Hands on with PeopleSoft: Effective PeopleSoft Security Practices

Logesh Balasubramaniam

Presence of IT
excellence in people

Agenda

01

Security Hardening

02

New Features

03

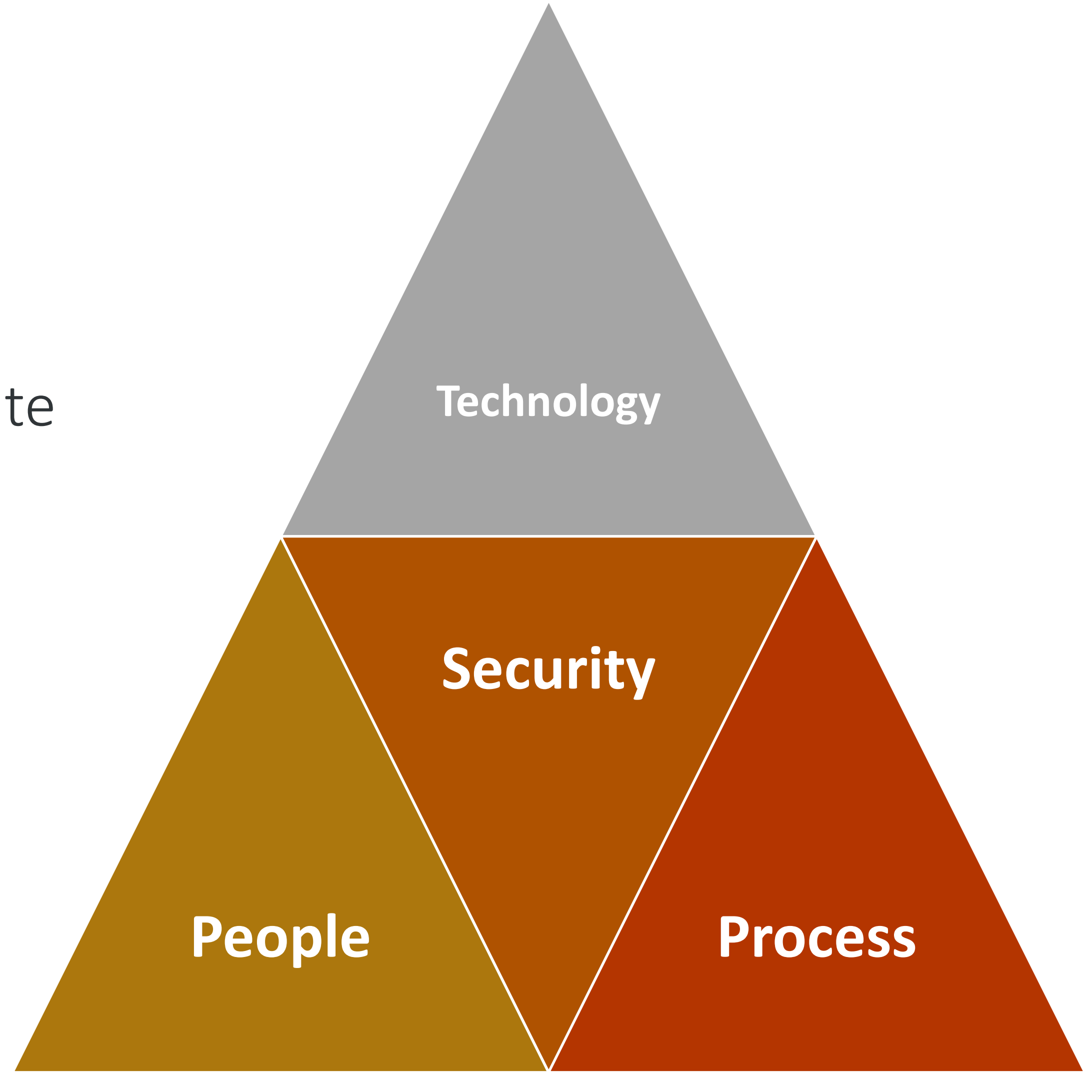
Enterprise Security Considerations

04

Cloud Security Considerations

Security - Essentials

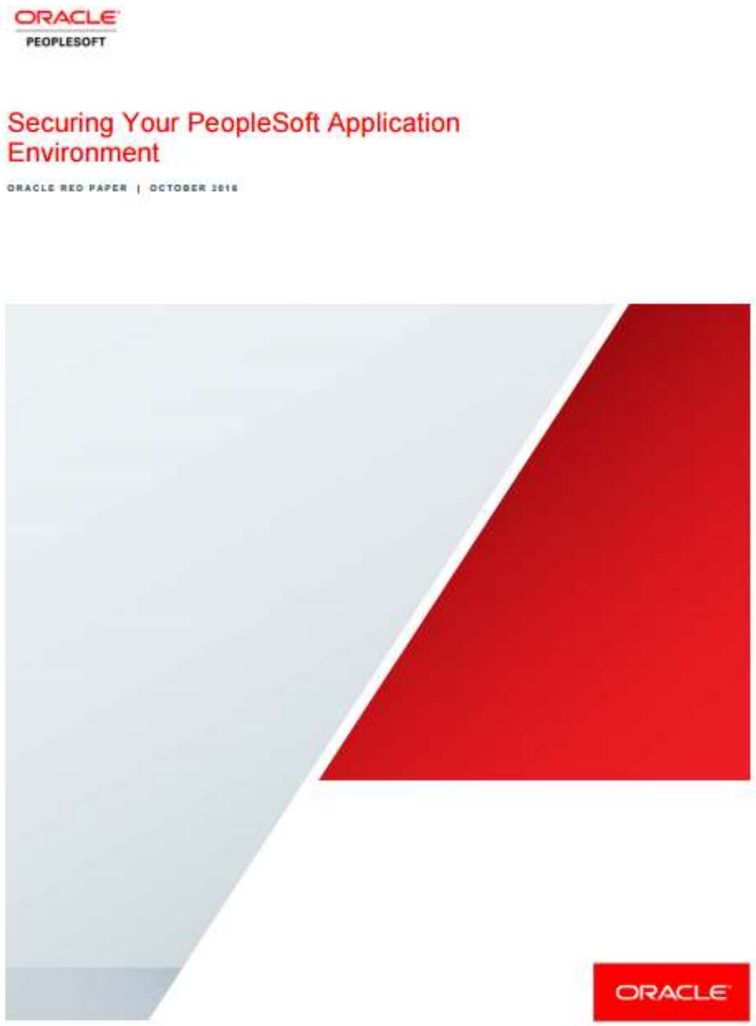
Roughly **58%** of data security breaches originate from authorized access.



