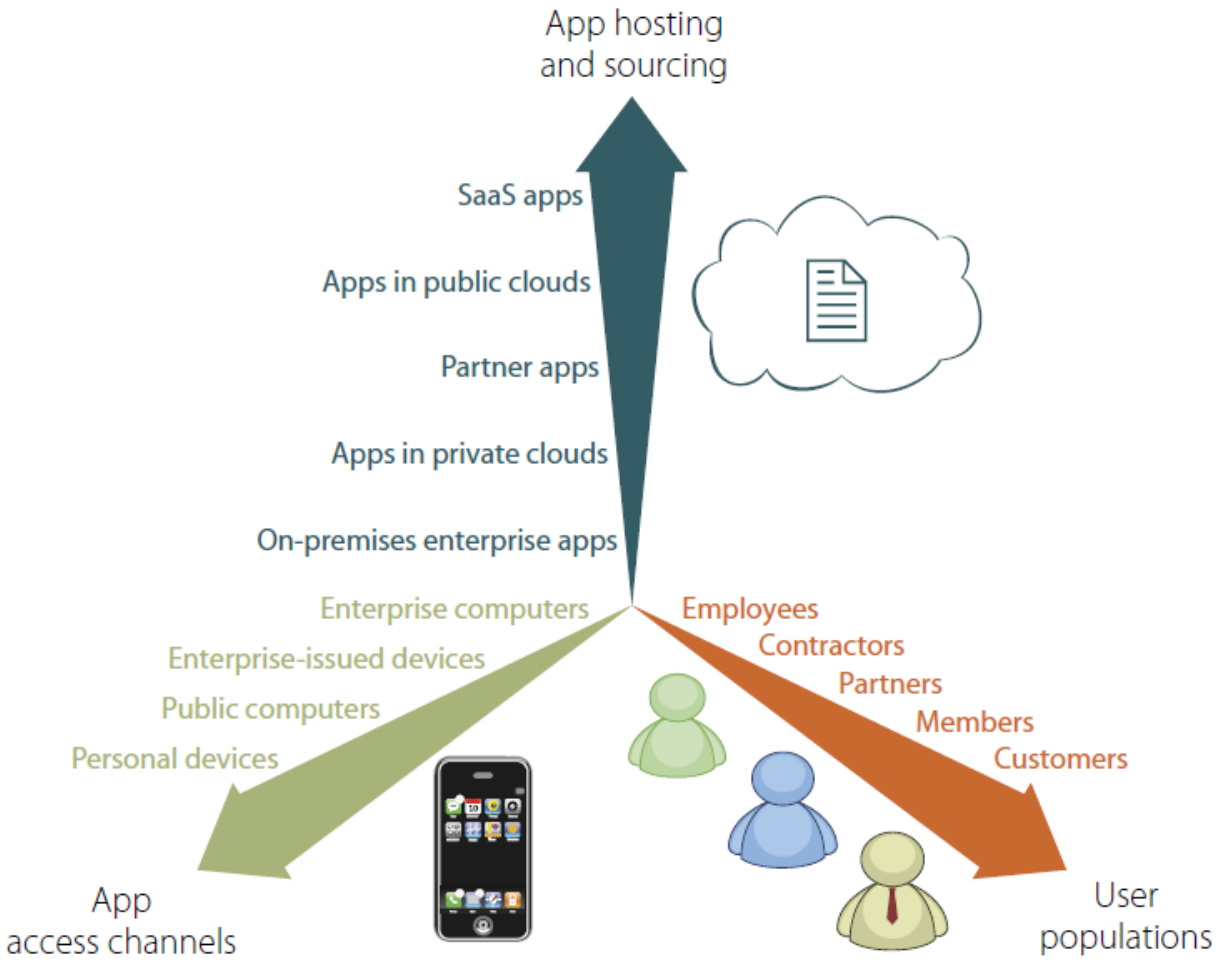
Rethinking Identity and Access Governance

Jörn Dierks
Chief Security Strategist EMEA
jdierks@netiq.com
20/03/2013

Every Organization is Different

Extended Enterprise Presents IAM Challenges In Three Dimensions



Forrester Research, Inc. "Navigate The Future Of Identity And Access Management" - Eve Maler, March 22. 2012

How Does IT Maintain Control?

You may need to rethink your approach to identity and access

Breaches are increasing

Everyone's gone mobile

The cloud is here

Budgets are shrinking

It's All About Access

What does it all mean and what should it do for you?

Elements of Identity

- Who/What are you?
  - Name, location, etc.
- Roles/Privilege
  - Title, Manager, etc.
- Relationship to business
  - Employee, Contractor, etc.

Access is a Relationship

- Applications
- Systems
- Data
- Resources
- Physical Facilities

Access Utilization

- Is activity aligned to roles and policy
  - Orphans, dormant access and entitlement creep
  - Privileged access control
- Distinguish attacker from insider activity

It’s All About The Right Access

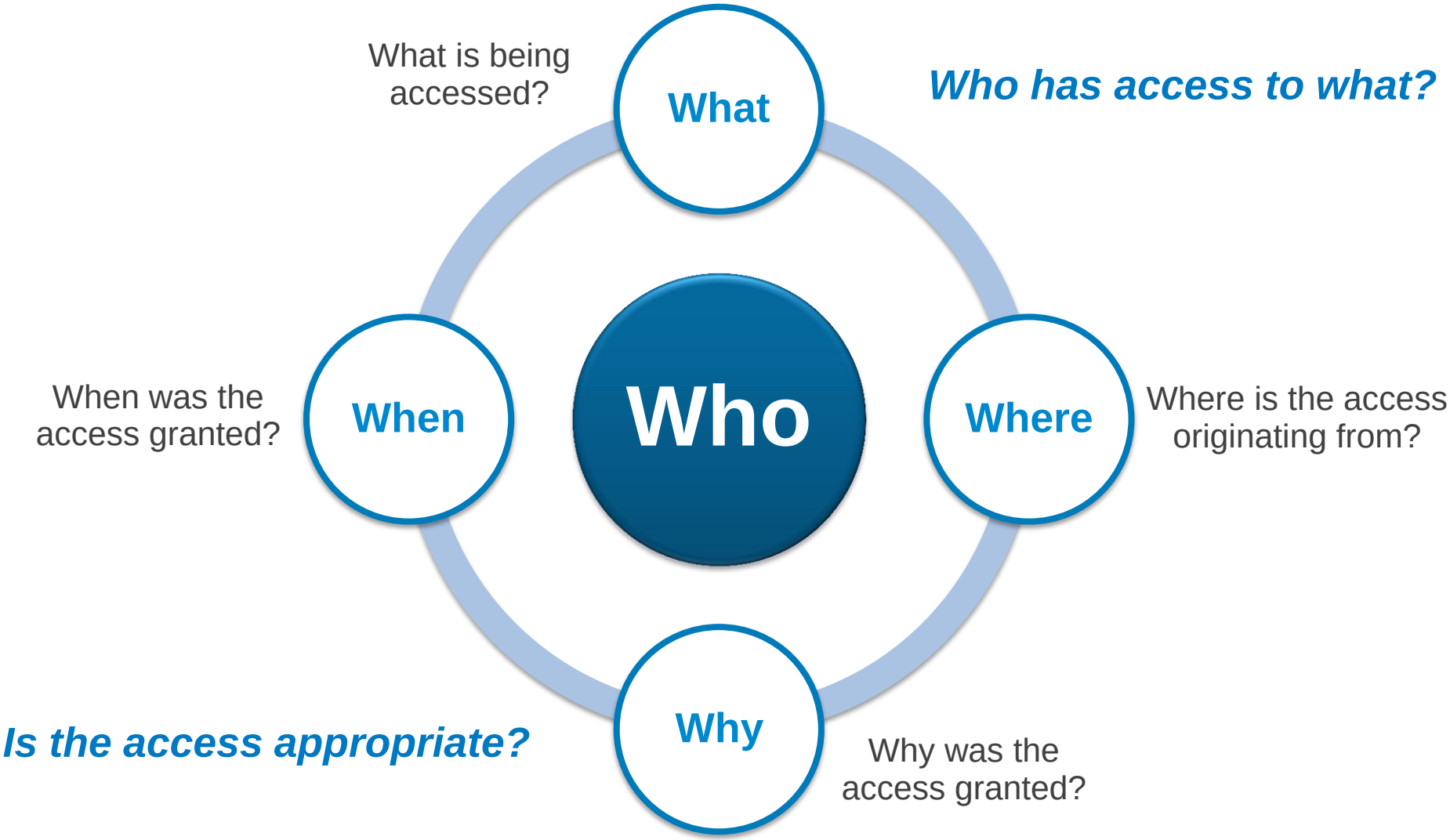
Right People, Right Resources, Right Time from Anywhere

What is “Right” Varies By Organization

Moving at the speed of business vs. mitigating business risks

Right Access Requires Proper Context

What, Where, Why and When add critical value to the Who



Right Access = Intelligent Access

Right people, right resources, right time, right device, right location

- Clearly understanding the 5 W's
  - More context around Who for better access decisions

- Organizational needs are in balance
  - Business Needs
    - Business policies and controls are in place
    - Organizational risk threshold is reflected in polices and controls
  - IT Resources and Assets
    - What is available, what are IT's capabilities?
    - What is the business getting out of the IT investment?

