Winning the Battle Against Internet Banking Fraud

Leveraging *HP Shadowbase Streams* for Real-time Data and Application Integration

2015 GTUG Conference & Exhibition

Paul J. Holenstein, Executive Vice President
Shadowbase Products Group, Gravic, Inc.

Introduction

Paul J. Holenstein
Executive Vice President
Shadowbase Products Group
Gravic, Inc.

2

Agenda

- The Problem of Internet Banking Fraud
- An Internet Banking Fraud Prevention System
- About HP Shadowbase Data Replication:
  - HP Shadowbase Streams
- Summary

Questions? Please ask as we go along…

The Problem

Internet Banking Fraud is Rampant

- **We've all seen this type of fraudulent email:**

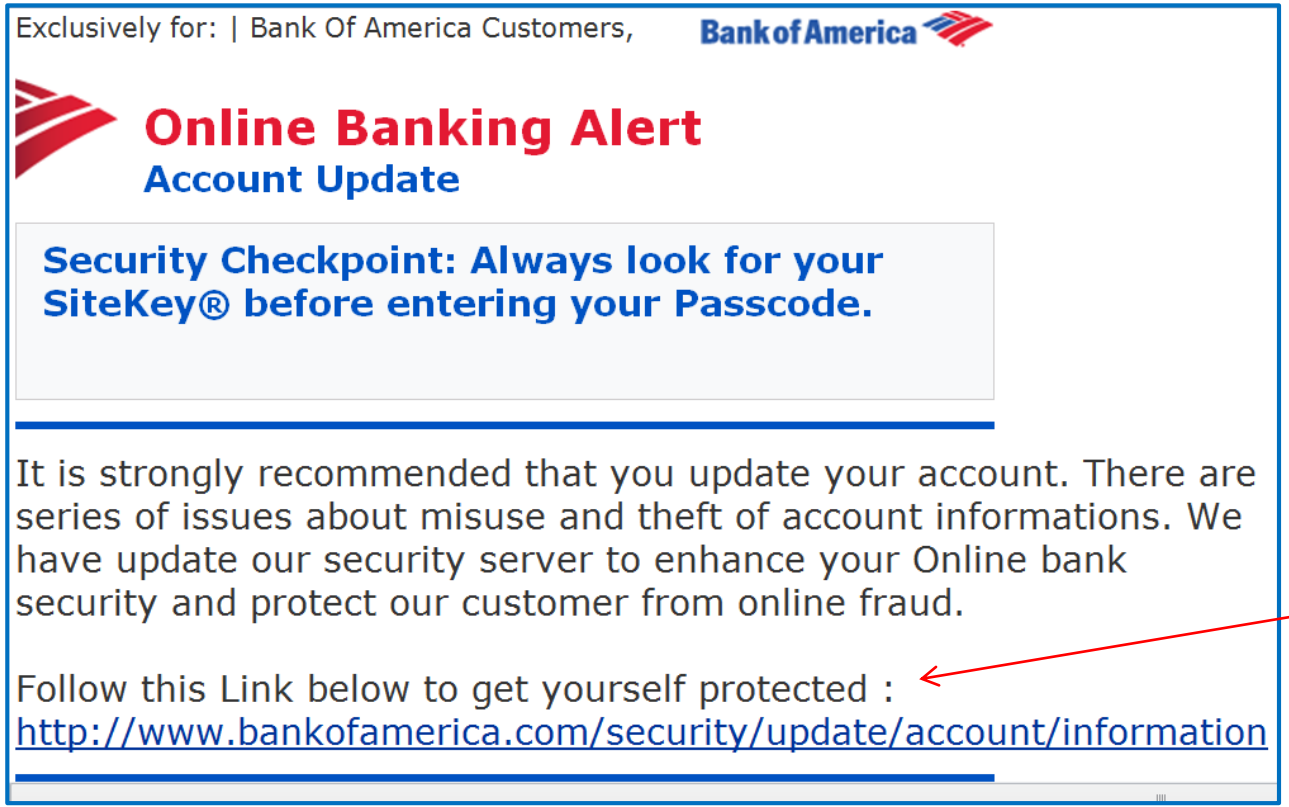
  Due to suspicious activity your bank account has been frozen.