Security Hardening

Red Paper on Securing PeopleSoft Application

- Red paper from Oracle available on customer support
- **Doc ID 747524.1**
- **Version 3: Updated in October 2016**



ORACLE
PEOPLESOFT

Securing Your PeopleSoft Application Environment

ORACLE RED PAPER | OCTOBER 2016

ORACLE

Hardening – Securing PeopleSoft Internet Architecture

- How to Security Harden the Web Server - WebLogic and WebSphere
- How to Enable SSL on a Web Server for HTTPS
- **How to Disable HTTP on a Web Server**
- How to Disable Configuration Re-Initialization - "AuditPWD"
- **How to Disable Browser Caching - note on "KIOSK"**
- How to Configure a Forward Proxy Server for the Portal and Integration Gateway
- Setting a Forward Proxy for WebLogic and WebSphere
- How to Bypass a Forward Proxy for Local Hosts
- How to Enable Mutual Authentication for Integration
- How to Enable LDAPS for Directory Integration
- **How to Enable TUXEDO Encryption (LLE and SSL)**
- **Useful hardening Lockdown links**

Hardening - Securing PeopleTools

- Delete or Disable Unused User IDs
- **Enable Password Controls**
- Expire Password At Next Logon
- Allow Password to be Emailed
- Review Sign-in and Time-out Security
- **Change the Access Password**
- **Change the Connect Password**
- Change the IB Gateway Properties Password
- **Review the Single Signon Configuration**
- **Use Strong Node Passwords or Use Certificates**
- **Review Signon PeopleCode and User Exits**

Hardening – Securing PeopleTools

- Limit Usage of the PeopleSoft Administrator Role
- Limit Access to Application Designer and Data Mover
- Limit Access to User Profiles, Roles, and Permission Lists
- Limit Ability to Start Application Server
- Limit Access to Weblogic Console
- Review Query Security
- **Enable SQL Error Message Suppression**
- **Track Users' Login and Logout Activity - PSACCESSLOG and PSPTLOGINAUDIT**
- Securing PS_HOME and PS_CFG_HOME
- Consider Auditing and Oracle Audit Vault

Hardening – Securing PeopleSoft Customisations

- Configure every Component for Row-Level Security
- Isolate all User-Entered Data to a Bind Variable
- Escape All User-Entered HTML
- **Turn Off Modifiable by HTML for Hidden Page Fields**
- User-Entered File Names Should Not Include Paths
- Understanding WS-Security
- **Protecting PDF files and XDO.CFG**

Security – New Features

PeopleSoft Security – New Features

- Web profile enhancements
- Implement SHA-2 (SHA-256) Certificate and Hash
- Extended Access and Connect ID DB Password Length
- Authentication for Cloud File Attachment
- Related Content - Event Mapping / Identity Validation Framework
- Other security related enhancements

PeopleTools 8.55 Security Features

Authorizing Resource Access Using Cross-Origin Resource Sharing (CORS)

- The Same-Origin Policy restricts the browser from performing certain actions by scripts or documents based on the origin.
- While it is a vital piece of web security, it also poses problems. What happens when you want to allow a site with a different origin to access your content?
- The CORS standard gives web servers cross-domain access controls, which enable secure cross-domain data transfers.
- Use the Authorized Site page to maintain sites that are authorized to request resources from this web server using the Cross-Origin Resource Sharing (CORS) standard.

HOW TO RESTRICT SITES WHICH CAN FRAME PEOPLESOFT APPLICATION CONTENT

- Setting to allow external sites to frame PeopleSoft pages
- Uses the X-FRAME-OPTIONS custom property on the Web Profile to specify which action should be taken by the browser.
- Based on the custom property setting, an HTTP response header of the same name will be included to instruct the browser on how framing should be controlled.

PeopleTools 8.55 Security Features

- SHA-256 hash with salt algorithm
- 4096 key size
    - When generating private keys for application server-based digital certificates, by default PeopleTools uses the SHA-256 with RSA encryption algorithm and the 4096 key size.
    - When using PSKeyManager to generate private keys for web server-based digital certificates, the default signing algorithm is SHA-256 with RSA encryption.
    - PS_TOKEN will continue to use SHA-1 digest. Customers will be recommended to use SHA-2 as Certificate Node Authentication
    - **New/modified PeopleCode functions**
      HashSHA256() - Hash without salt
      HashWithSalt() - Hash with salt

PeopleTools 8.55 Security Features

The maximum length for the database access ID password and for the connect ID password has been extended to 32 characters.

- Issue with 3DES and encrypting a string of 8 or fewer characters
- Intermediate solution – use Initialization Vector
- Actual solution – extend space to 32 characters
- Password in PSOPRDEFN will be SHA-2 hashed with salt
- The PSACCESSPRFL table has been replaced by the PSACCESSPROFILE table to accommodate the longer passwords.
- Enhanced login audits – PS_PT_LOGIN_AUDIT, PS_ACCESSLOG

