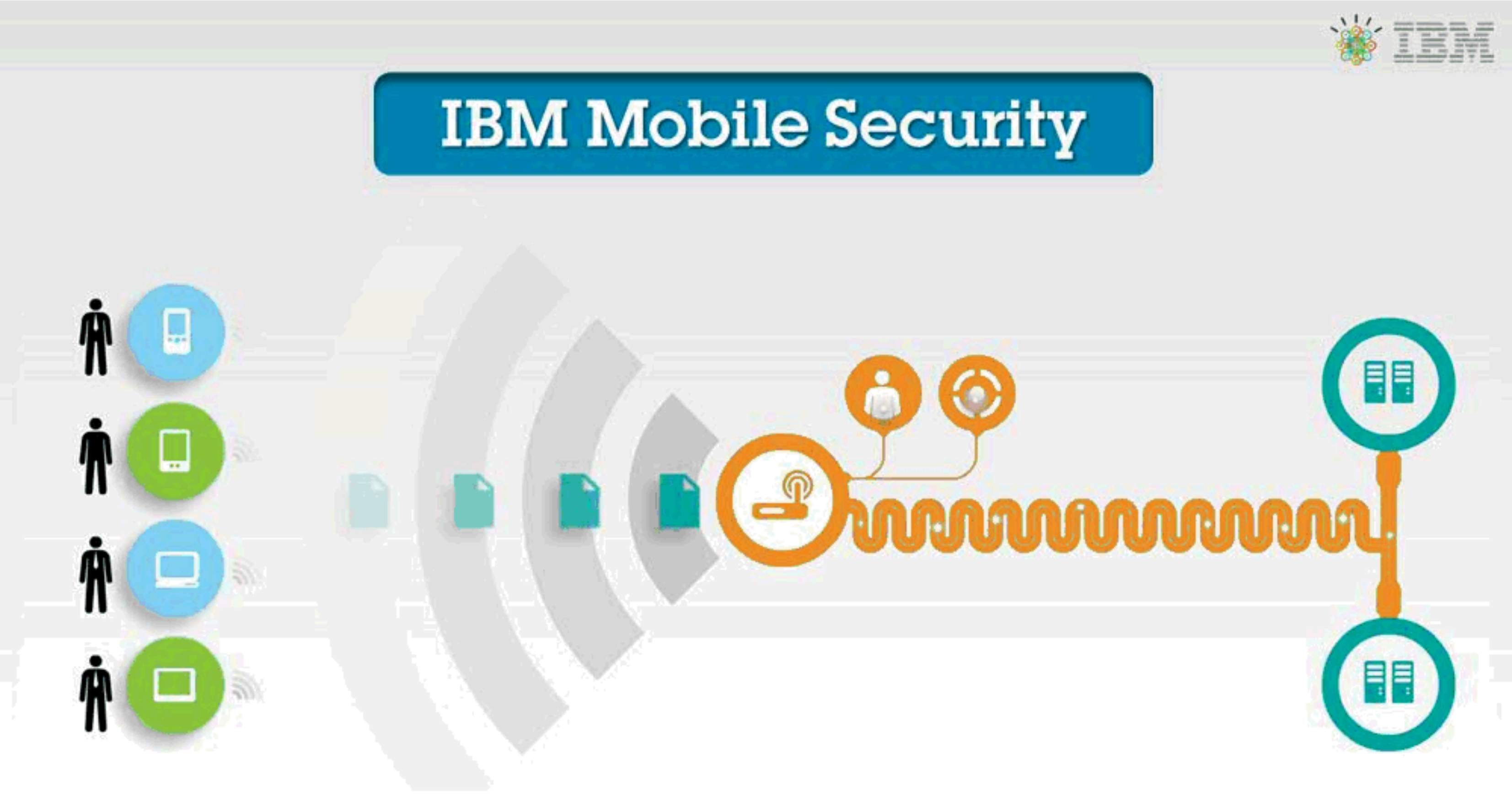
Secure usage of Public Cloud applications – *focusing on Audit, Access and Secure Connectivity*

Securing the Private Cloud stack *– focusing on building security into the cloud infrastructure and its workloads*