  Click <here> to reset your account.

  – Clicking takes you to a bogus web site which captures your personal information (account numbers, user IDs, passwords, etc.)
- **Thieves obtain personal information to access your Internet bank account and steal money**
  – Email phishing, phone calls from alleged bank agents, computer viruses, etc.
- **Such information is also available for sale on the *Underground Internet***
  – Cybersecurity firm Hold Security found 360 million stolen accounts' information available for purchase
- **Internet banking fraud business is very lucrative**
  – Globally, the cost is measured in tens of billions of dollars annually
  – In the UK alone, the estimated cost for the first 6 months of 2014 was £29.3M*

* Source: Financial Fraud Action UK

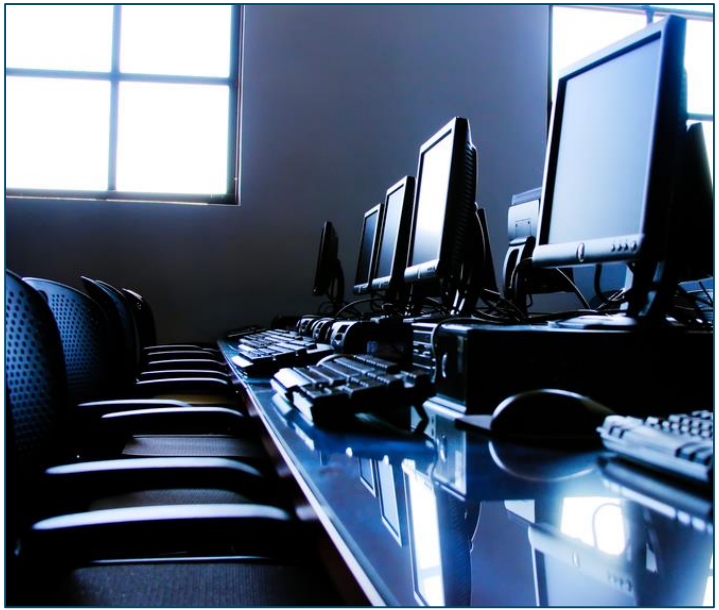
Typical Phishing Email



This Web Site link looks OK but is bogus…

The Problem

- **What is a bank to do to defend itself – and us – when the means to defraud are easily obtained?**
  - Prevent the fraud itself?
  - Facilitate identification and prosecution of the perpetrators so they cannot defraud again?
- **These two goals were achieved by a major European retail bank, using a combination of:**
  - Clever application design with
  - ***HP Shadowbase Streams*** change data capture (CDC) technology



Impact of Local Laws on Fraud Prevention System Design

Fraud Laws are Very Specific in the Bank's Home Country

- **An *intent* to commit fraud is *not* a criminal offence**
- **An *act* of fraud *is* a criminal offense**
- **For example, stealing user account information, and using it to log into the account, demonstrates an intent to commit fraud, but is not a criminal act of fraud**
  - However, using that access to transfer the customer's money to another account, *is* a criminal act
- **To enable prosecution, the bank's fraud-prevention system has to allow progress of the fraudulent activity up to the act of fraud being committed**
  - For example, denying a suspicious log in – while protecting the customer and the bank – would not provide sufficient grounds for prosecution, since no *act* of fraud was committed

Internet Banking Fraud Prevention System

Fraud Prevention Application Architecture Overview

- **Bank's Internet banking application runs on HP NonStop servers**
- **HP Shadowbase Streams uses Change Data Capture (CDC) to read the application updates to the banking database (SQL/MP) from the TMF audit trail**
  - The updates are fed via a TCP/IP connection to Shadowbase running on a Linux server
  - Customized user exit procedures running inside Shadowbase converts the updates on the Linux server into an architected message format (similar to a CSV format), and forwards them via another TCP/IP connection to a RiskShield* fraud detection application
- **The RiskShield application contains a knowledgebase to detect and flag potentially fraudulent transactions**
  - Examples: user IDs whose credentials are known to be compromised, known target accounts for fraudulent money transfers, successive transfers from different accounts to the same account, etc.
- **The RiskShield application returns a response to the Internet banking application via a private connection, indicating whether or not the transaction is *suspicious***
- **The Internet banking application then proceeds accordingly**

