October 22–25, 2018
SAN FRANCISCO, CA

#OOW18

ORACLE OPEN WORLD

PRO4443
Harden and Protect PeopleSoft On-Premises and in the Cloud

Greg Kelly, Product Strategy Manager, Oracle

oracle.com/openworld

ORACLE

When a crisis arises

The time for preparation has passed

ORACLE

Agenda

- Threat Architecture
- Hardening
- Security Considerations for a Security Strategy
- Security Considerations for Cloud
- Prevent PeopleSoft Becoming Collateral Damage
- Past Cases Discussion

ORACLE

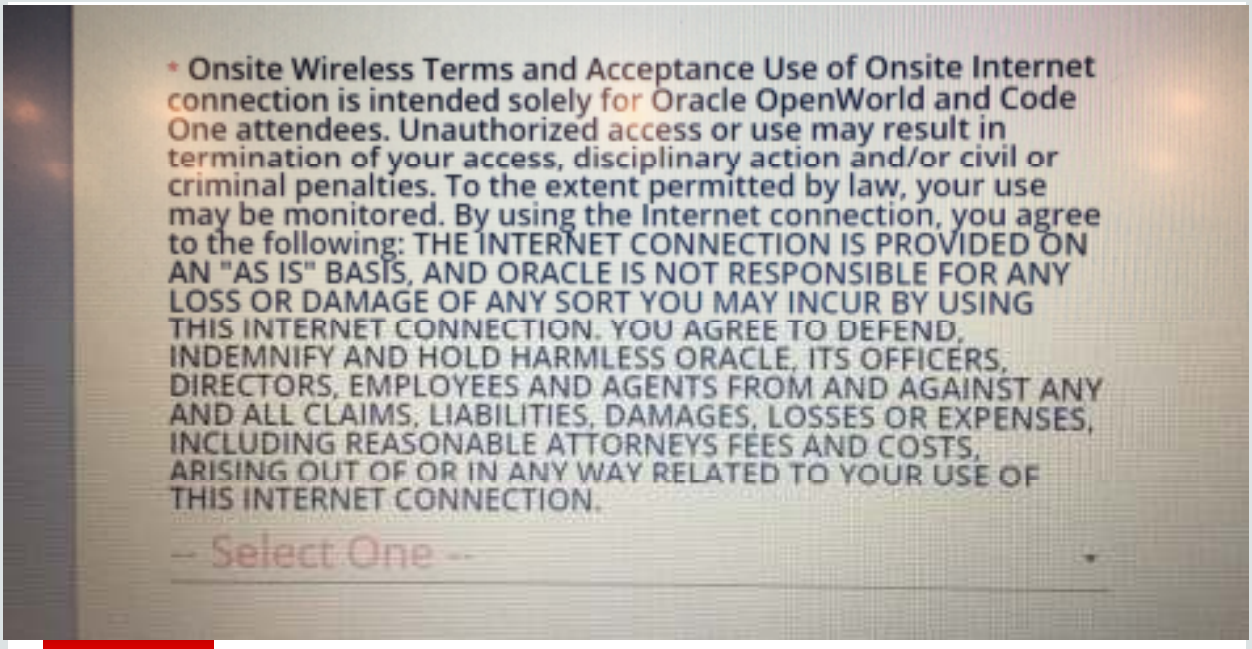
 3

Safe Harbor Statement

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

ORACLE

 4



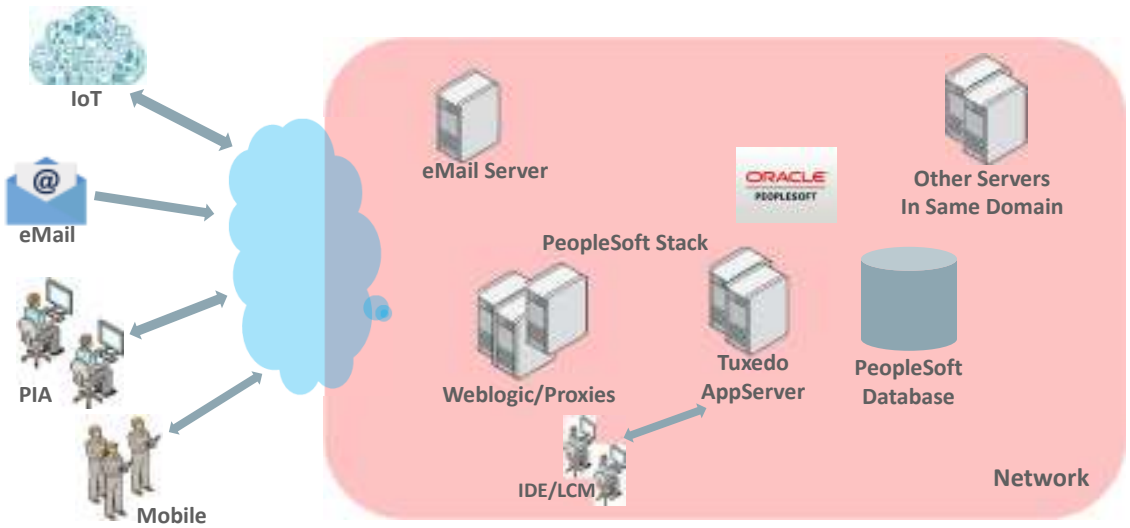
 5

Agenda

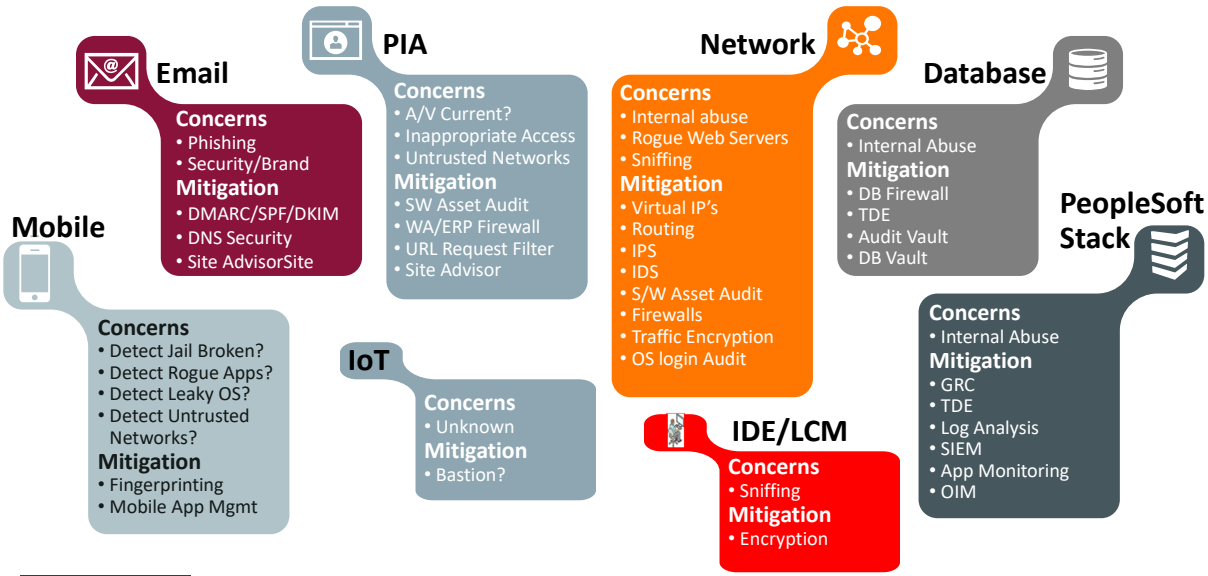
- Threat Architecture
- Hardening
- Security Considerations for a Security Strategy
- Security Considerations for Cloud
- Prevent PeopleSoft Becoming Collateral Damage
- Past Cases Discussion