3

Private Cloud

The IBM Mobile Security Strategy secures the path that data travels through



Device Management

Security for endpoint device and data

Network, Data, and Access Security

Achieve visibility and adaptive security policies

Application Layer Security

Develop and test applications

IAM continues to be key part of next wave of security technology innovation

Advanced Analytics

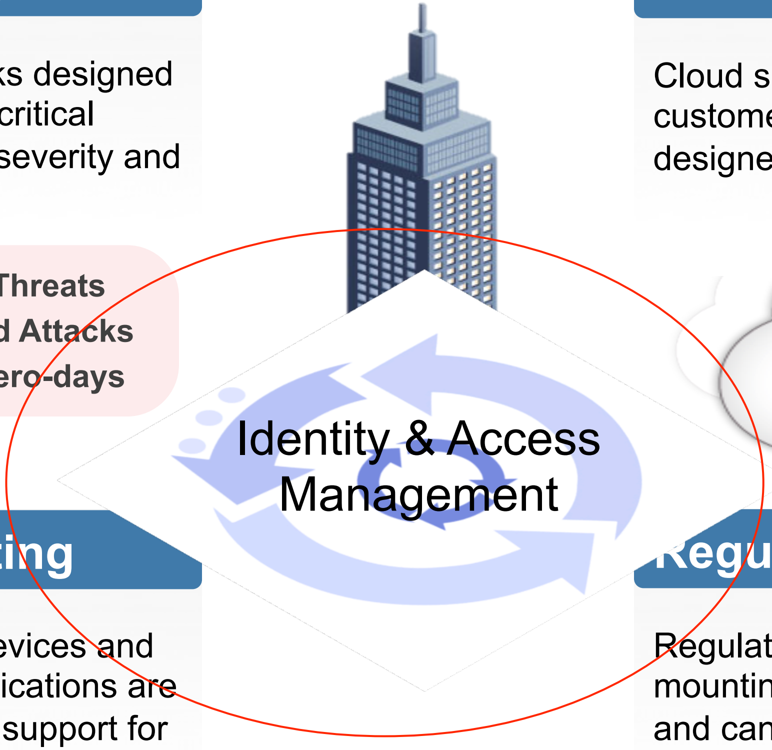
Sophisticated, targeted attacks designed to gain continuous access to critical information are increasing in severity and occurrence

Advanced Persistent Threats
Stealth Bots **Targeted Attacks**
Designer Malware **Zero-days**

Cloud Computing

Cloud security is a key concern as customers rethink how IT resources are designed, deployed and consumed

IBMSmartCloud
salesforce
vmware



Identity & Access Management

Mobile Computing

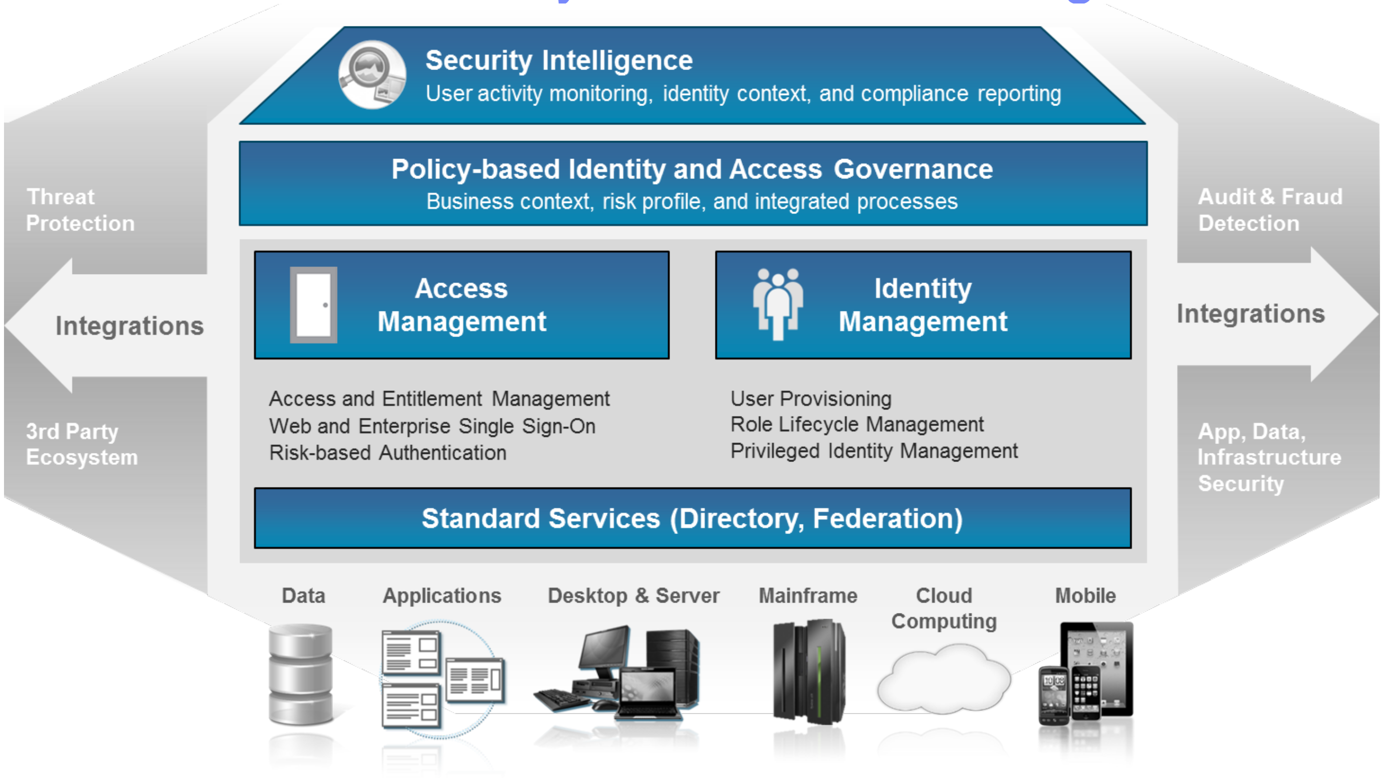
Securing employee-owned devices and connectivity to corporate applications are top of mind as CIOs broaden support for mobility

Regulation and Compliance

Regulatory and compliance pressures are mounting as companies store more data and can become susceptible to audit failures