PeopleTools 8.55 Security Features

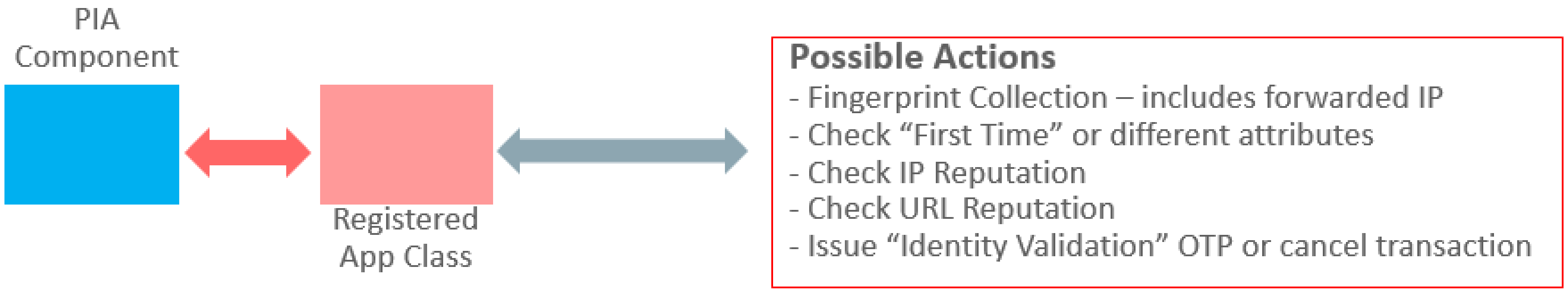
App/Web Server Encryption

- Link Level Encryption (LLE) is the default encryption for Java server listener (JSL) connections to the WebLogic Java container to the Tuxedo application server.
- LLE is being deprecated.
- While LLE is still supported, you should upgrade to SSL.

To implement SSL, see “Configuring SSL for JSL/WSL connections for Tuxedo in PeopleSoft” attached to Doc ID 1242154.1 on the Oracle support web site.

PeopleTools 8.55 Security Features

PeopleSoft Related Content Framework can also be used to map application class PeopleCode to component and component record events. This allows custom PeopleCode programs to be defined for a component without customizing the component definition.



Possible Actions

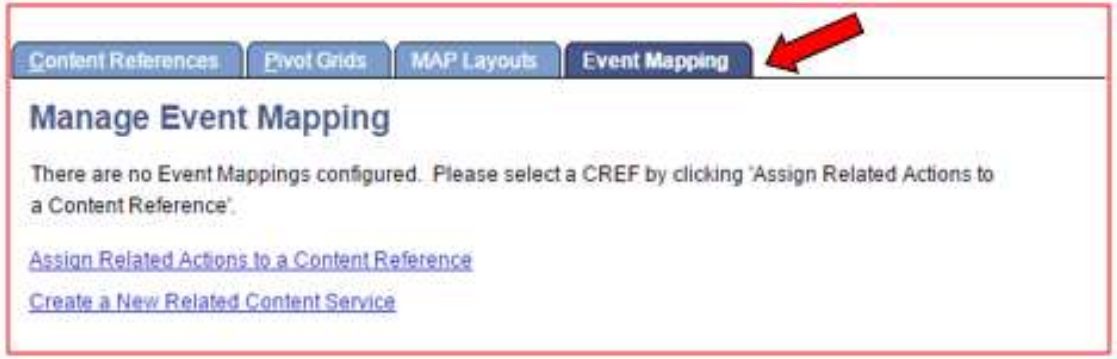
- Fingerprint Collection – includes forwarded IP
- Check “First Time” or different attributes
- Check IP Reputation
- Check URL Reputation
- Issue “Identity Validation” OTP or cancel transaction

Sample Resources:

- **Nexmo Verify** (OTP)
  https://www.nexmo.com/products/verify/
- **BrightCloud® IP Reputation Service**
  https://webroot-cms-cdn.s3.amazonaws.com/1114/5462/0565/BCSS-IPRS-DS.pdf
- **IP Location**
  https://www.iplocation.net/

PeopleTools 8.55 Security Features

There is a new Tab called “Event Mapping” under "Manage Related Content Services" page where developers can associate components and Event Mapping application classes.



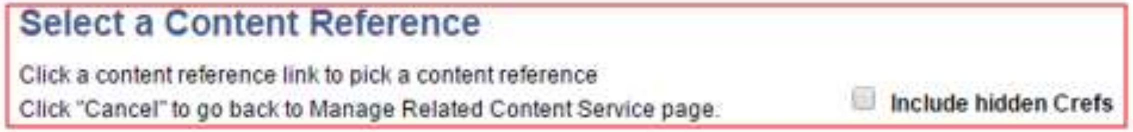
Manage Event Mapping

There are no Event Mappings configured. Please select a CREF by clicking 'Assign Related Actions to a Content Reference'.

Assign Related Actions to a Content Reference

Create a New Related Content Service

Developer chooses the Content Reference (CREF) from Select content reference page