"We have brakes on our cars not so that we can stop, but so that we can go fast" – Sara Gates

Why Should You Care About Intelligent Access?

Mitigate Risk – Stay Out of the Press

"Security Breach Exposes Data on Millions of Payment Cards" —InformationWeek

UBS

~ $2 Billion Loss

SOCIETE GENERALE

~ $7 Billion Loss

"British parliament shut down e-mail system to prevent damage" —ZDNet

"Hospital patient data revealed"

SONY

PLAYSTATION® Network

Regulatory & Oversight Pressures

Internal Audit

Board of Directors – Oversight Groups

Move At The Speed of Business

IT should enable business agility vs. acting as a roadblock

vs.

IT should be the catalyst for the solution

Bringing IT and The Business Together

Flexibility

Control

Business Needs

IT Resources / Assets

3 Key Processes of Intelligent Access

Access Fulfillment

- **Identity Management**
- Granted access
  - Active decision
  - Automated process
- Access administration

Access Authorization

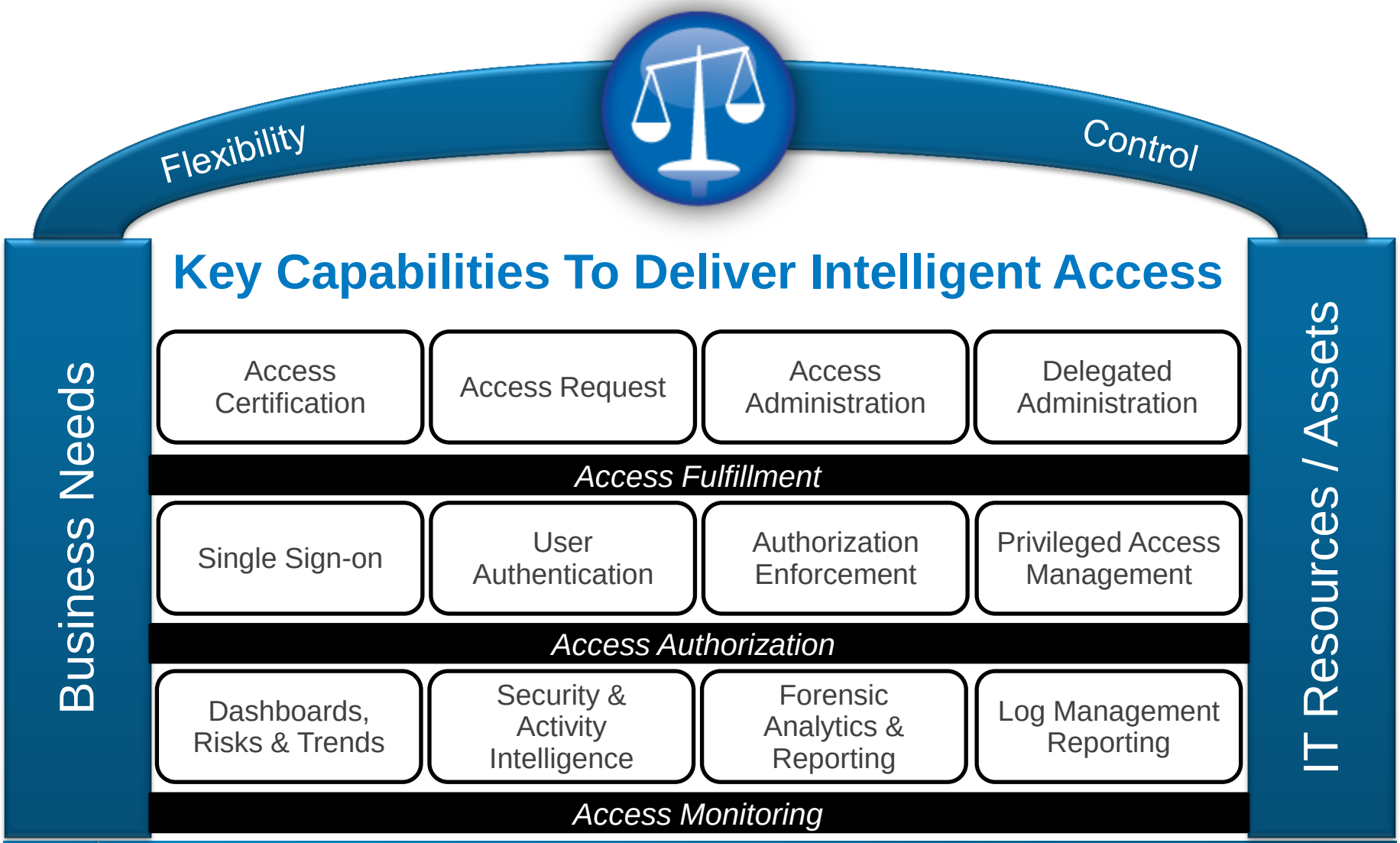
- **Access Management**
- Enforcement of access
  - Users, partners, customers, etc.

Access Monitoring

- **Security Management**
- Tracking and observing what is being done with the access
- Improper activity

What Are Your Priorities and Needs?

Access fulfillment, authorization and monitoring

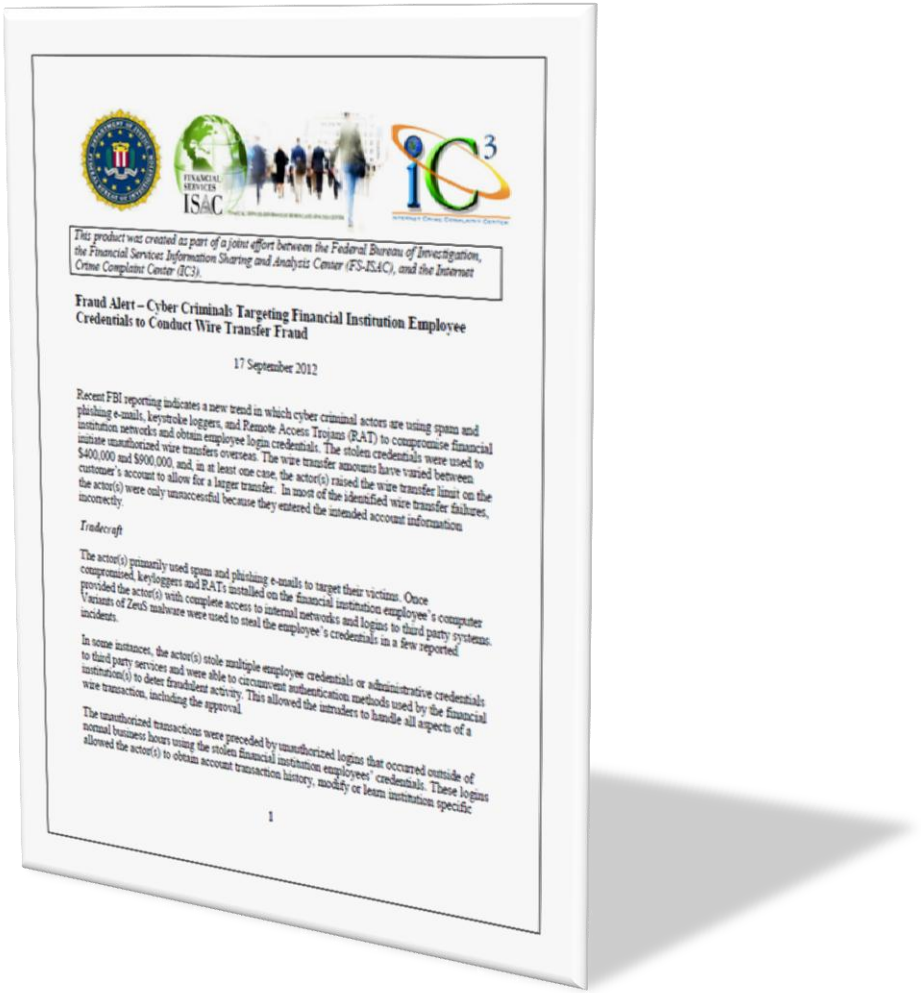


Use-Case

Use-Case – Wire Transfer Fraud

FBI Fraud Alert

Cyber Criminals Targeting Financial Institution Employee Credentials to Conduct Wire Transfer Fraud



This product was created as part of a joint effort between the Federal Bureau of Investigation, the Financial Services Information Sharing and Analysis Center (FS-ISAC), and the Internet Crime Complaint Center (IC3).