GLBA
FFIEC
PCI Security Standards Council
Sarbanes-Oxley
Financial and Accounting Disclosure Information

IBM Next Generation Identity and Access Management Strategy


Security Intelligence
User activity monitoring, identity context, and compliance reporting
Policy-based Identity and Access Governance
Business context, risk profile, and integrated processes
Access Management
Identity Management
Access and Entitlement Management
Web and Enterprise Single Sign-On
Risk-based Authentication
User Provisioning
Role Lifecycle Management
Privileged Identity Management
Standard Services (Directory, Federation)
Threat Protection
Integrations
3rd Party Ecosystem
Audit & Fraud Detection
Integrations
App, Data, Infrastructure Security
Data
Applications
Desktop & Server
Mainframe
Cloud Computing
Mobile

Key Themes

Standardized IAM and Compliance Management

Expand IAM vertically to provide identity and access intelligence to the business; Integrate horizontally to enforce user access to data, app, and infrastructure

Secure Cloud, Mobile, Social Interaction

Enhance context-based access control for cloud, mobile and SaaS access, as well as integration with proofing, validation and authentication solutions

Insider Threat and IAM Governance

Continue to develop Privileged Identity Management (PIM) capabilities and enhanced Identity and Role management

Secure user access with IBM’s Next Generation Access Management

- **IBM Security Access Manager for Web**
  - User access + integrated web content protection
  - New Hardware Appliance (Access Manager Proxy)
  - Highly scalable web access management
  - Lower TCO and easy to deploy 3rd party integration

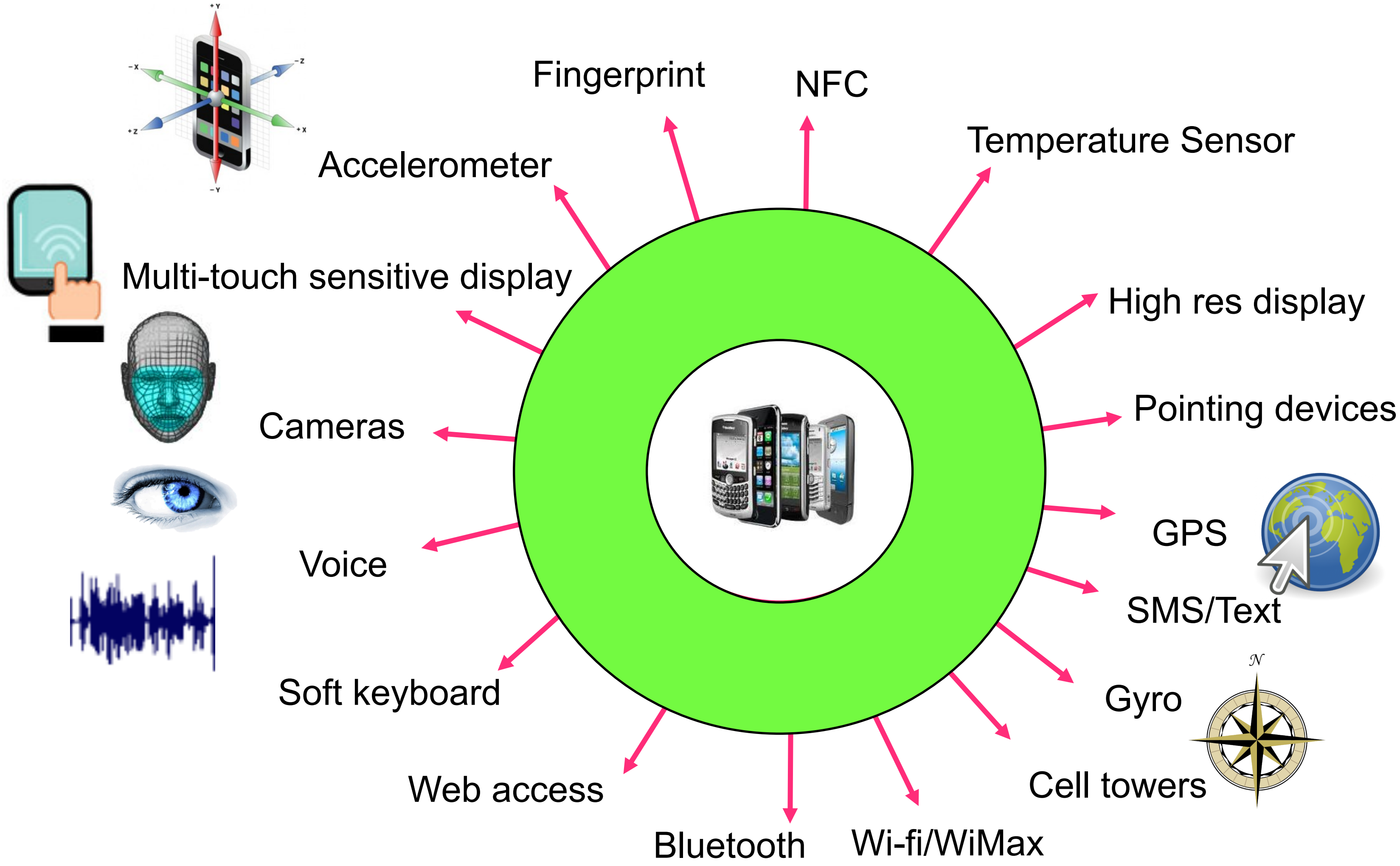
- **IBM Security Access Manager for Cloud & Mobile***
  - Federation and built-in Risk-based Access control
  - Ease of SaaS / Cloud SSO with out-of-box Integration
  - Entitlement management with risk-based access policy support and new policy simulator for ease of deployment