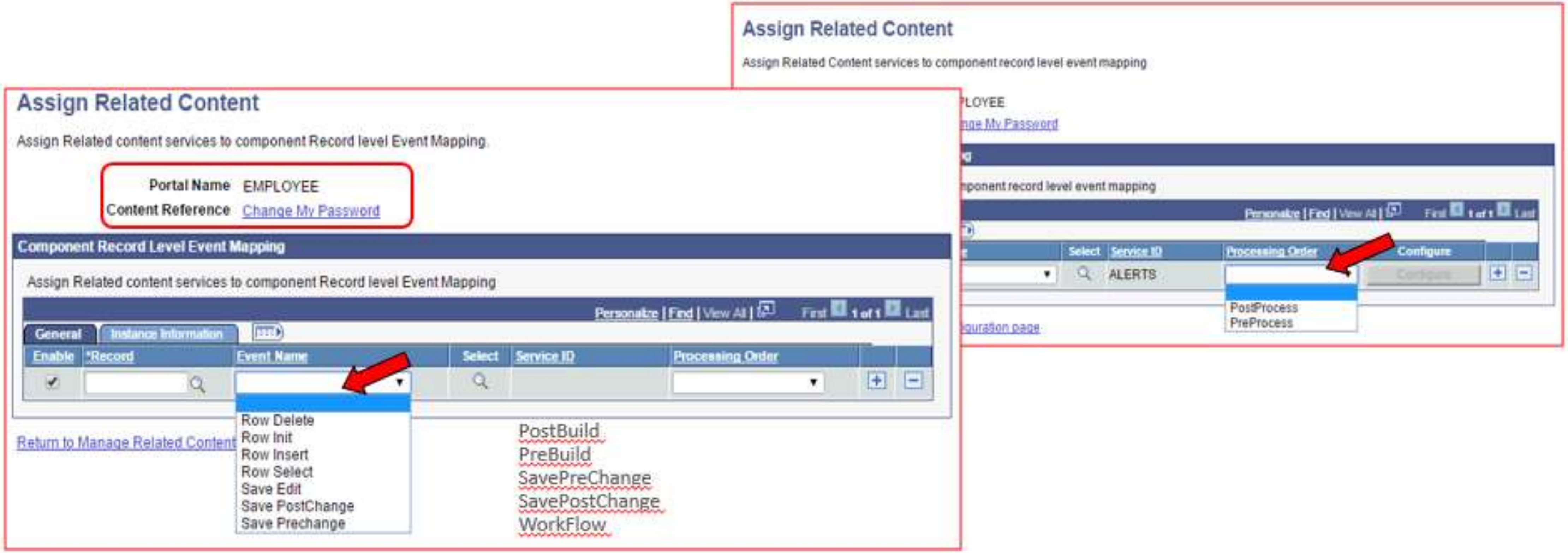
Select a Content Reference

Click a content reference link to pick a content reference
Click "Cancel" to go back to Manage Related Content Service page.

□ Include hidden Crefs

PeopleTools 8.55 Security Features

Developer chooses the event from Event name dropdown and processing order



Assign Related Content

Assign Related content services to component Record level Event Mapping.