 6

PeopleSoft Architecture and Threat Vectors

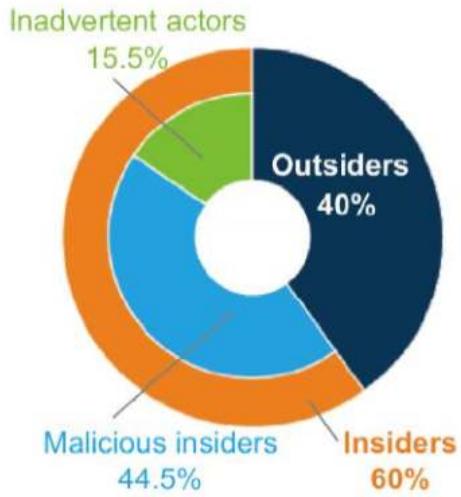


Elements of Threat Architecture and Enterprise Protection



Insider Abuse - Contributing Factors

- Moral Luck
- Moral Hazard
- Normalization of Deviance
  - "*Familiarity Breeds Contempt*"
- Broken Pane Syndrome
- Willful Blindness
- Hubris
- Disengagement/Disenchantment



ORACLE

 9

Forecast Impending Attack Tsunamis

Phishing attackers have moved beyond individuals' credentials, because users click on links in email – see also "Click Bait"

- Ransomware
- cryptomining malware

The big one, when it hits:
Massive Shibboleth IDP Attack

Mitigations:
- Monitoring
- URL Request Filtering
- Site Advisor
- IP Reputation
- Auditing

ORACLE

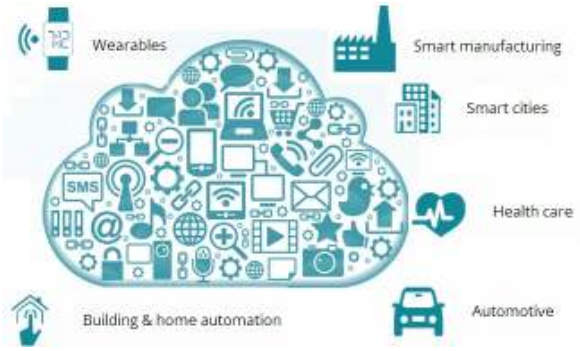
 10

IoT BotNet Threat

Massive DDoS attack harnesses 145,000 hacked IoT devices
http://www.healthcareitnews.com/news/massive-ddos-attack-harnesses-145000-hacked-iot-devices

Security expert says these types of attacks are likely to become more common. EHRs and other hospital IT systems could face dramatic new risks.

In what some are calling the biggest distributed denial-of-services attack ever seen, a botnet comprising thousands of hacked Internet-of-Things devices took aim at a European web host earlier this month – flooding it with a data deluge that at times exceeded one terabit per second.



IoT Breach

Smart teddy bears for kids suffer a contentious data breach
http://www.pcworld.com/article/3175229/security/smart-teddy-bears-involved-in-a-contentious-data-breach.html
The toy maker experienced a serious data breach, say security researchers, but the company denies that any voice recordings were stolen.

...
In the case of CloudPets, the brand allegedly made the mistake of storing the customer information in a publicly exposed online MongoDB database that required no authentication to access. That allowed anyone, including hackers, to view and steal the data.

On the plus side, the passwords exposed in the breach are hashed with the bcrypt algorithm, making them difficult to crack. Unfortunately, CloudPets placed no requirement on password strength, meaning that even a single character such as letter "a" was acceptable, according to Hunt, who was given a copy of the stolen data last week.

What's Wrong With This Picture

ORACLE

Agenda

- Threat Architecture
- Hardening
- Security Considerations for a Security Strategy
- Security Considerations for Cloud
- Prevent PeopleSoft Becoming Collateral Damage
- Past Cases Discussion

ORACLE

Hardening – Security Red Paper
Chapter 3 - SECURING NETWORK INFRASTRUCTURE

Secure Setups
- NAT DMZ Infrastructure
- Publicly Addressed DMZ Infrastructure
- Additional Security DMZ
- Firewall Application Server

Additional Network Protection
- Intrusion Detection Systems
- Intrusion Prevention Systems
- Web Application Firewalls
- Oracle Adaptive Access Manager