Web Access & Application Protection (software, virtual, HW appliance)

Federated, Risk-based Access

* Marketing bundle of Federated Identity Manager and Security Policy Manager

Smartphones: Extremely Rich in Channels and Modalities that can be leveraged to improve users' assurance



Accelerometer

Fingerprint

NFC

Temperature Sensor

Multi-touch sensitive display

High res display

Cameras

Pointing devices

GPS

Voice

SMS/Text

Gyro

Soft keyboard

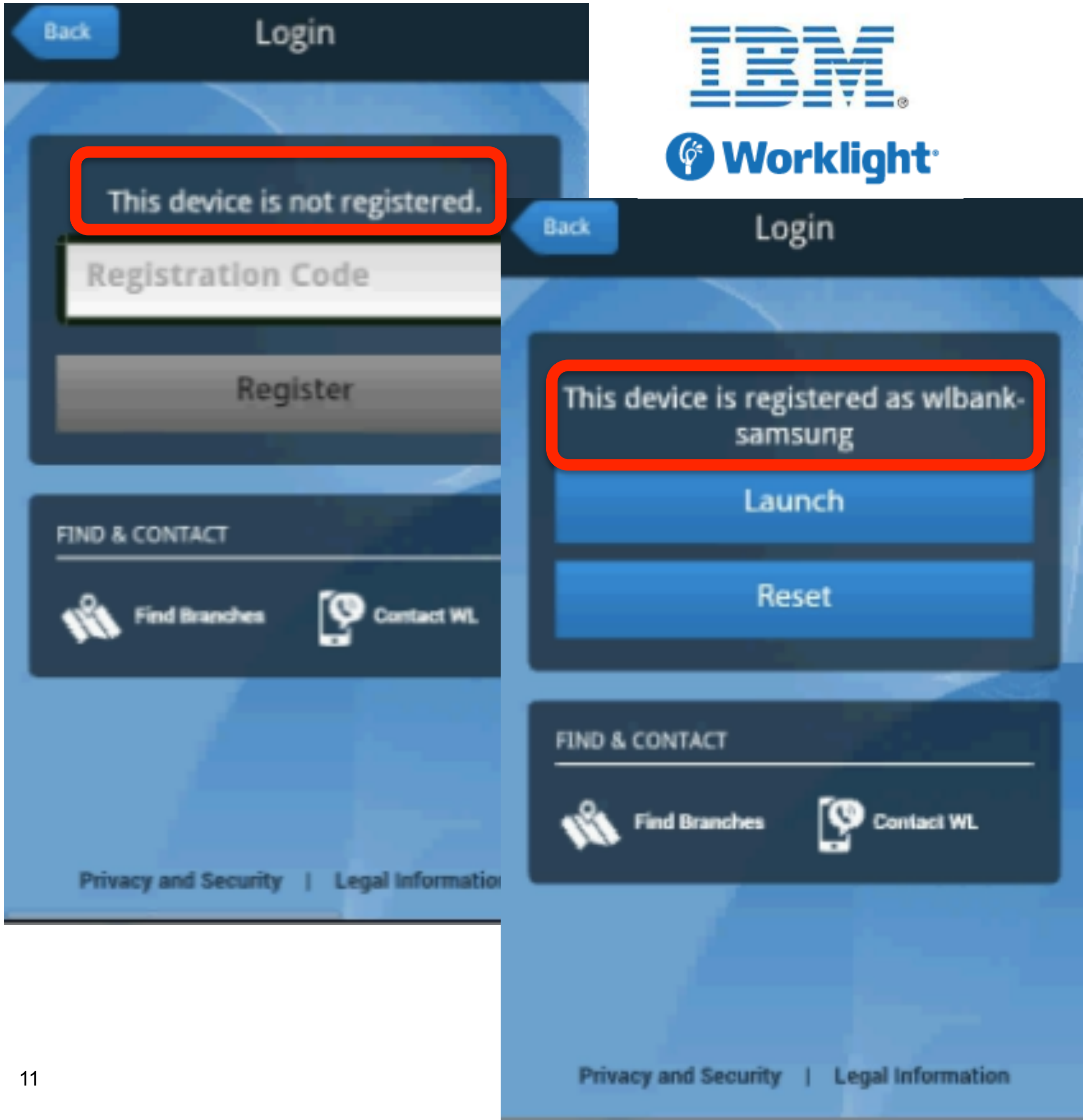
Cell towers

Web access

Bluetooth

Wi-fi/WiMax

Build secure access into the DNA of native and hybrid mobile apps



Back

Login

This device is not registered.