Portal Name EMPLOYEE

Content Reference Change My Password

Component Record Level Event Mapping

Assign Related content services to component Record level Event Mapping

Return to Manage Related Content

PostBuild
PreBuild
SavePreChange
SavePostChange
WorkFlow

Assign Related Content

Assign Related Content services to component record level event mapping

PLOYEE

nge My Password

mponent record level event mapping

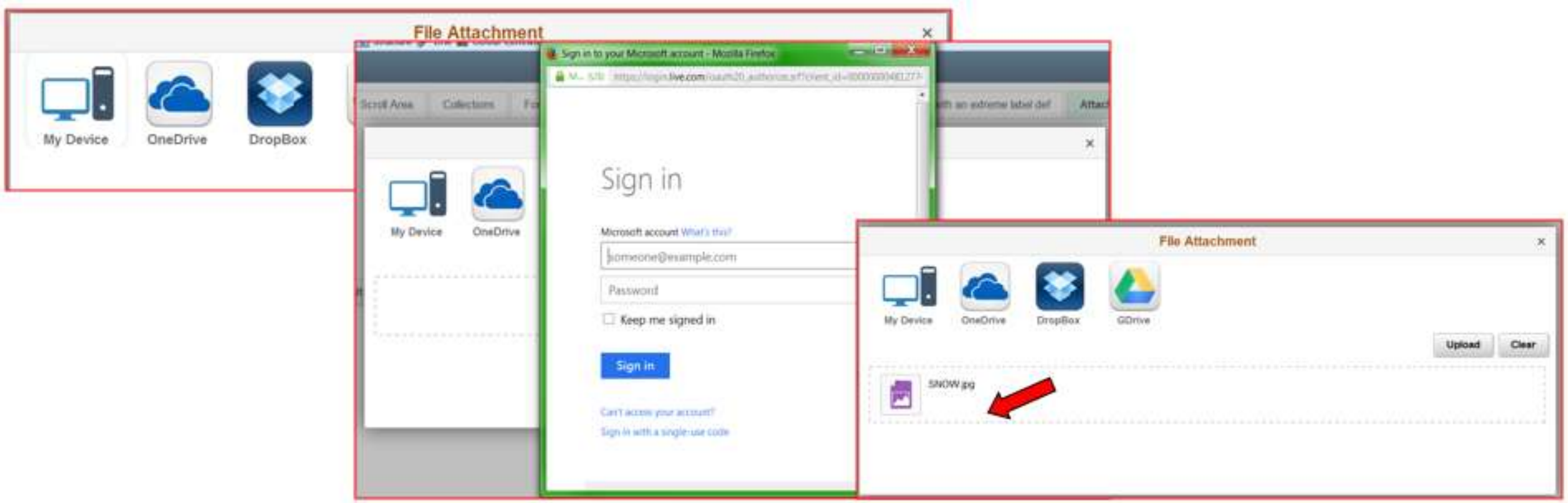
ALERTS

guration page

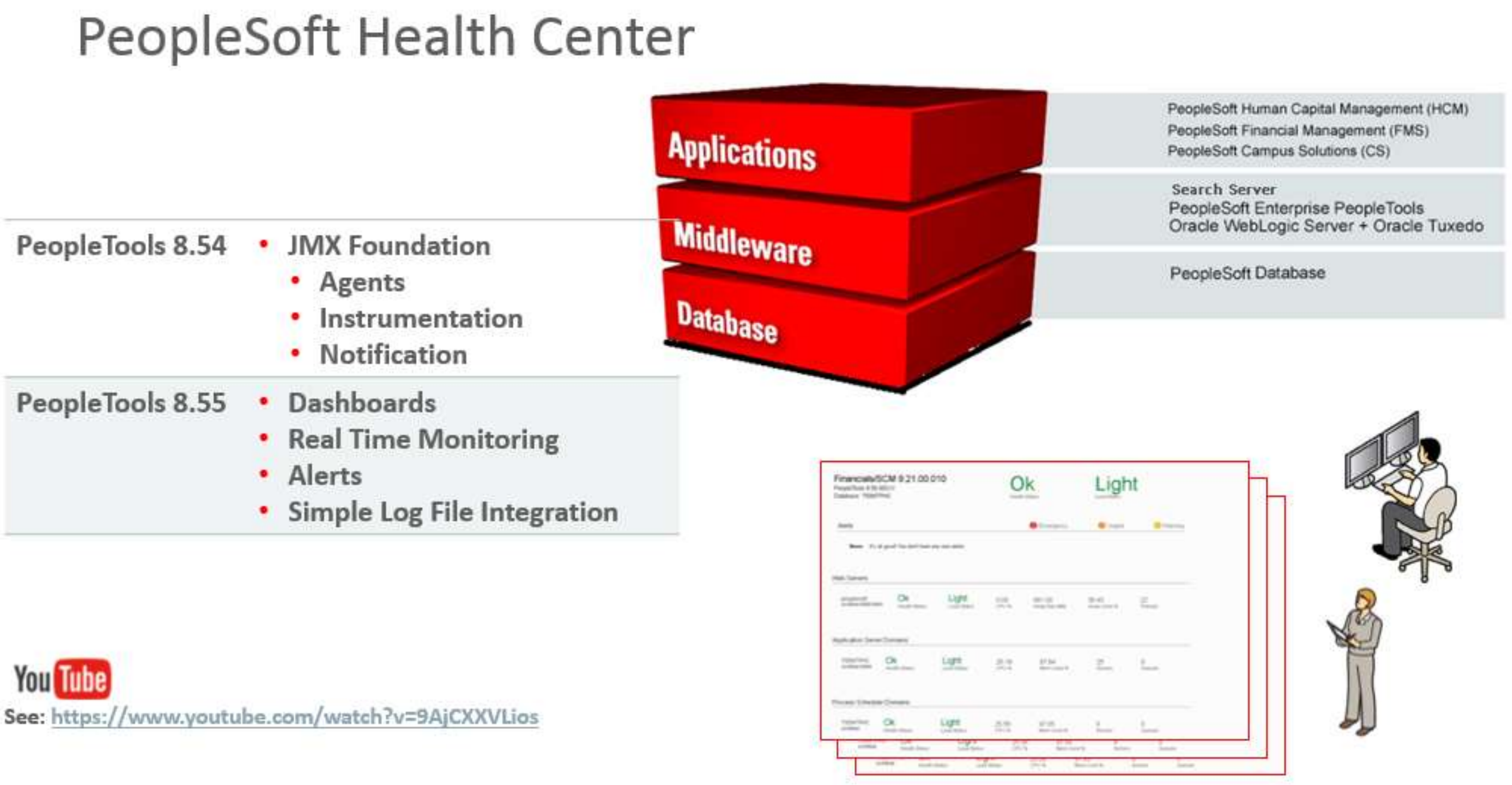
Authentication for Cloud File Attachment

PeopleSoft will allow upload files, for instance, their resume, directly from the cloud based storage services such as OneDrive, DropBox and others.

PeopleSoft will use the authentication, OAuth, used by the Cloud Storage provider so that the user can initiate the file transfer.



PeopleSoft Health Center



PeopleSoft Health Center

Applications
- PeopleSoft Human Capital Management (HCM)
- PeopleSoft Financial Management (FMS)
- PeopleSoft Campus Solutions (CS)

Middleware
- Search Server
- PeopleSoft Enterprise PeopleTools
- Oracle WebLogic Server + Oracle Tuxedo

Database
- PeopleSoft Database

PeopleTools 8.54	• JMX Foundation • Agents • Instrumentation • Notification
PeopleTools 8.55	• Dashboards • Real Time Monitoring • Alerts • Simple Log File Integration

YouTube

See: https://www.youtube.com/watch?v=9AjCXXVLios

PeopleTools 8.55 Features

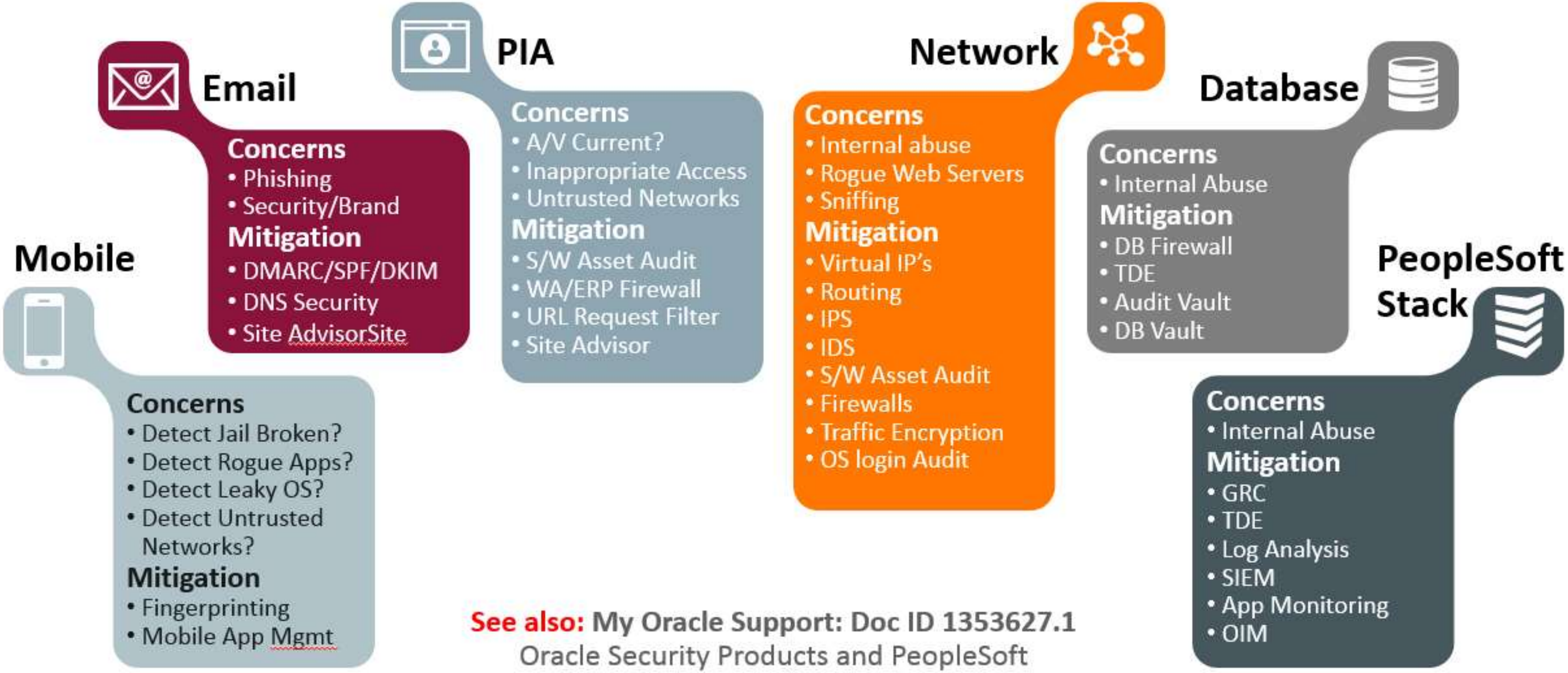
- **Security Deployment Tool**
  - New method of delivering security related updates to your target environment for menus, roles, and permission lists through PeopleSoft Update Manager.
  - Previously, updates to existing menus, roles, and permission lists were delivered via manual instruction documents that resulted in manual steps in your change package.
  - Review each of the delivered changes online by bug number and/or by object name. Determine whether you want to accept the change to be processed and applied to your target environment.
- **Automated Configuration Manager**
  - Manage security and integration end-points during environment replication and refresh activities