Fraud Alert – Cyber Criminals Targeting Financial Institution Employee Credentials to Conduct Wire Transfer Fraud

17 September 2012

Recent FBI reporting indicates a new trend in which cyber criminal actors are using spam and phishing e-mails, keystroke loggers, and Remote Access Trojans (RAT) to compromise financial institution networks and obtain employee login credentials. The stolen credentials were used to initiate unauthorized wire transfers overseas. The wire transfer amounts have varied between $400,000 and $900,000, and, in at least one case, the actor(s) raised the wire transfer limit on the customer's account to allow for a larger transfer. In most of the identified wire transfer failures, the actor(s) were only unsuccessful because they entered the intended account information incorrectly.

Tradecraft

The actor(s) primarily used spam and phishing e-mails to target their victims. Once compromised, keyloggers and RATs installed on the financial institution employee's computer provided the actor(s) with complete access to internal networks and logins to third party systems. Variants of ZeuS malware were used to steal the employee's credentials in a few reported incidents.

In some instances, the actor(s) stole multiple employee credentials or administrative credentials to third party services and were able to circumvent authentication methods used by the financial institution(s) to deter fraudulent activity. This allowed the intruders to handle all aspects of a wire transaction, including the approval.

The unauthorized transactions were preceded by unauthorized logins that occurred outside of normal business hours using the stolen financial institution employees' credentials. These logins allowed the actor(s) to obtain account transaction history, modify or learn institution specific

1

Use-Case – Wire Transfer Fraud

- Use-Case:
  - Cyber Criminals Target Finalcial Institution Employee Credentials to Conduct Wire Transfer Fraud
  - Released by the FBI (and others) on Sept 17, 2012
- What‘s the story?
  - Spam and phishing to target victims
  - Keyloggers and Remote Access Trojans installed on employee‘s computer
  - Variants of ZeuS malware used to steal employee‘s credentials in some cases
  - In some cases, multiple employee credentials and admin credentials were stolen, wire tranfer limits raised

Use-Case – Wire Transfer Fraud

- What‘s the story? (continued)
  - Authentication methods used to deter fraudulent activity were circumvented, allowing intruders to handle all aspects of a wire transaction, incl. approval.
  - Unauthorized logins outside of normal hours, allowing actors to obtain account transaction history, learn about wire transfer system, read manuals and training on the use of the systems.
  - In at least one instance, the actors browsed through accounts, apparently selecting the ones with the highest balance.
  - Victims: Small-to-medium sized banks, however a few large banks have also been affected.
  - In some incidents, DDoS attacks were used to distract bank‘s personnel.

Align Business and Security

- Difficult to achieve
- Common issues:
  - Language
  - Needs
  - Awareness
  - Complexity
  - Management buy-in
  - Silo-thinking
  - And many more

Identify the Real Risks

- What is our risk posture?
- Do we understand risk?
- Do we measure risk?
- Do we do it right?
  - ...really?
  - Who determines what is “right“?
  - ...so again:
- Do we understand the risks we‘re facing?

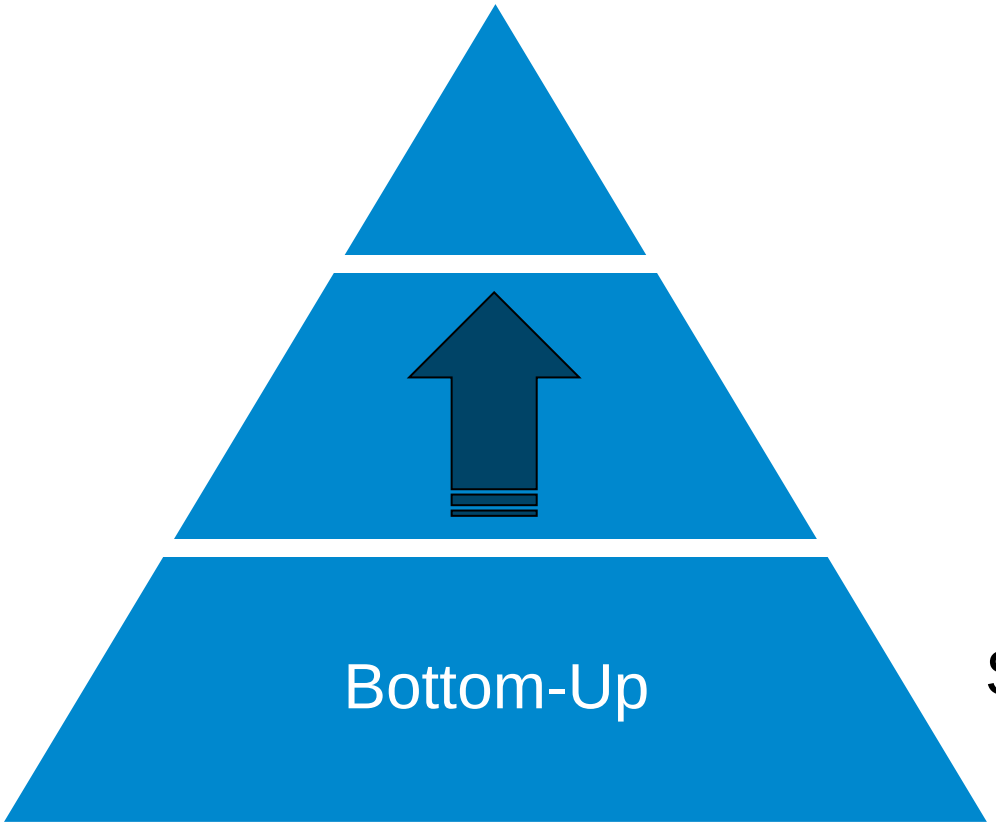
People are Key

Very often, people are the weakest link.