Registration Code

Register

FIND & CONTACT

Find Branches

Contact WL

Privacy and Security | Legal Informatio

Back

Login

This device is registered as wlbank-samsung

Launch

Reset

FIND & CONTACT

Find Branches

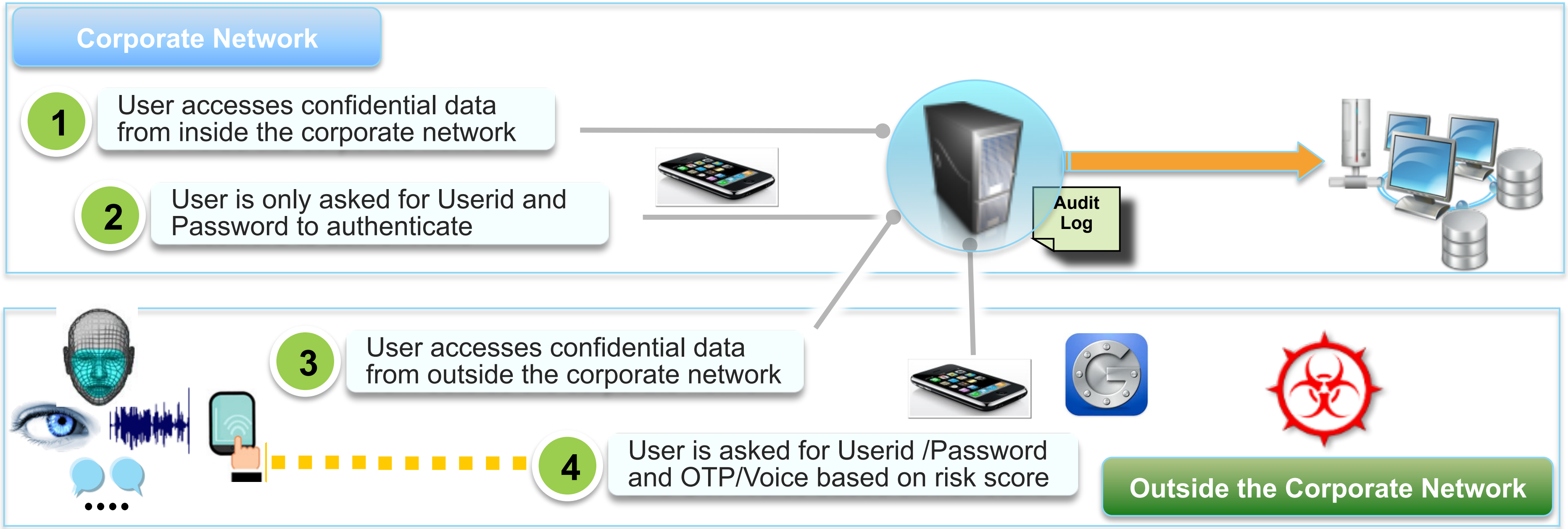
Contact WL

Privacy and Security | Legal Information

IBM Worklight

- Secure device registration and fingerprinting using OAuth 2.0 for IBM Worklight Applications
- Reduce risk of mobile app fraud using Risk-based Access
- Increased security and flexibility for mobile app authentication with built-in OTP and Google Authenticator support

Context-aware access to secure mobile user access can be strengthened by Voice Biometrics

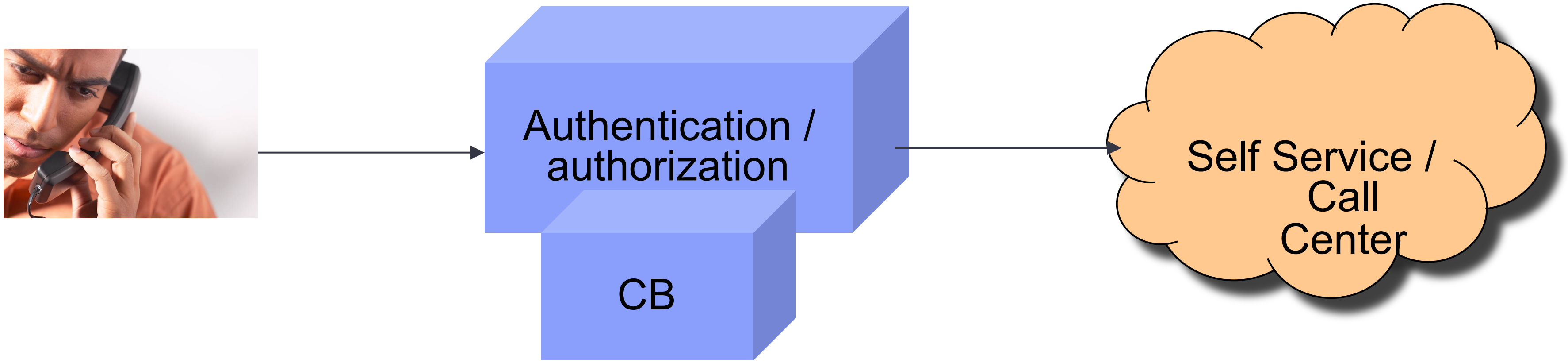

Corporate Network
1
User accesses confidential data from inside the corporate network
2
User is only asked for Userid and Password to authenticate
Audit Log
3
User accesses confidential data from outside the corporate network
4
User is asked for Userid /Password and OTP/Voice based on risk score
Outside the Corporate Network

- Risk-based Access feature to determine and score risk levels using user attributes and real-time context (e.g. location, device)
- Enforce mobile user access based on risk-level (e.g. permit, deny, step-up authenticate)
- Support mobile authentication with built-in One-Time Password (OTP) and provide ability to integrate with 3rd party strong authentication vendors, as needed