PeopleTools 8.55 Features

- Input Only Field
- Robust Forgotten Password
- Updated OpenSSL Libraries
- Log Correlation

Enterprise Security - Considerations

Elements of Threat Architecture and Enterprise Protection



Email

Concerns
- Phishing
- Security/Brand

Mitigation
- DMARC/SPF/DKIM
- DNS Security
- Site AdvisorSite

PIA

Concerns
- A/V Current?
- Inappropriate Access
- Untrusted Networks

Mitigation
- S/W Asset Audit
- WA/ERP Firewall
- URL Request Filter
- Site Advisor

Network

Concerns
- Internal abuse
- Rogue Web Servers
- Sniffing

Mitigation
- Virtual IP's
- Routing
- IPS
- IDS
- S/W Asset Audit
- Firewalls
- Traffic Encryption
- OS login Audit

Database

Concerns
- Internal Abuse

Mitigation
- DB Firewall
- TDE
- Audit Vault
- DB Vault

Mobile

Concerns
- Detect Jail Broken?
- Detect Rogue Apps?
- Detect Leaky OS?
- Detect Untrusted Networks?

Mitigation
- Fingerprinting
- Mobile App Mgmt

PeopleSoft Stack

Concerns
- Internal Abuse

Mitigation
- GRC
- TDE
- Log Analysis
- SIEM
- App Monitoring
- OIM

See also: My Oracle Support: Doc ID 1353627.1
Oracle Security Products and PeopleSoft

Enterprise Security - Considerations

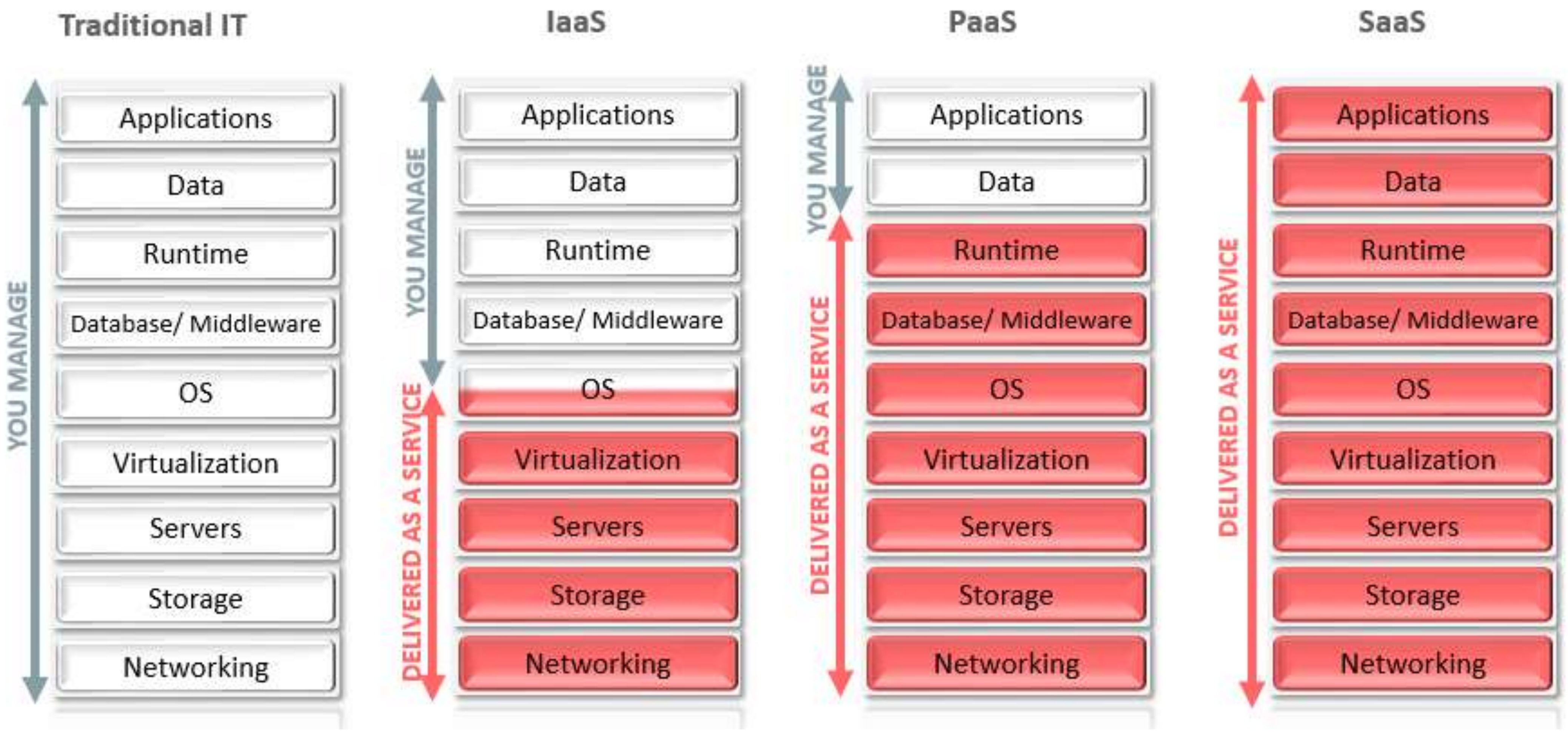
- Each new technology opens new Attack Vectors
- Compliance Does Not Equal Security
- IT Security Is Not Just For The IT Department
- Real Consequences for Loss of Security
- Balancing the Need for Security With the Need for Productivity