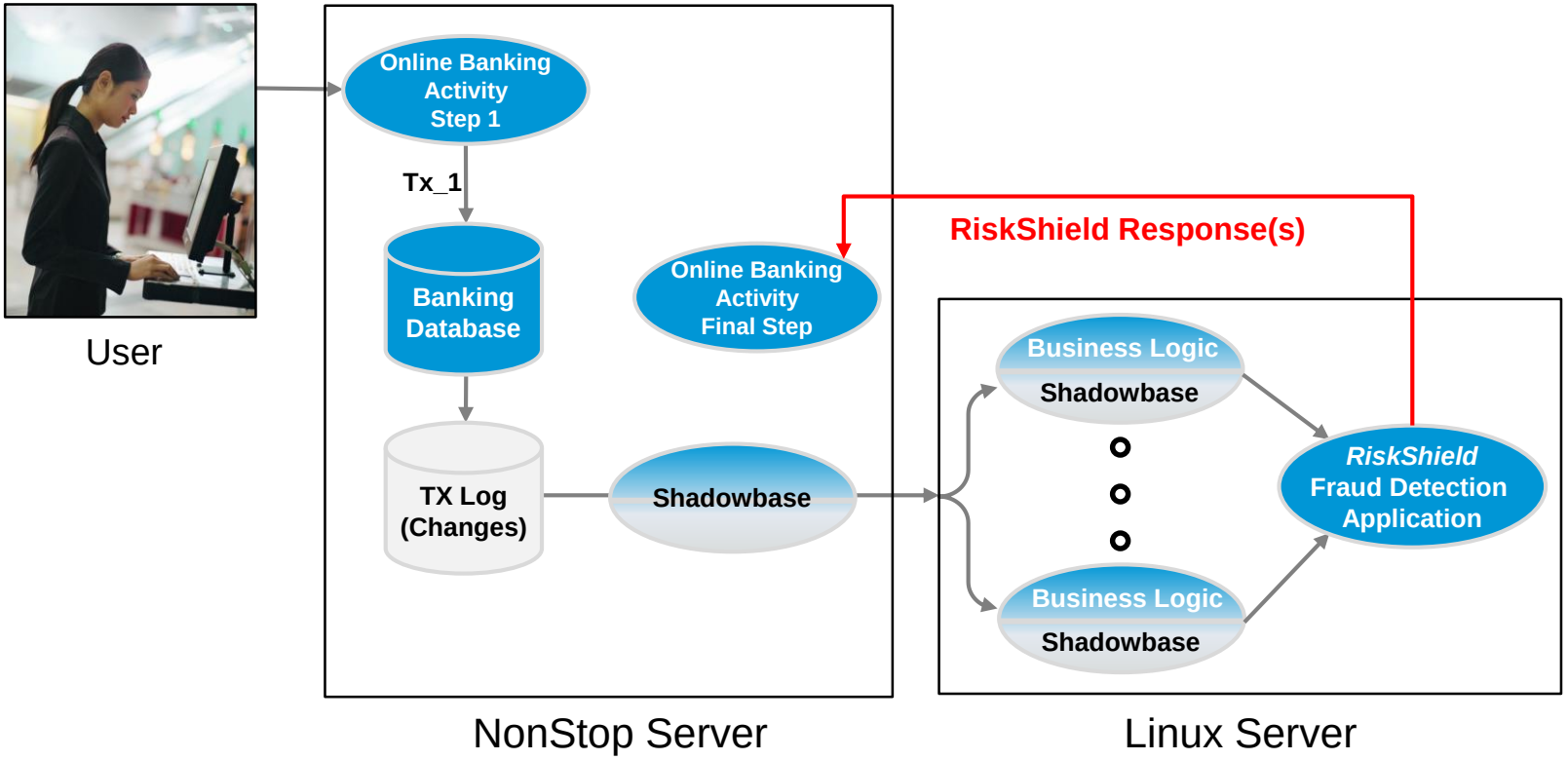
*www.informationrm-software.com/products/riskshield/