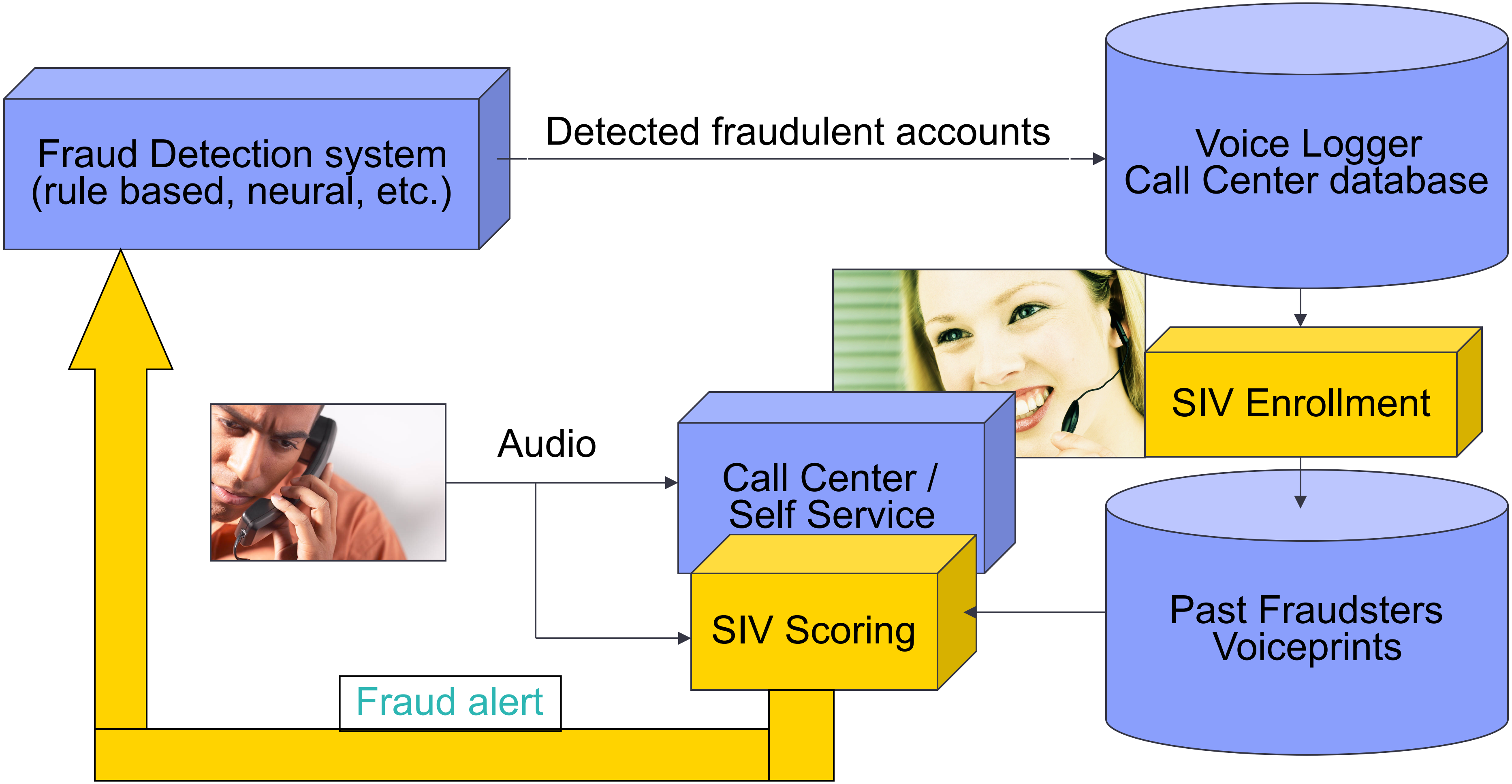
A Few Key Scenarios

Phone Channel / Scenario 1: Automated User Authentication and Authorization

- User calls a VRU self service application, or calls a call center and goes through the automated system
- Value add of using CB:
  - Faster user authentication of true users
  - Higher fraud detection rate
  - Ability to authenticate and authorize simultaneously