Prevent PeopleSoft Becoming Collateral Damage

- Invest in Collaboration
  - Enterprise Security Virtual Teams
- Enterprise Wide, Tested and Updated, Security Processes
- System Health Dashboard
- **Weighted, Organization Specific, CPU Advisory Analysis**
- Phishing Awareness and Protection

Cloud Security - Considerations

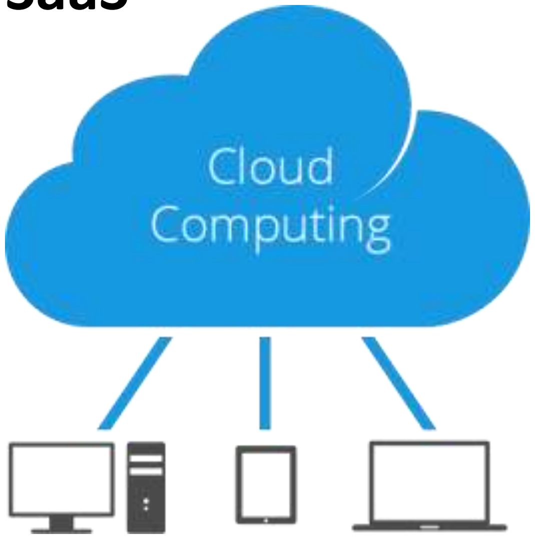
Operational Differences in Cloud Models



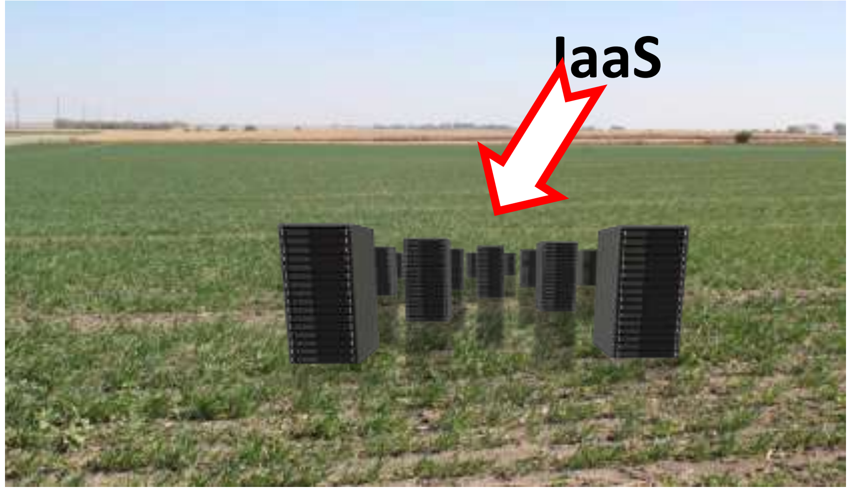
Traditional IT	IaaS	PaaS	SaaS
Applications	Applications	Applications	Applications
Data	Data	Data	Data
Runtime	Runtime	Runtime	Runtime
Database/ Middleware	Database/ Middleware	Database/ Middleware	Database/ Middleware
OS	OS	OS	OS
Virtualization	Virtualization	Virtualization	Virtualization
Servers	Servers	Servers	Servers
Storage	Storage	Storage	Storage
Networking	Networking	Networking	Networking

Cloud Security - Considerations

SaaS



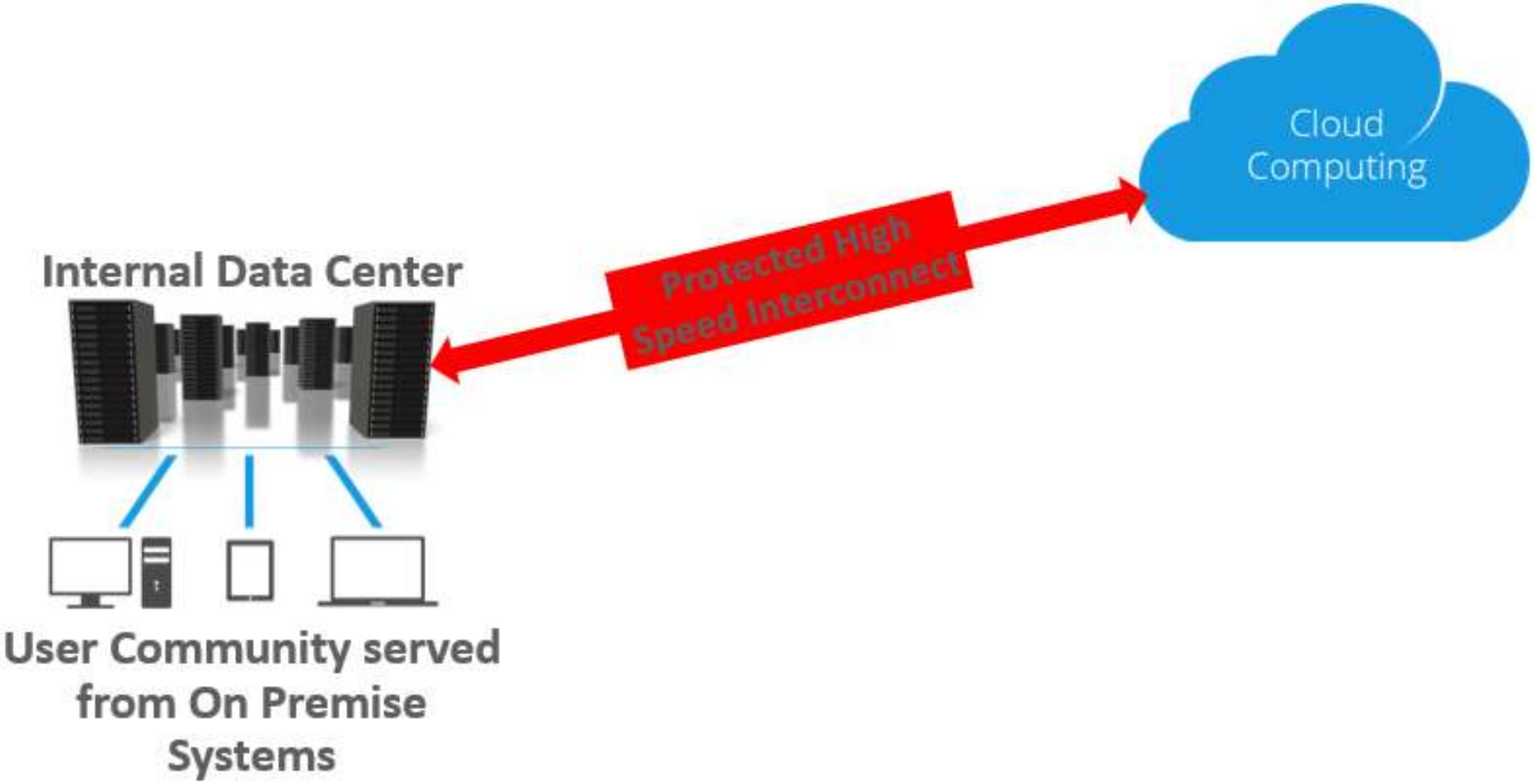
- **Delivered Security Bundle**
- **Additional Fee Based Services**
- **Visibility and Transparency?**
- **Brand Protection**