Killing Two Birds With One Stone

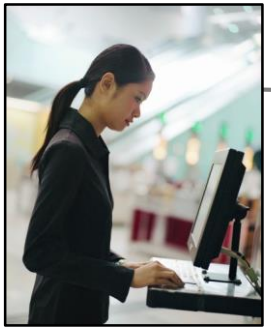
Preventing Fraud *and* Enabling Prosecution

- **When a criminal tries to transfer money from another account to his own account, the user authentication process is initiated**
  - User ID and password is captured by the banking app and logged in its database via a TMF transaction
  - Shadowbase Streams reads this info from the TMF audit trail and quickly delivers it to RiskShield
  - Bank allows the activity to proceed *since an actual criminal act has not yet been committed*
- **Each action is logged, and forwarded to the RiskShield application for further analysis via Shadowbase Streams**
- **The criminal is presented with a confirmation screen and is asked to click "Execute Transfer" which initiates the final transfer (and TMF transaction)**
  - If the RiskShield application indicates the activity is suspicious, the final TMF transaction is aborted, the money transfer is not performed, and the fraud is prevented
  - The bank notifies the account holder that his credentials were compromised, and suspends the account
  - Since an *actual* crime was committed, the bank contacts the authorities, who can investigate and possibly prosecute the perpetrators

Internet Banking Fraud Prevention System



Internet Banking Fraud Prevention System



User

Online Banking Activity Step 1

Online Banking Activity Step 2

Tx_2

Banking Database

Online Banking Activity Final Step

TX Log (Changes)

Shadowbase

NonStop Server

RiskShield Response(s)

Business Logic

Shadowbase

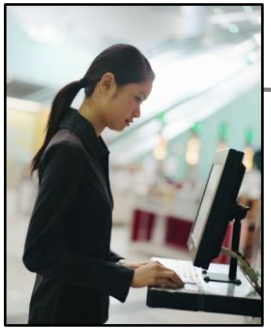
Business Logic

Shadowbase

RiskShield Fraud Detection Application

Linux Server

Internet Banking Fraud Prevention System



User

Online Banking Activity Step 1

Online Banking Activity Step 2

Online Banking Activity Final Step

Tx Final

Banking Database

TX Log (Changes)

Shadowbase

NonStop Server

RiskShield Response(s)