Think of Awareness

Needs Analysis

Typical / Traditional Approach



Operationalization

Security Management

Security Point Products

Typical Approach:
Silos Prevent Intelligent Analytics

What is the

IMPACT

Verizon Data Breach Report 2012

- **92%**

  of breaches was discovered by a third party

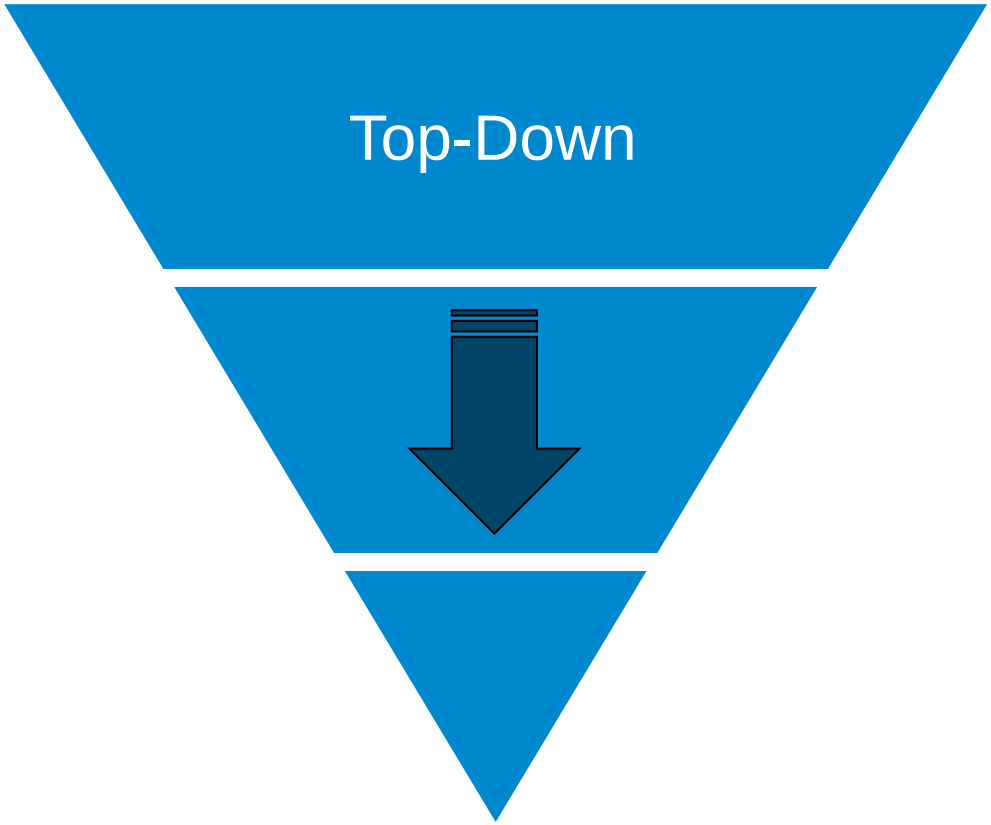
- **85%**

  of breaches took weeks or more to discover

- **84%**

  of organizations had evidence in their log files

Alternative Approach

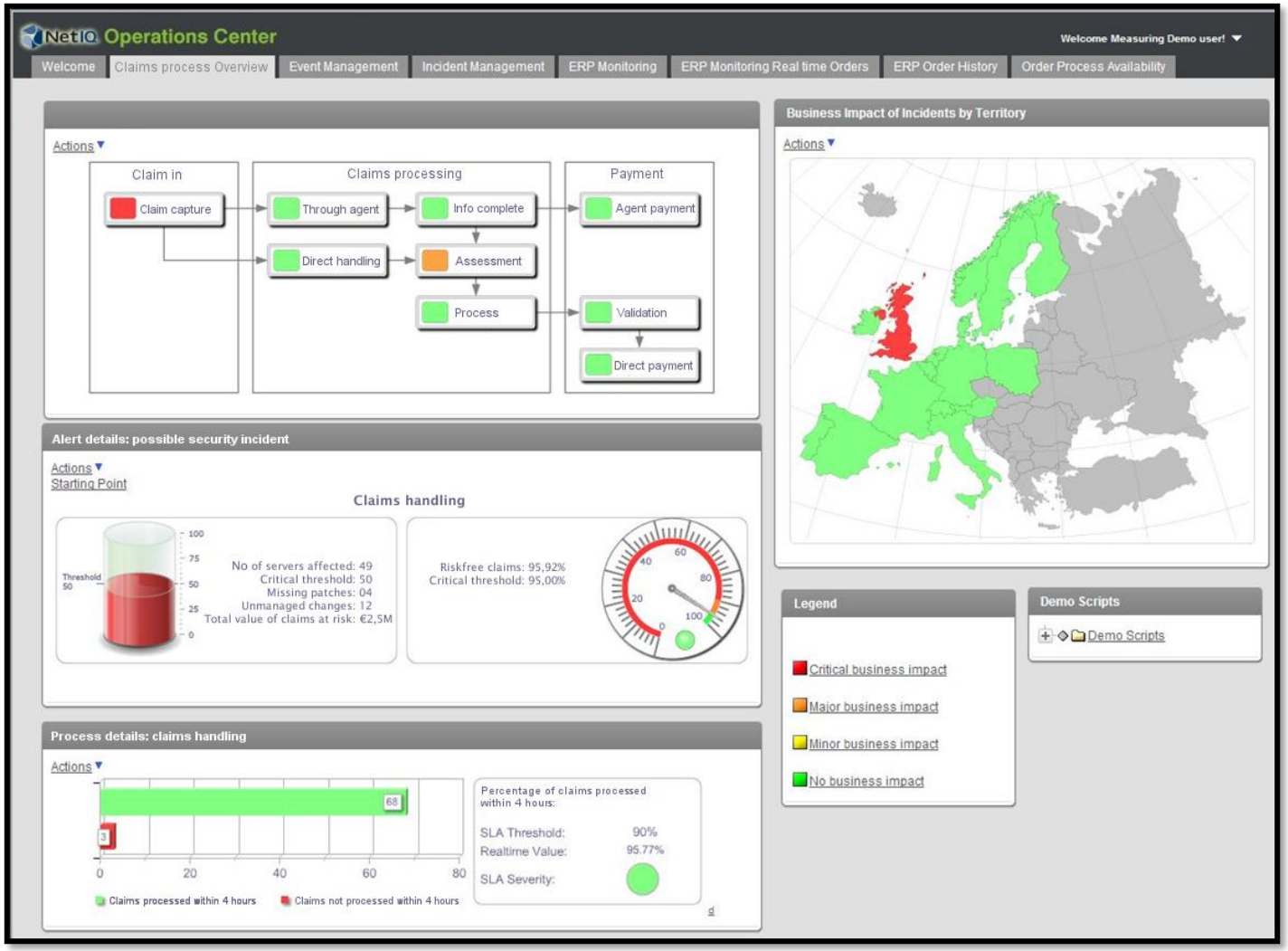


Business Processes

Security Metrics

Security Management and Operations

Threat Landscape in a Single Pane of Glass



Let‘s Come Back to the Use-Case

Use-Case – Wire Transfer Fraud

- So what to do?
  - FBI released a list of advices around people, process and technology
  - Bird‘s Eye View:
    - Many components come together
    - Including spam and phishing, account mis-use, out-of-hour usage, privileged account mis-use, DDoS activity, etc.
  - What can Security Management do?
    - Change Detection and Privileged User Monitoring
    - Security Information and Event Management (SIEM)
    - Anomaly Detection and Security Dashboards
    - Privileged user access restrictions

Use-Case – Wire Transfer Fraud

- So what to do? (continued)
  - And outside of Security Management?
    - Identity and Access Management
    - Seggragation of duty and two-man rule
    - Access Governance
    - Fraud Detection
    - Anti-Virus, Anti-Spam, Anti-Phishing
    - Application White-Listing
  - And what about Dashboards and Metrics?
    - Build the Business Service of Wire Transfers
    - Implement supporting technology event feeds to visualize service disruptions AND anomalies

Solution Overview

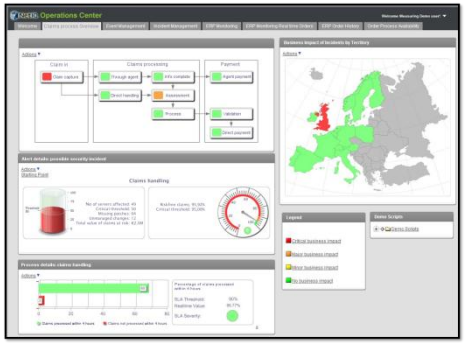
Wire Transaction Process

Understand the business process…

…and analyze its building blocks.

NetIQ Solution Design – Example

NetIQ Operations Center Dashboard



Secure Configuration Manager:

- Detecting configuration drift
- Policy compliance
- Baselining
- Exception management
- Patch Assessment

Change Guardian:

- Highly enriched audit trails
- Change detection and alerting
- Privileged user monitoring

Other NetIQ Solutions:

- Identity Manager
- Access Manager
- Access Governance Suite
- Privileged User Manager

Secure Configuration Manager

Change Guardian

Configuration Audits

Out-of-Compliance Events

Change Events

e.g. Identity Tracking

Sentinel 7:

- Security Information and Event Management (SIEM) drives the Security Operation Center

Sentinel 7

Integration

Integration

Integration

Events

3rd Party Security Solutions

- IDS-Intrusion Detection Systems
- DLP-Data Leakage Prevention

3rd Party IT Solutions

- System Monitoring / Management
- CMDB
- Etc.