- **Bring Your Own License - BYOL**
- **Bring Your Own In House Expertise**
- **Bring Your Own Management Processes**
- **Bring Your Own Audit and Monitoring**
- **Bring Your Own Policy Management**
- **Bring Your own Disaster Recovery**
- **Bring Your own Brand Protection**

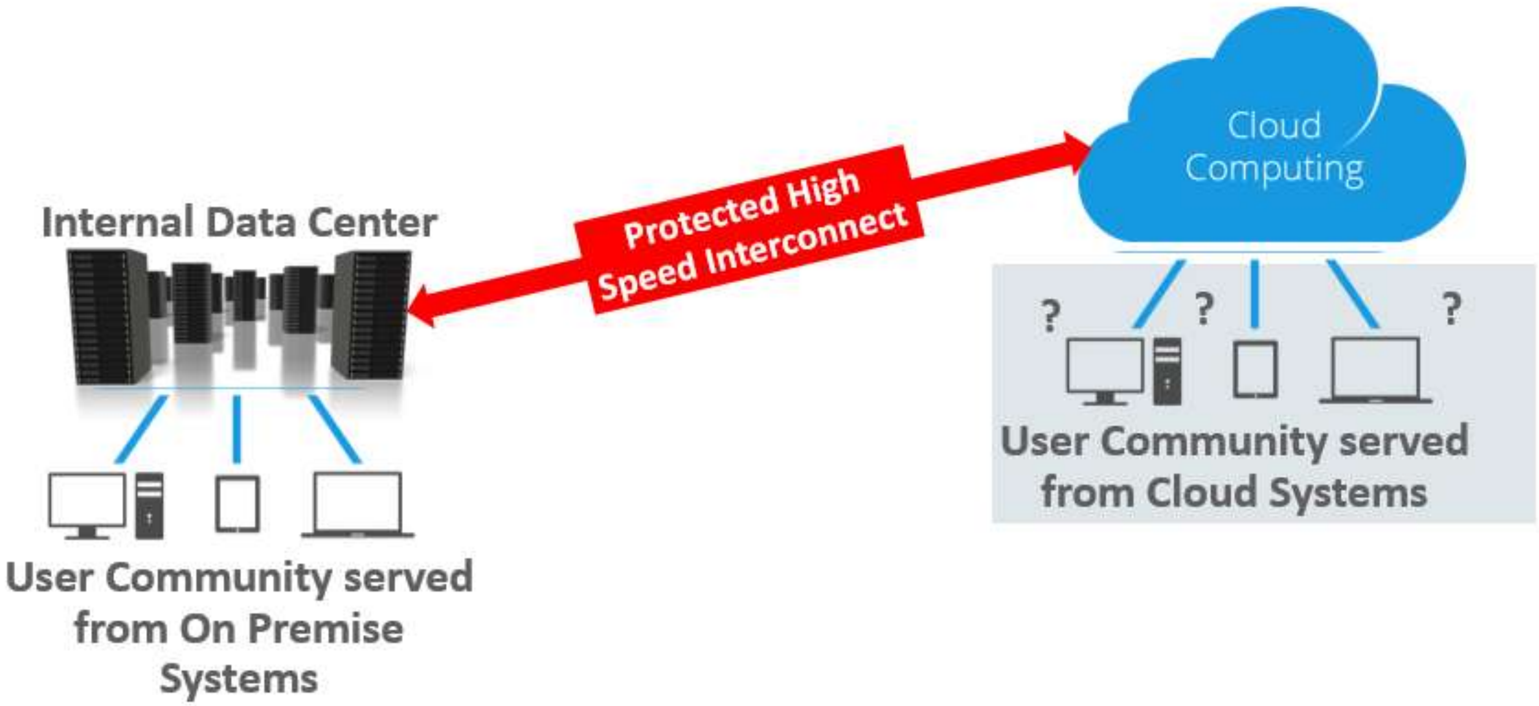
Cloud Security - Considerations

The cloud (I/PaaS) can be simply an extension of your existing data center …


Cloud Computing
Protected High Speed Interconnect
Internal Data Center
User Community served from On Premise Systems

Cloud Security - Considerations

… or the basis of delivering services separately to end users.



Internal Data Center
Protected High Speed Interconnect
Cloud Computing
?
?
?
User Community served from On Premise Systems
User Community served from Cloud Systems

If you are considering delivering user services directly from the cloud and you do not have your on-premise system security in place, you are unlikely to be successfully secure in the cloud.

Q/A Time

How do you treat your passwords?

Partner

Toothbrush

Underwear

- ✓ **Choose a good one**
- ✓ **Don’t share with anyone**
- ✓ **Change it occasionally**

Q&A

Logesh Balasubramaniam
Presence of IT | Excellence in People
Logesh.balasubramaniam@presenceofit.com
m. +64 021 251 9921 | **t.** 1300 665 503
blog: https://leanitdesigns.wordpress.com