Business Logic

Shadowbase

Business Logic

Shadowbase

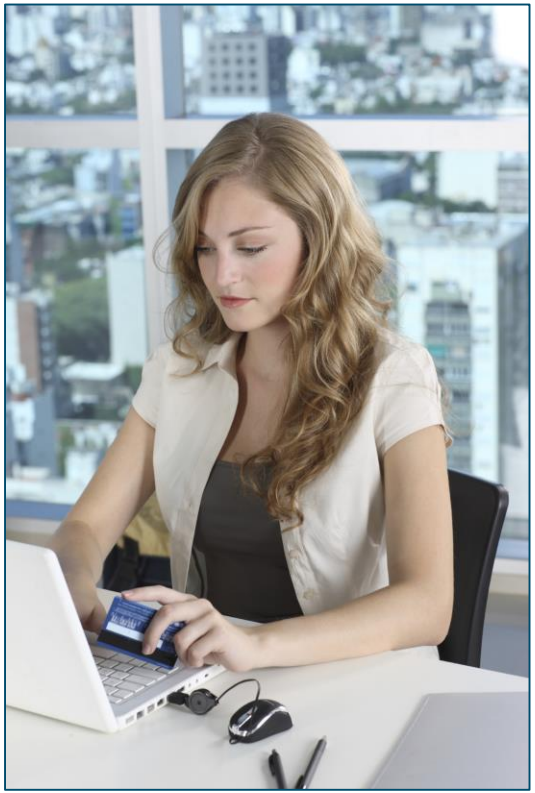
RiskShield Fraud Detection Application

Linux Server

But First, Do No Harm

Minimizing Impact of Fraud Detection on Legitimate Banking Activities

- **Fraudulent transactions are a very small subset of online banking activity**
  - most transactions are legitimate
- **Bank is optimized for non-fraudulent banking processing so that fraud prevention does not impact normal services**
  - Usually, the RiskShield response is received before the money transfer is completed
  - However, the money transfer completes even if the response from the RiskShield application is *not* received by the final step
  - Necessary steps are taken retroactively if the RiskShield response indicates possible fraud



Big Data Analytics

This Application Comprises:

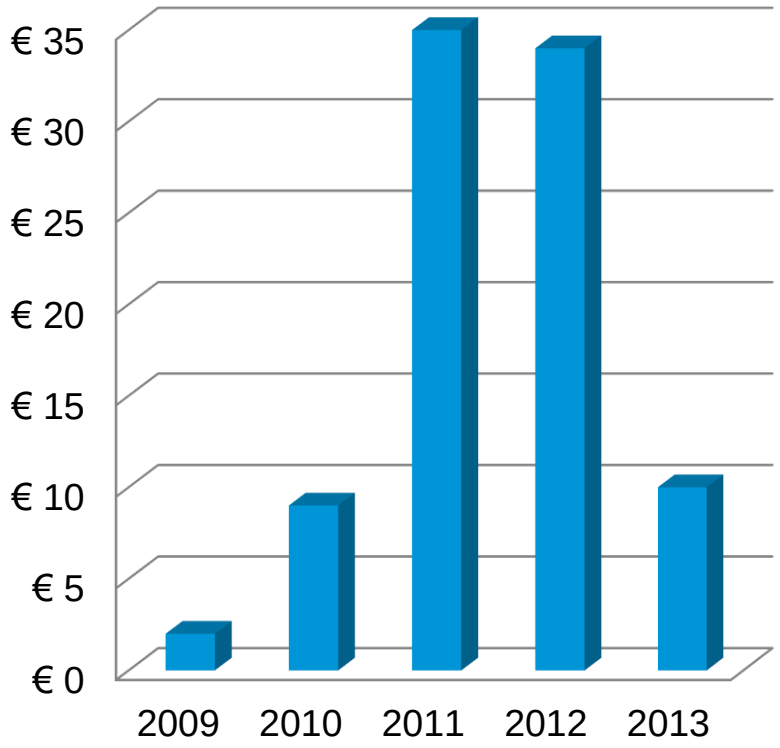
- **Big Data Analytics,**
- **Application Integration, and**
- **Real-time Business Intelligence (RTBI)**

- Can be as many as 5,000-6,000 transactions per second moving through this system
- Requires the reading and distribution of a very large amount of data by Shadowbase Streams, between heterogeneous applications (running on HP NonStop and Linux systems)
- Analysis of all data by the RiskShield application
- All done in real-time, with the addition of minimal latency and overhead

The System is Working!

Cost of Internet Banking Fraud is Decreasing in the Bank's Home Country

- **Between 2009 – 2011 the cost increased exponentially each year**
  - Peak of €35M in 2011
- **Between 2011 – 2013 the cost of fraud decreased significantly, as more fraud prevention systems are deployed**
  - Dropped by 72% between 2012 – 2013
  - Down to €10M in 2013



*Cost of Internet Banking Fraud in Bank's Home Country (€M)**

* Source: NVB, 2013

The HP Shadowbase Product Suite & HP Shadowbase Streams

HP Shadowbase Product Suite Overview

The Shadowbase Extensible Architecture

Business Continuity and Application Availability Environments

- Active/passive disaster recovery
- Sizzling-hot-takeover (SZT)
- Active/active continuous availability
- Eliminate planned downtime for migrations and upgrades (ZDM)