NetIQ

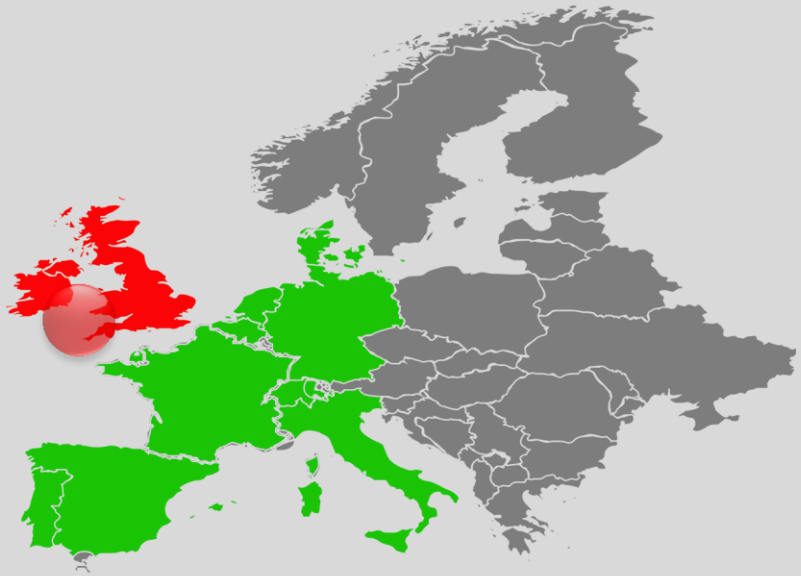
Wire Transaction Process Dashboard

NetIQ

PROCESS

Transaction request → Transaction approval → Wire transfer

GEOGRAPHY



THREAT LEVEL

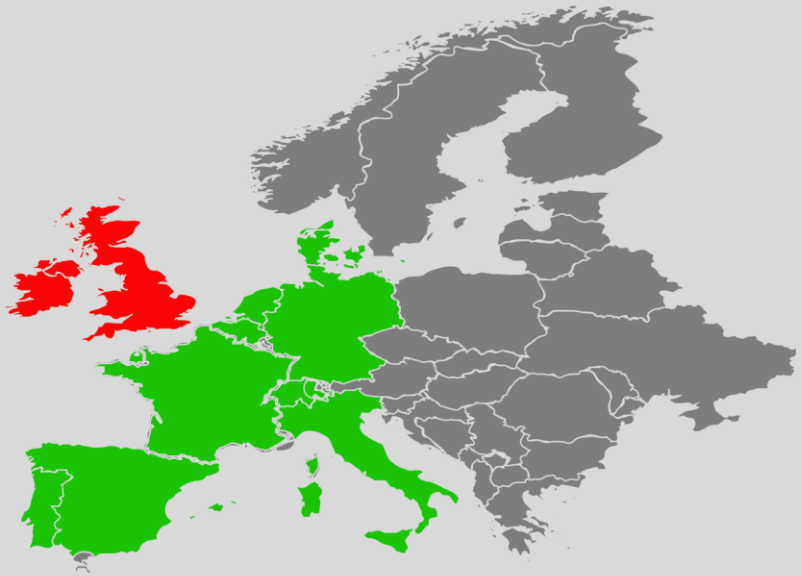
Wire Transaction Process Dashboard

NetIQ

PROCESS

Transaction request → Transaction approval → Wire transfer

GEOGRAPHY



CRITICAL ALERT

Security Incident Detected

SUMMARY

Abnormal behavior (File System)

Abnormal behavior (Remote Access)

Abnormal behavior (Transaction Approval Workflow)

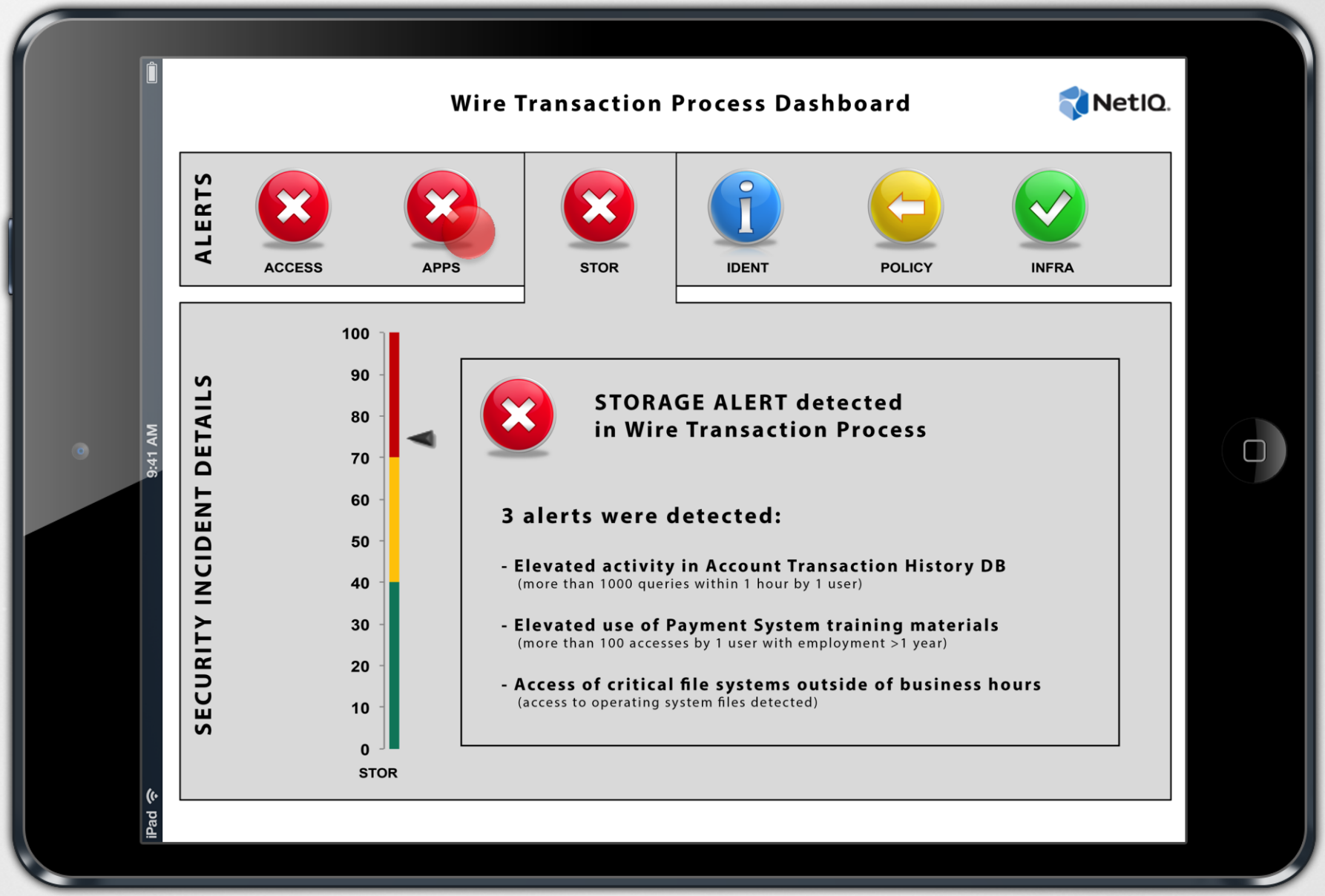
DETAILS

9:41 AM

iPad


Wire Transaction Process Dashboard
NetIQ
ALERTS
ACCESS
APPS
STOR
IDENT
POLICY
INFRA
SECURITY INCIDENT DETAILS
100
90
80
70
60
50
40
30
20
10
0
ACCESS
APPS
STOR
IDENT
POLICY
INFRA
9:41 AM
iPad


Wire Transaction Process Dashboard
NetIQ
ALERTS
ACCESS
APPS
STOR
IDENT
POLICY
INFRA
SECURITY INCIDENT DETAILS
100
90
80
70
60
50
40
30
20
10
0
POLICY
POLICY VIOLATIONS detected
in Wire Transaction Process
3 policy violations were detected:
- Unauthorized use of Internet on Restricted Computer
(Wire Tranfer Computers must not be used for Internet access)
- Unauthorized Use of Email on Restricted Computer
(Wire Transfer Computers must not be used for Email access)
- USB Token not Removed after Wire Transaction
(Wire Transfer Access Token must be removed after use)
9:41 AM
iPad


Wire Transaction Process Dashboard
NetIQ
ALERTS
ACCESS
APPS
STOR
IDENT
POLICY
INFRA
SECURITY INCIDENT DETAILS
100
90
80
70
60
50
40
30
20
10
0
STOR
STORAGE ALERT detected
in Wire Transaction Process
3 alerts were detected:
- Elevated activity in Account Transaction History DB
(more than 1000 queries within 1 hour by 1 user)
- Elevated use of Payment System training materials
(more than 100 accesses by 1 user with employment >1 year)
- Access of critical file systems outside of business hours
(access to operating system files detected)
9:41 AM
iPad

