



Common Customer / User Experience

*Scalable / agile removed from applications
authentication services*

Stuart Wilson – Managing Director - Pirean

IBM Software

PCTY2010



Pulse Comes to You

Optimising the World's Infrastructure

[27 May, London]

Growing security challenges driving the need for access management

- Data Protection and Secure Collaboration
 - Growing risk of Intellectual Property Theft
 - Need to control access to critical data
- Application Security and IT Compliance
 - Increasing regulations requires secure access control (e.g. PCI, ITAR, HIPAA)
 - Need to demonstrate that only right people have access to right resources
- Service Transformation & IT Cost
 - Reducing cost of business applications and services rollout (SOA, SaaS/Cloud)
 - Need to manage and change user access control without modifying applications or web services



Rethinking RISK

Costly Impact of data and application breaches

Date 2010

Data Security Breach at Lincoln National Corp.

Revealed a data breach that could affect 1.2 million customers data. Initial forensics showed that Lincoln National and its subsidiaries were sharing usernames and passwords to access portfolio information

Source: Information Week

Date 2009

Heartland Payment Systems loses credit and debit cards

SQL injection errors that allowed hackers to break into the payment processor's network and steal data on approximately 130 million credit and debit cards.

Source: Computer World

Date 2009

Monster Database Security Breach Official Alert

Monster is the target of illegal attempts to access and extract information from its database. Our database was illegally accessed and certain contact and account data were taken including usernames, passwords, names, phone numbers.

Source: monster.com

285 Million

Compromised records from 90 confirmed cases within 2008. More in one year than 230 million records from 2004-2007

Source: 2009 Data Breach Investigations Report by Verizon Business RISK Team

81%

Of US firms lost laptops with sensitive data in the past year

Source: Poneman Institute on Privacy and Information management research

Less than 3% of data within an organization is properly classified and protected

Source: Gartner on Content awareness report

99% records

Were online assets exposed from servers and applications despite concerns over portable and mobile devices

Source: 2009 Data Breach Investigations Report by Verizon Business RISK Team

The need for a common way of doing things?

- A single, standardised approach to Application Security brings:
 - Centralised control and management;
 - Improved visibility and audit;
 - Consistent controls across applications; and
 - Reduced maintenance – security is now outside of your application.
- Which means:
 - Reduced cost;
 - Tighter security; and
 - Faster, more agile deployment of new business services.

Real world requirements

“We need to secure our on-line banking platform, we want strong security controls to manage access to multiple systems.”

“We want to roll out a new portal for schools – we want a centralised security service and single sign-on across applications.”

“We’re going through a major merger, we have lots of applications with different security systems – we want a single security layer which sits in front of these applications... We don’t have time to re-write security across applications.”



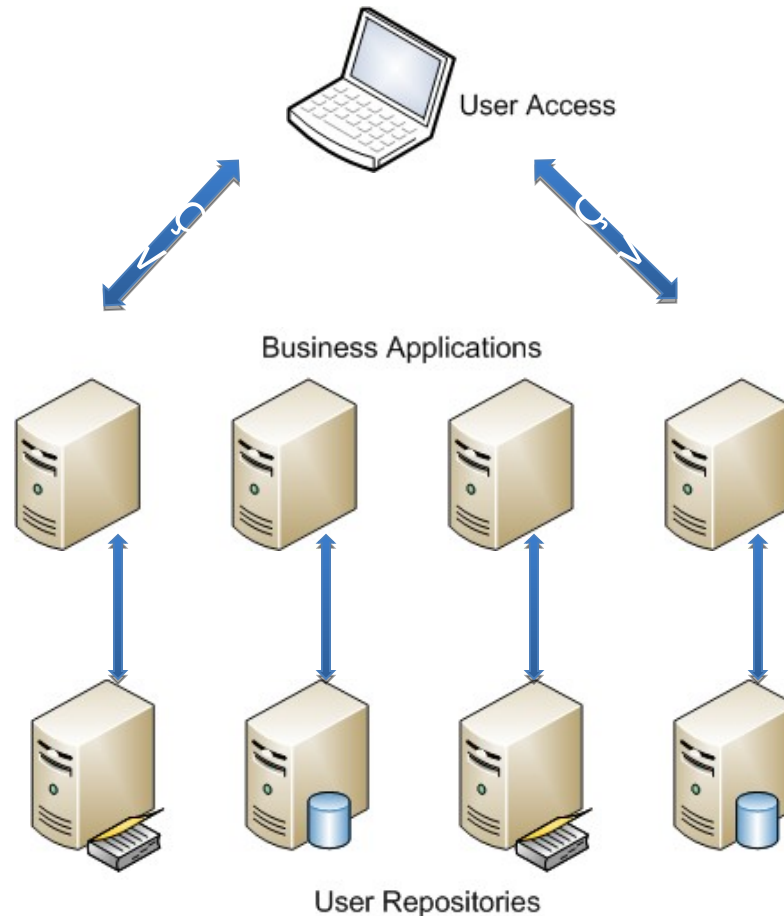
More real world requirements

“We want to revisit all of our web applications to use a single, authoritative source for customer data. We need to address a major audit point with strong authentication and we don’t have bandwidth to modify every application.”