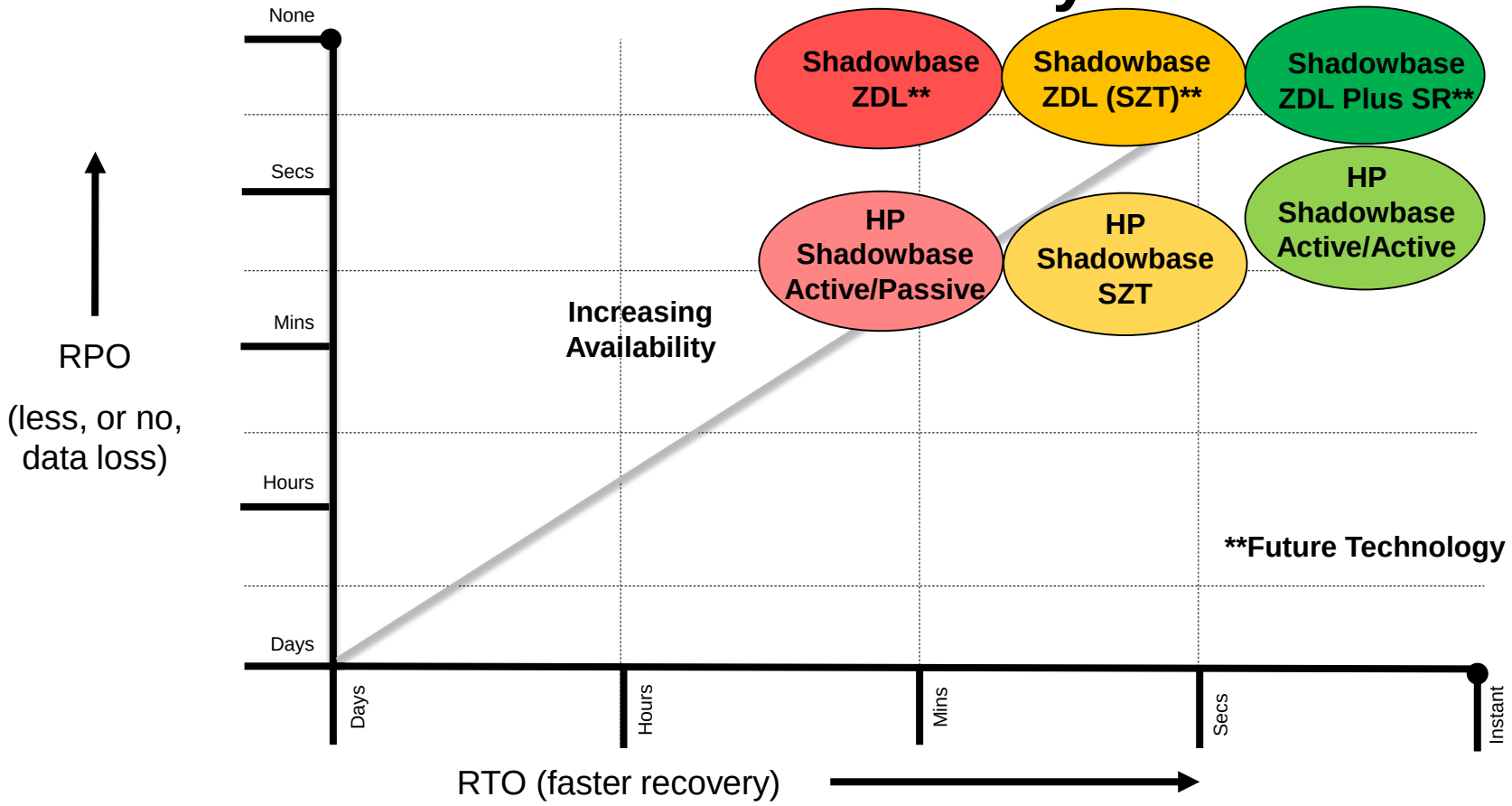
Data Integration and Data Synchronization

- Homogenous and heterogeneous environments
- Data transformation, scrubbing, filtering and cleansing
- Extend replication capabilities with embedded application logic