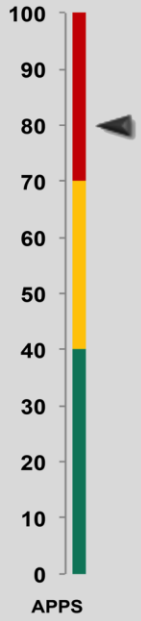
Wire Transaction Process Dashboard

NetIQ

ALERTS

ACCESS | APPS | STOR | IDENT | POLICY | INFRA

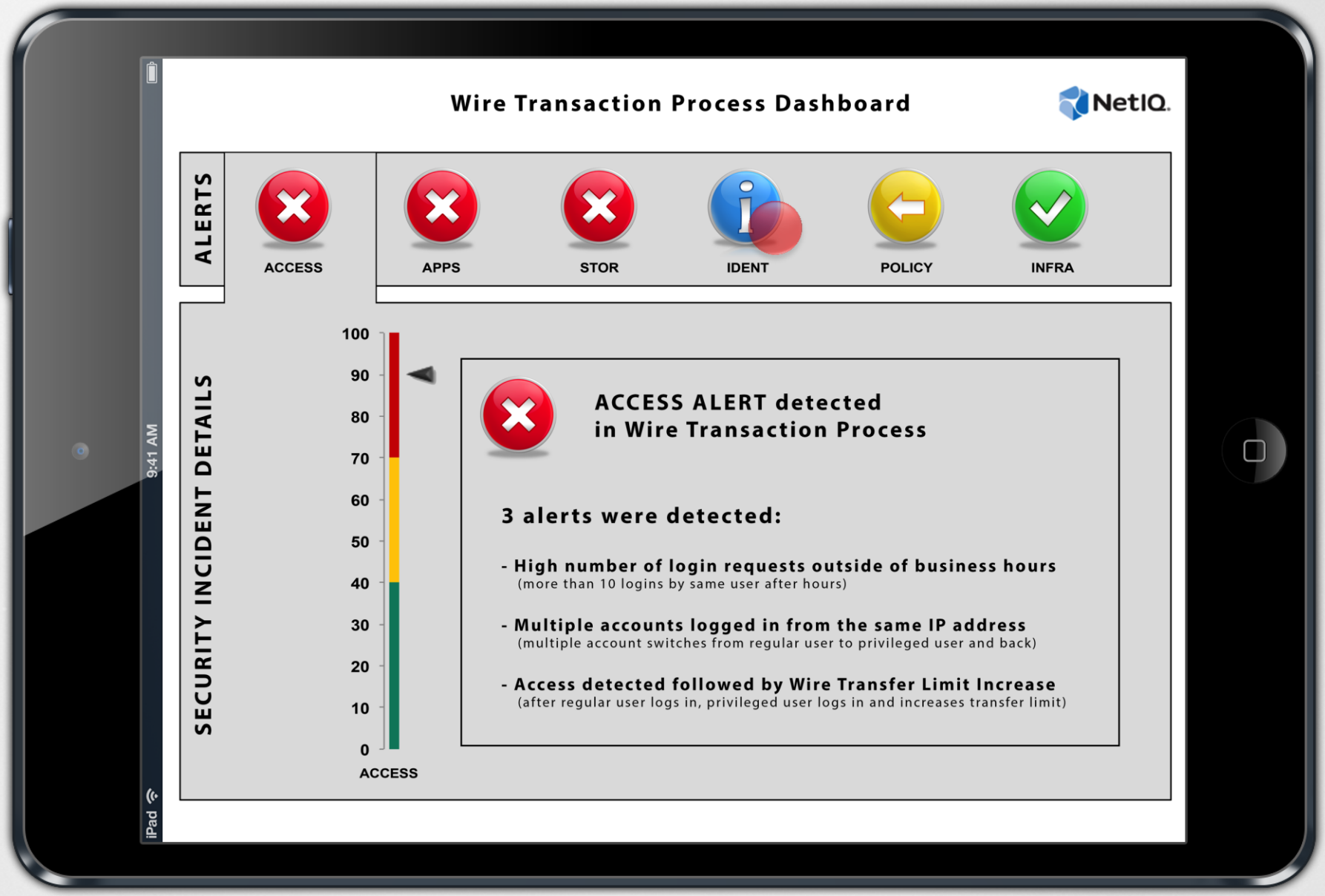
SECURITY INCIDENT DETAILS

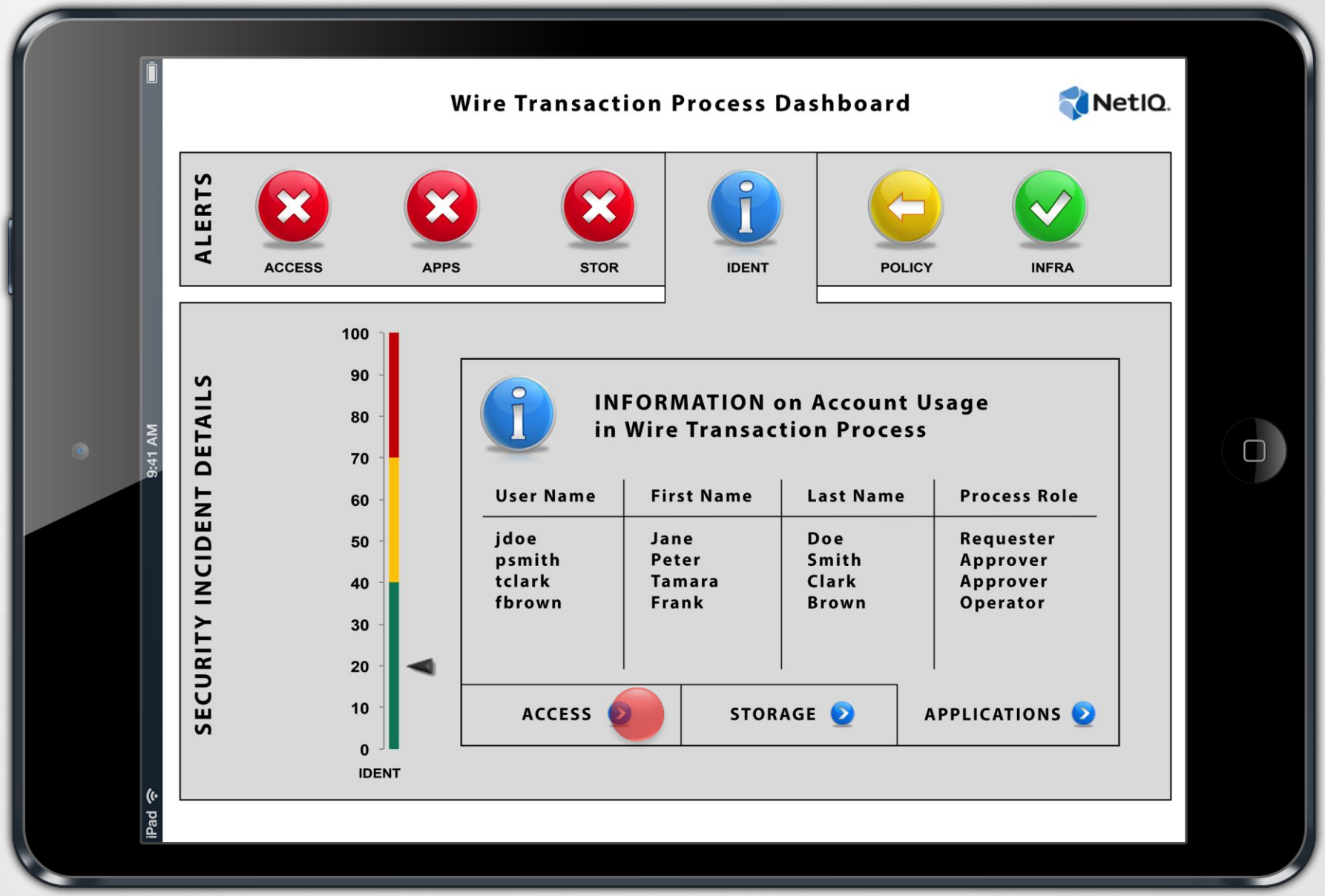


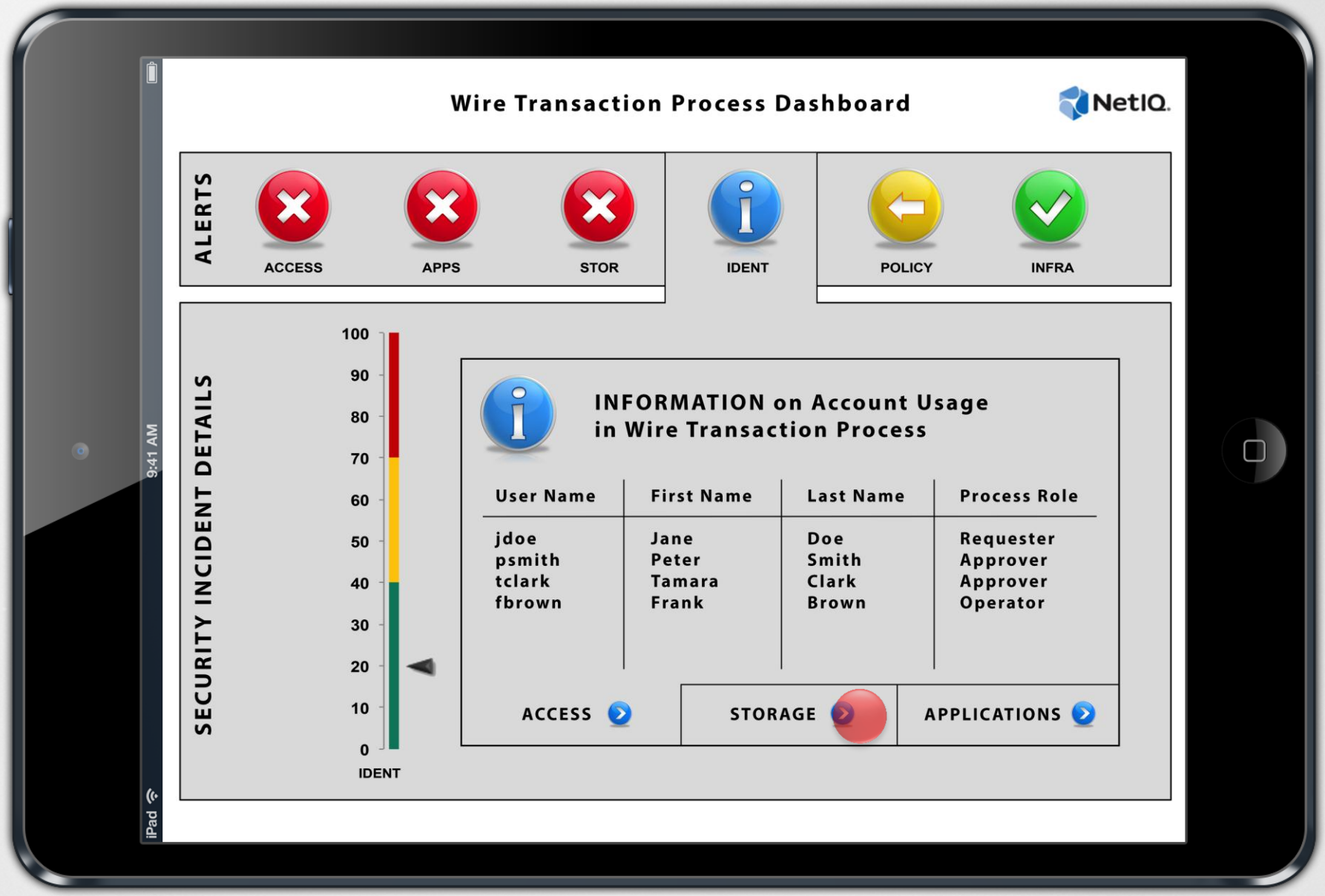
APPLICATIONS ALERT detected in Wire Transaction Process

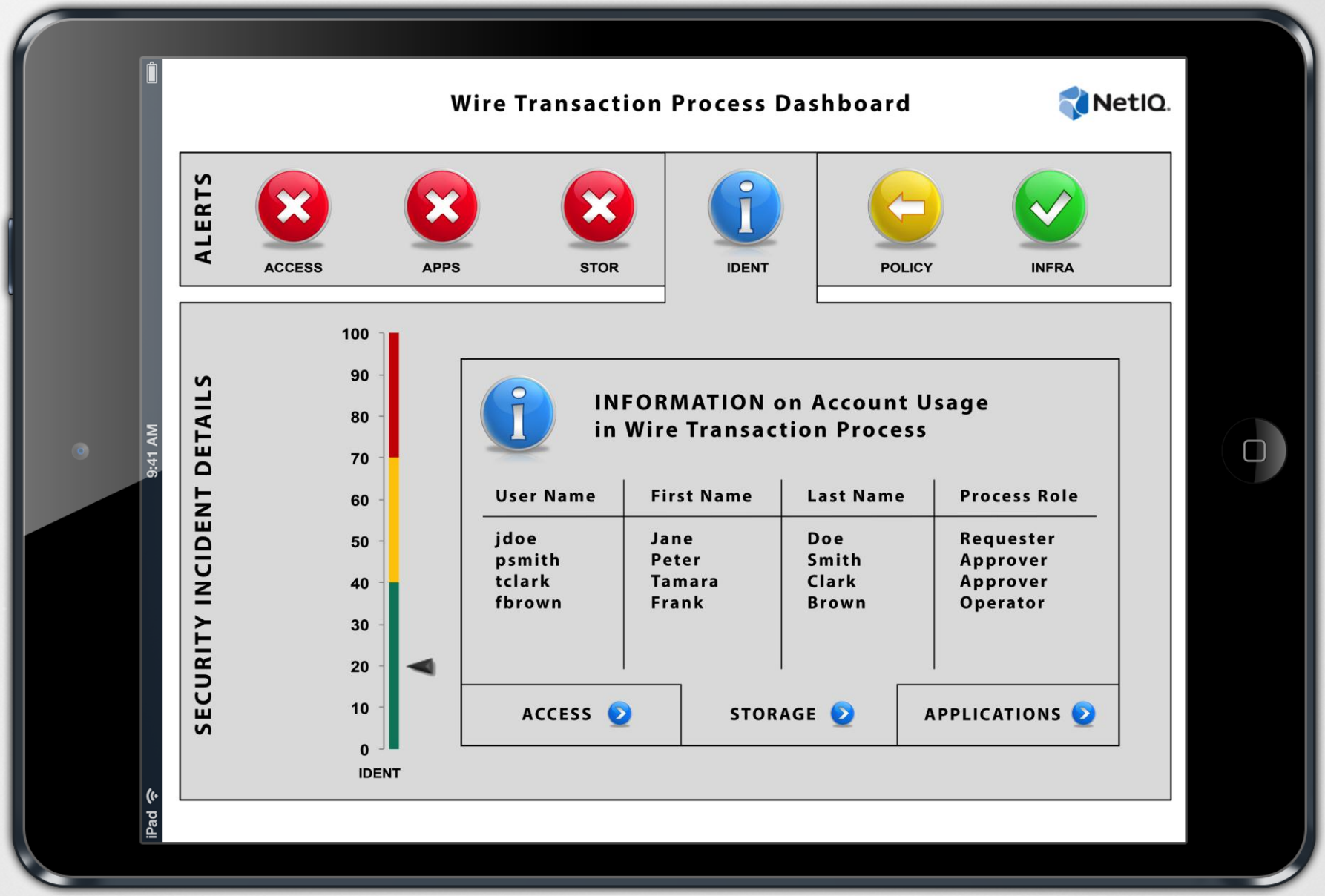
3 alerts were detected:

- **Elevated activity outside of normal business hours**
  (number of accesses increased by 200% compared to normal (baseline))
- **High number of balance inquiries within 1 hour**
  (more than 1000 accesses to account balances within 1 hour detected)
- **Deviations in the approval process workflow**
  (seggregation of duty violations (requesters cannot be approvers))


Wire Transaction Process Dashboard
NetIQ
ALERTS
ACCESS
APPS
STOR
IDENT
POLICY
INFRA
SECURITY INCIDENT DETAILS
100
90
80
70
60
50
40
30
20
10
0
ACCESS
ACCESS ALERT detected
in Wire Transaction Process
3 alerts were detected:
- High number of login requests outside of business hours
(more than 10 logins by same user after hours)
- Multiple accounts logged in from the same IP address
(multiple account switches from regular user to privileged user and back)
- Access detected followed by Wire Transfer Limit Increase
(after regular user logs in, privileged user logs in and increases transfer limit)
9:41 AM
iPad