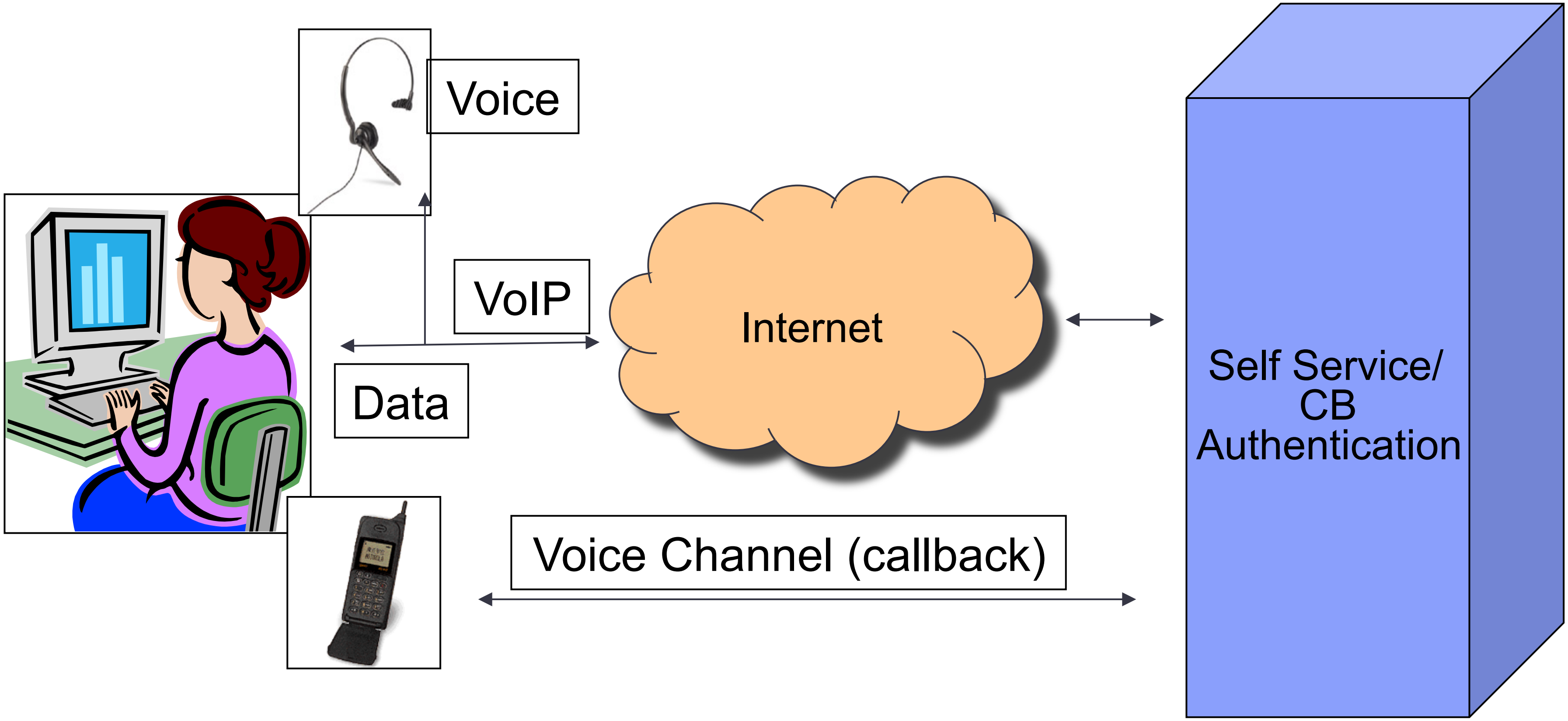


Phone Channel / Scenario 2: Offline fraud detection - Detecting repeating fraudsters



ibm.com/security

Internet Channel: Data, VoIP and Callback Scenarios



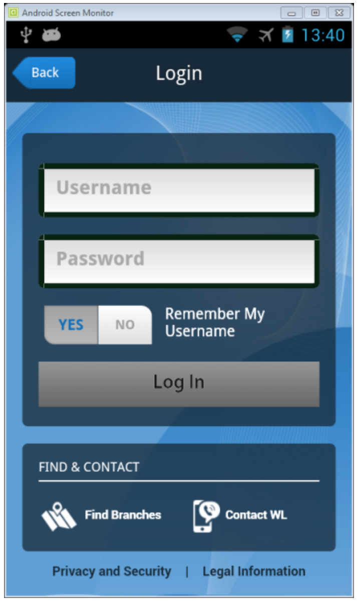
Appropriate CB policy can also handle No-Voice (Data-Only) authentication

Scenario 1: One-time registration with OAuth

- OAuth-enabled Worklight banking application.
  - User credentials are not entered or stored on the device.
  - User is not required to authenticate each time the application opens.
  - Revocation is possible on a application and per-device basis.

Before

U/P every application launch



Android Screen Monitor

13:40

Back Login

Username

Password

YES NO Remember My Username

Log In

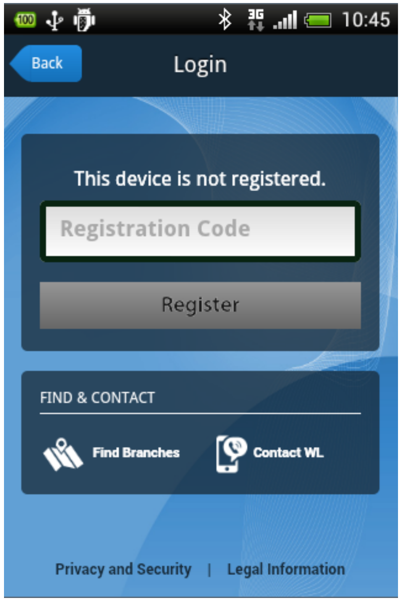
FIND & CONTACT

Find Branches Contact WL

Privacy and Security | Legal Information

After

One-time registration code



10:45

Back Login

This device is not registered.