Application Integration

- Build *event-driven* architectures
  - Process events as they occur; no more polling for needed data
- Build *real-time* architectures
  - Process events when they occur; no more working with “stale” data
- Integrate disparate applications with no application code changes
  - Integrate at the data-layer, avoiding costly adapters, middleware, and code changes

HP Shadowbase Business Continuity Overview



HP Shadowbase Streams for Data Integration

Shadowbase Streams Manages Data Mapping for Source to Target

- Many datatypes mapped automatically
  - For example: CHAR, VARCHAR, numerics, many dates/times, etc.
- Complex datatypes mapped via either Data Mapping scripts or the Shadowbase User Exit capability

Data Scrubbing and Cleansing

- Blank and null-fill processing, NULL mapping, date/time cleansing, etc.

Data Filtering and/or Aggregation

- Remove events being replicated based on data content
- Consolidate multiple events into one

Non-Relational to/from Relational Data Formats

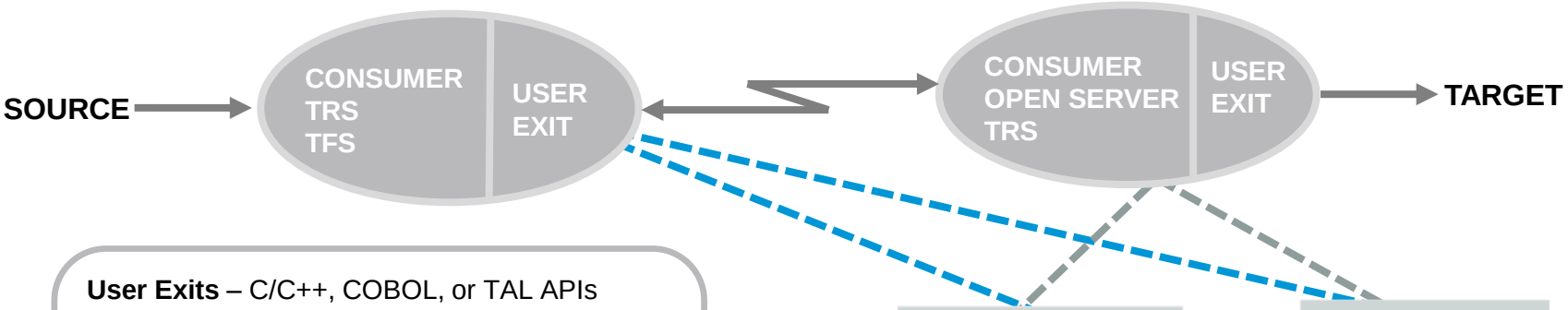
- Data normalization support provided (for redefinition support, array fan-out, etc.)
- For example NonStop Enscribe to Oracle

HP Shadowbase Streams for Data Integration

Shadowbase Streams Replication Engine

Data Transformation, Scrubbing, Filtering Capabilities

(Available on source and/or target systems)



User Exits – C/C++, COBOL, or TAL APIs

- Non-native and Native Code Supported
- Data Scrubbing and Cleansing
- Field Splits and Merges
- Aggregation and Summations
- Integrate Data from Other Databases
- Sophisticated Data Selection, Filtering and Transformation

API LIBRARY

SBGET...
SBPUT...
SBSETEXECUTE
SBSETIGNORE
etc.
NonStop & SBOS

Transformation and Mapping Facility

ASCII text file of transformation commands.
Read at start up.
SBOS Only.