Wire Transaction Process Dashboard
NetIQ
ALERTS
ACCESS
APPS
STOR
IDENT
POLICY
INFRA
SECURITY INCIDENT DETAILS
100
90
80
70
60
50
40
30
20
10
0
IDENT
INFORMATION on Account Usage
in Wire Transaction Process
User Name
First Name
Last Name
Process Role
jdoe
psmith
tclark
fbrown
Jane
Peter
Tamara
Frank
Doe
Smith
Clark
Brown
Requester
Approver
Approver
Operator
ACCESS
STORAGE
APPLICATIONS
9:41 AM
iPad

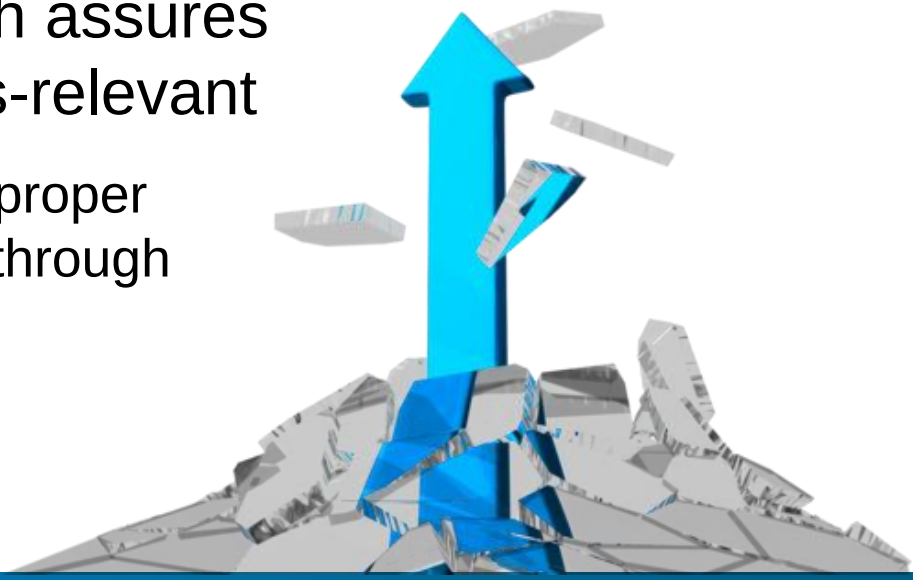

Wire Transaction Process Dashboard
NetIQ
ALERTS
ACCESS
APPS
STOR
IDENT
POLICY
INFRA
SECURITY INCIDENT DETAILS
100
90
80
70
60
50
40
30
20
10
0
IDENT
INFORMATION on Account Usage
in Wire Transaction Process
User Name
First Name
Last Name
Process Role
jdoe
psmith
tclark
fbrown
Jane
Peter
Tamara
Frank
Doe
Smith
Clark
Brown
Requester
Approver
Approver
Operator
ACCESS
STORAGE
APPLICATIONS
9:41 AM
iPad


Wire Transaction Process Dashboard
NetIQ
ALERTS
ACCESS
APPS
STOR
IDENT
POLICY
INFRA
SECURITY INCIDENT DETAILS
100
90
80
70
60
50
40
30
20
10
0
IDENT
INFORMATION on Account Usage
in Wire Transaction Process
User Name
First Name
Last Name
Process Role
jdoe
psmith
tclark
fbrown
Jane
Peter
Tamara
Frank
Doe
Smith
Clark
Brown
Requester
Approver
Approver
Operator
ACCESS
STORAGE
APPLICATIONS
9:41 AM
iPad

Summary

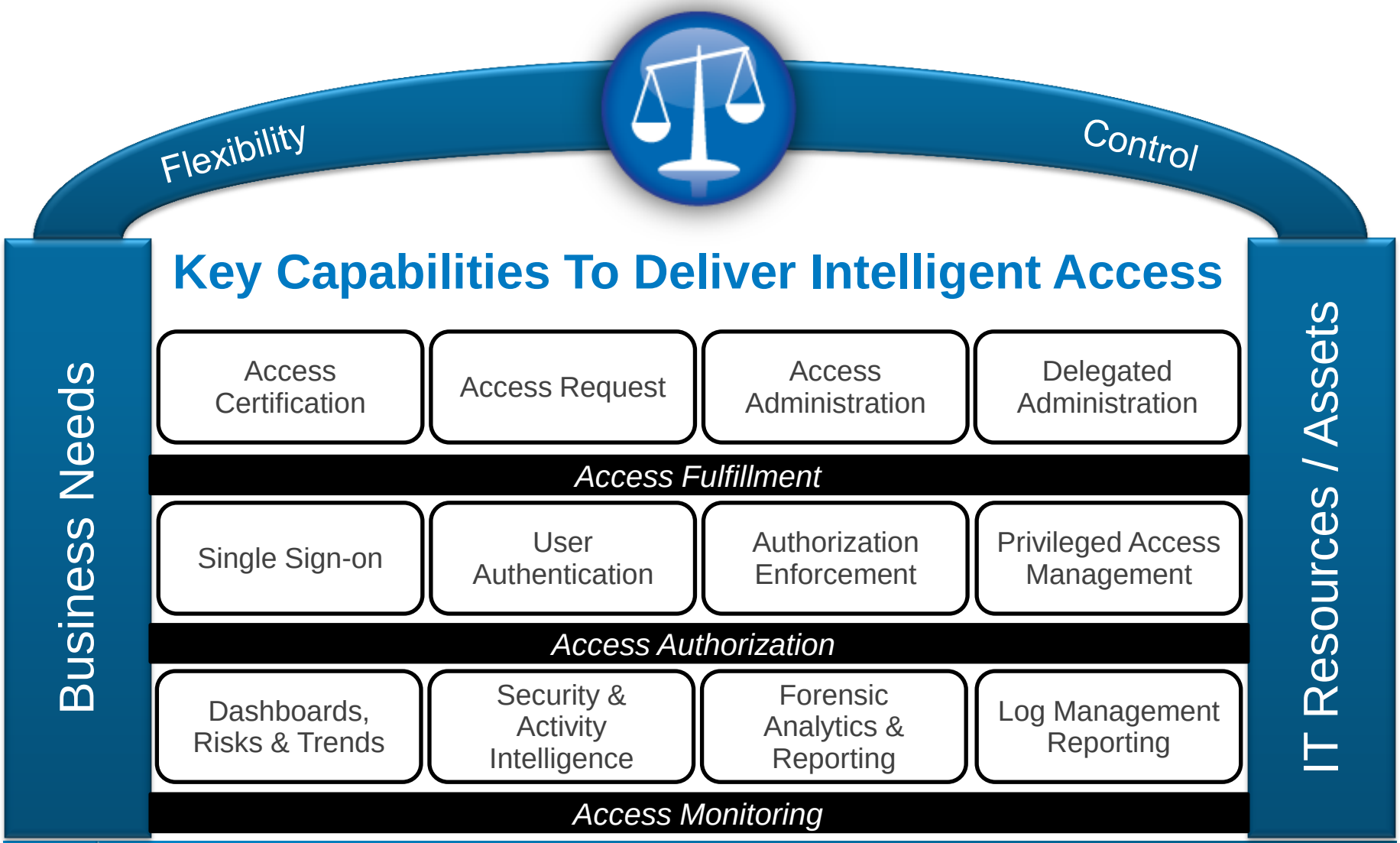
NetIQ's Approach

- Rethinking Identity and Access by viewing Security as a business process and aligning activities
- Bottom-up approaches only solve point problems, but don't show the big picture
  - One of the results of this: Security is seen as a cost center
- NetIQ's top-down approach assures that IS is seen as business-relevant
  - Result: Business alignment, proper visibility, greater awareness through executive sponsoring, etc.



What Are Your Priorities and Needs?

Access fulfillment, authorization and monitoring



So, What's Next?

Rethinking your identity, access and security

- Every organization is different – no one size fits all solution exists
  - Where do you start?
  - What is most important to you?
    - Short-term and long-term goals
- NetIQ has the answers
  - Leader in Identity, Access, Governance, and Security
  - This is just the first conversation
    - We would love to continue the discussion

For More Information

- NetIQ Website
  - www.netiq.com
- Local NetIQ Contact

White Papers

Any Questions?

Jörn Dierks
jdierks@netiq.com

Thank you.

Worldwide Headquarters
1233 West Loop South
Suite 810
Houston, TX 77027 USA

+1 713.548.1700 (Worldwide)
888.323.6768 (Toll-free)
info@netiq.com
NetIQ.com

http://community.netiq.com

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. NetIQ Corporation may make improvements in or changes to the software described in this document at any time.