“We want a single system to manage application access across our diverse production, test and development environments.”

“We need to be faster to market. We need a repeatable solution for strong authentication that can be implemented and tailored quickly and easily for new services.”

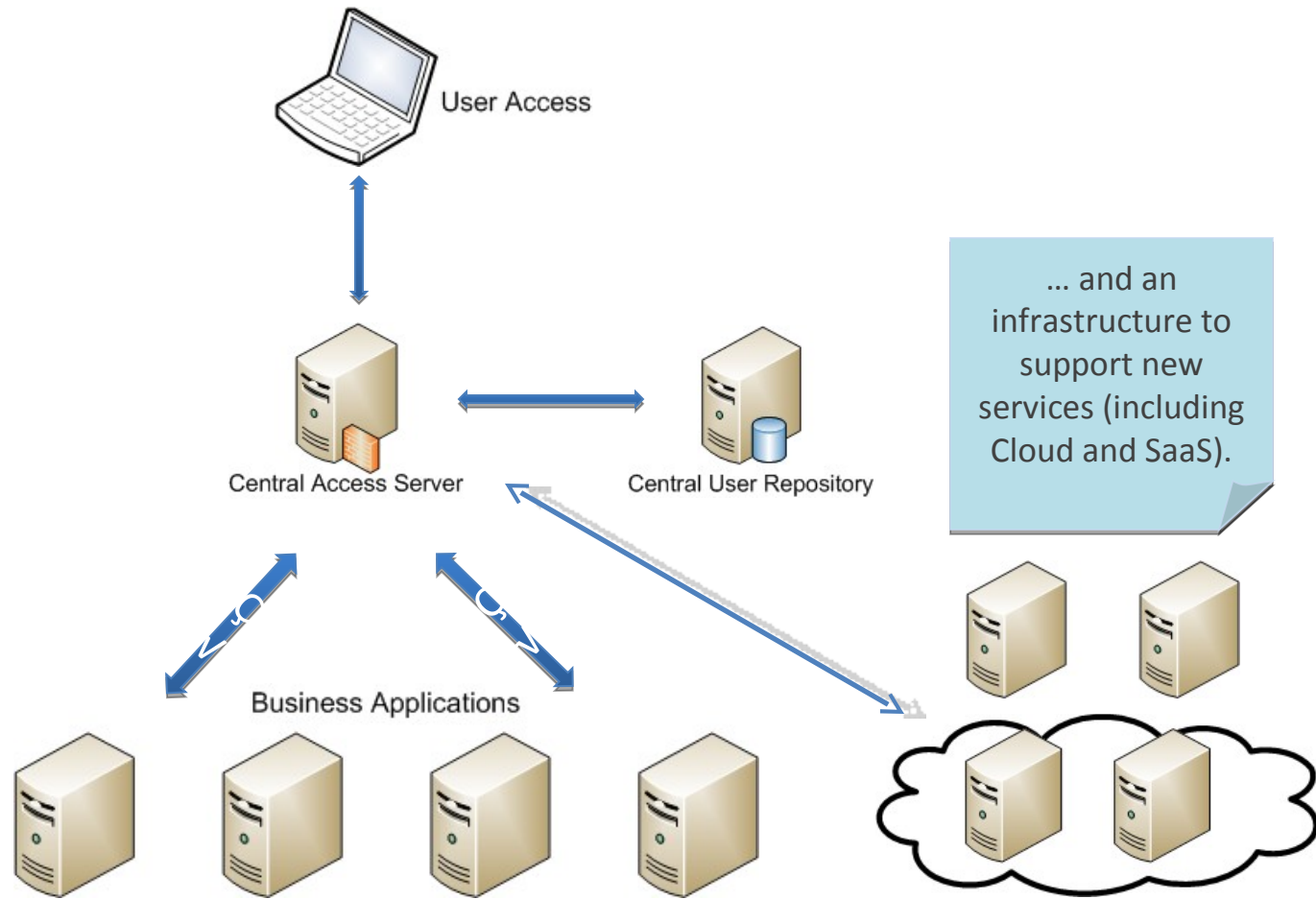
Common Architecture Model



Now consider the challenges associated with audit, maintenance and introducing new security controls...

Centralised Architecture Model

We now have simplified management, centralised maintenance, a single point of audit and control.



... and an infrastructure to support new services (including Cloud and SaaS).

We now have a common way of doing things...

- A single, standardised approach to Application Security:
 - Centralised control and management;
 - Improved visibility and audit;
 - Consistent controls across applications; and
 - Reduced maintenance – security is now outside of your application.
- Which means:
 - Reduced cost;
 - Tighter security; and
 - Faster, more agile deployment of new business services.

What are our customer's saying?

“Having to manage access and security for each application separately was proving to be extremely time consuming and negating some of the savings we had made ... Pirean delivered a solution that allows us to rein in those costs and deploy new applications quickly without generating more management overheads for the IT department.”

Bill Rafferty, development manager at City University London,

“Our work with Pirean is helping us deliver a new focus on web service that enables us to better interact with our partners and customers in an environment where security and speed to market are absolutely paramount...”

Ian Chapple, Director of IT Strategy & Architecture for Aviva UK



Thank
You