HP Shadowbase Streams for Application Integration

Shadowbase Streams Enables *Event-Driven* Architectures

- SB Streams monitors the transaction log and can “trigger” on all DML or DDL database activity (e.g., inserts, updates, or deletes)
  - Avoid inefficient polling for changes

Shadowbase Streams Provides *Real-Time* Event Delivery

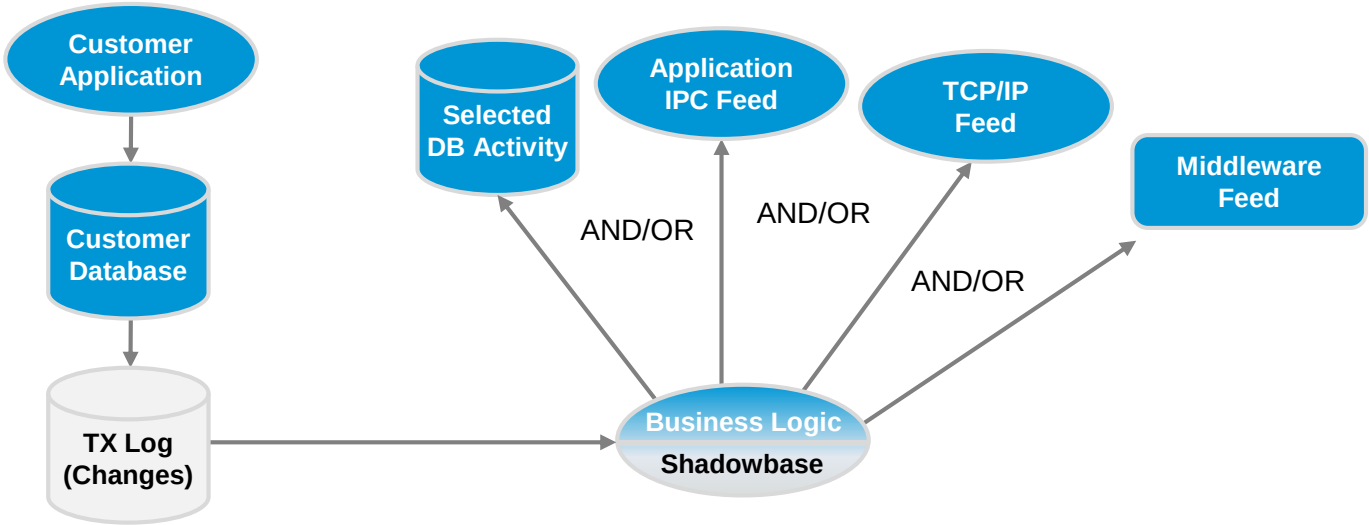
- As soon as the event occurs in the database, SB Streams sees it and can processes it
  - Avoid using “stale” data

Shadowbase Streams Integrates at the *Data Layer*

- No need to modify application code (assuming you **have** the code)
- SB Streams acts as the hub, feeding pertinent database change events to all other system(s)
- Build efficient data-driven Publish/Subscribe event-notification architectures using replication as the middleware
- Events being replicated can be delivered in any format using any supported connectivity option

HP Shadowbase Streams for Application Integration

Database Event Capture & Delivery



Function:
Shadowbase Streams "sees" all changes to the customer's database…and can act on them in real-time.

Uses:
Shadowbase Streams acts as a *capture process* for change events from the database/audit trail and notifies or delivers them to downstream files, applications, or middleware.

Summary

Winning the Battle Against Internet Banking Fraud

- **This case study provides a powerful demonstration of what can be achieved by clever application design, coupled with the HP Shadowbase Streams high-speed/high-throughput heterogeneous data distribution fabric**
  - Delivery of large amounts of data in real-time to a data analytics engine
- **System provides critical functionality and produces tangible positive results for the bank**
  - Prevents Internet banking fraud with a significant decrease in overall cost
  - Enables businesses to detect and defeat criminal activity and gain other competitive advantages
- **Consider how the benefits of HP Shadowbase Streams data and application integration could be used to competitive advantage in your company!**
  - Real-time Business Intelligence (RTBI) solutions are available here and now, thanks to HP Shadowbase Streams!

Contact Gravic or your HP account team for a free 60-day trial.

Thank you

Gravic, Inc.

17 General Warren Blvd.
Malvern, PA 19355 USA

Shadowbase@gravic.com
SBSales@gravic.com
www.gravic.com/shadowbase

Phone: +1.610.647.6250
Fax: +1.610.647.7958

Find us on…

Make it matter.