Registration Code

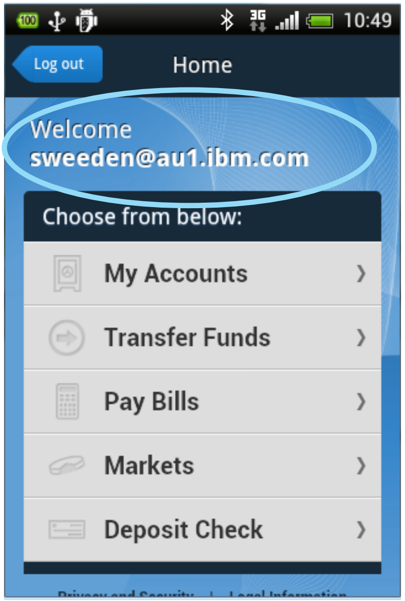
Register

FIND & CONTACT

Find Branches Contact WL

Privacy and Security | Legal Information

Identity-aware application launch



10:49

Log out Home

Welcome
sweeden@au1.ibm.com

Choose from below:

My Accounts ›

Transfer Funds ›

Pay Bills ›

Markets ›

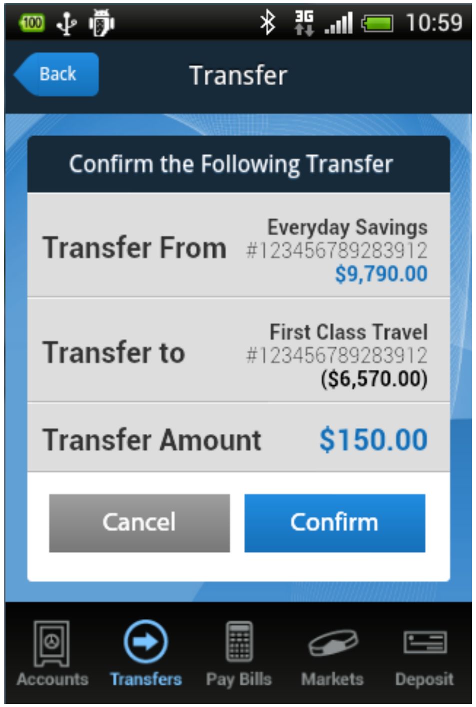
Deposit Check ›

Privacy and Security | Legal Information

Scenario 2: Risk-based access policy and strong authentication

- Transactions < $100 are allowed with no additional authentication
- User attempts transfer of amount >= $100 – requires strong authentication

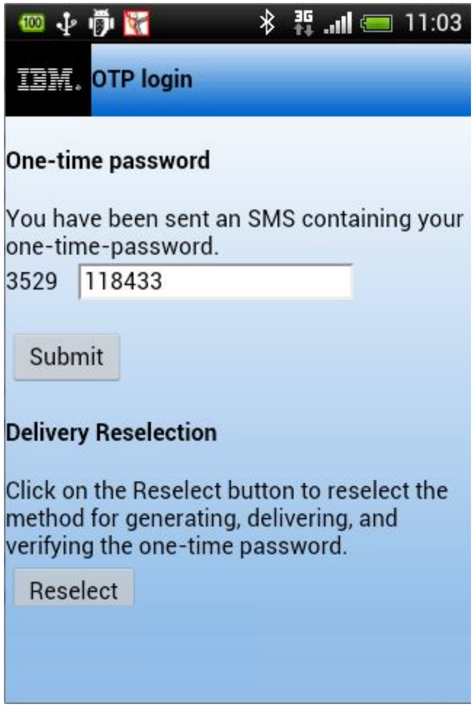
User attempts high-value transaction



Confirm the Following Transfer

Transfer From	Everyday Savings #123456789283912 $9,790.00
Transfer to	First Class Travel #123456789283912 ($6,570.00)
Transfer Amount	$150.00

Strong authentication challenge



One-time password

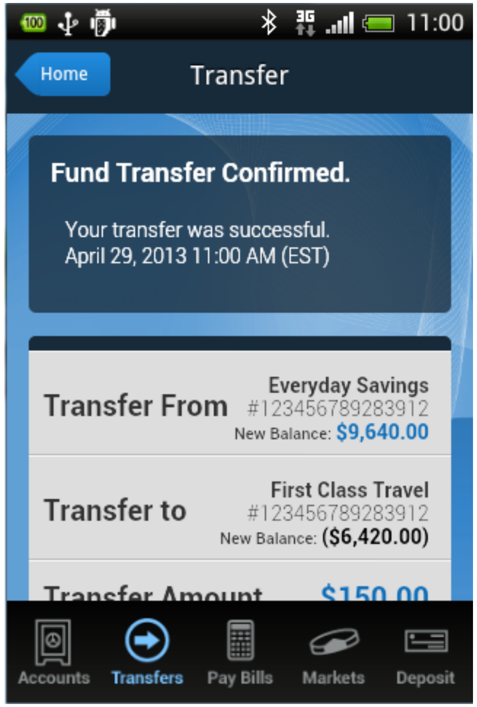
You have been sent an SMS containing your one-time-password.

3529 118433

Delivery Reselection

Click on the Reselect button to reselect the method for generating, delivering, and verifying the one-time password.

Transaction completes



Fund Transfer Confirmed.

Your transfer was successful.
April 29, 2013 11:00 AM (EST)

Transfer From	Everyday Savings #123456789283912 New Balance: $9,640.00
Transfer to	First Class Travel #123456789283912 New Balance: ($6,420.00)
Transfer Amount	$150.00