Hardening – Security Red Paper
Chapter 3 - SECURING NETWORK INFRASTRUCTURE

Secure Setups
- NAT DMZ Infrastructure
- Publicly Addressed DMZ Infrastructure
- Additional Security DMZ
- Firewall Application Server

Additional Network Protection
- Intrusion Detection S
- Intrusion Prevention
- Web Application Fire
- Oracle Adaptive Acc

- **Intrusion Detection Systems**
- **Intrusion Prevention Systems**
- **Web Application Firewalls**
- **Oracle Adaptive Access Manager**

Hardening – Security Red Paper
Chapter 4 - 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

ORACLE

Hardening – Security Red Paper
Chapter 4 - 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

How to Disable Configuration Re-Initialization - "AuditPWD"

How to Disable Browser Caching - note on "KIOSK“

How to Enable TUXEDO Encryption (LLE and SSL)

ORACLE

Hardening – Security Red Paper
Chapter 5 - PEOPLETOOLS SECURITY HARDENING (#1)

- 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

ORACLE

 19

Hardening – Security Red Paper
Chapter 5 - PEOPLETOOLS SECURITY HARDENING (#1)

- Delete or Disable Unused User IDs
- Enable Password Controls
- Expire Password At Next Logon
- Allow Password to be Emailed
- Review Sign-i
- Change the A
- Change the C
- Change the IB
- Review the Si
- Use Strong N
- Review Signo

- **Change the Access Password**
- **Change the Connect Password**
- **Review the Single Signon Configuration**
- **Use Strong Node Passwords or Use Certificates**

ORACLE

 20

Hardening – Security Red Paper
Chapter 5 - PEOPLETOOLS SECURITY HARDENING (#2)

- 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

NOTE:
Oracle® Access Manager Integration Guide 10g (10.1.4.2)
https://docs.oracle.com/cd/E12530_01/oam.1014/e10356.pdf

ORACLE

 21

Hardening – Security Red Paper
Chapter 5 - PEOPLETOOLS SECURITY HARDENING (#2)

- 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 Applica
- Limit Access to Weblogic C
- Review Query Security
- Enable SQL Error Message S
- Track Users' Login and Logo
- Securing PS_HOME and PS_
- Consider Auditing and Orac

- **Limit Access to Weblogic Console**
- **Review Query Security**
- **Enable SQL Error Message Suppression**
- **Track Users' Login and Logout Activity - PSACCESSLOG and PSPTLOGINAUD**
- **Consider Auditing and Oracle Audit Vault**

NOTE:
Oracle® Access Manager Integration Guide 10g (10.1.4.2)
https://docs.oracle.com/cd/E12530_01/oam.1014/e10356.pdf

ORACLE

 22

Hardening – Security Red Paper
Chapter 6 - SECURING CUSTOMIZED PEOPLESOFT APPLICATIONS

- 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

Hardening – Security Red Paper
Chapter 6 - SECURING CUSTOMIZED PEOPLESOFT APPLICATIONS

- Configure every Component for Row-Level Security
- Isolate all User-Entered Data to a Bind Variable
- Escap • **Escape All User-Entered HTML**
- Turn
- User-
- Unde • **User-Entered File Names Should Not Include Paths**
- Prote • **Understanding WS-Security**

Hardening – Security Red Paper
Appendices

APPENDIX A - IMPLEMENTING SELF SERVICE OR GATEWAY
- Real time Synchronization
- Periodic (Near Real Time) Synchronization

APPENDIX B – SECURITY BUILDING BLOCKS

APPENDIX C – SECURITY CHECK LIST
- Security Hardening recommendations, Hosted, On-Premise or Cloud based Systems
- Questions for the IT/Security Team

ORACLE

New Content

HOW TO RESTRICT SITES WHICH CAN FRAME PEOPLESOFT APPLICATION CONTENT
If a PeopleSoft application needs to allow external sites to frame PeopleSoft pages, use 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.

Enabling TUXEDO Encryption
Currently, 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.

To enable TUDEDO-level encryption, LLE, edit the configuration file psappsrv.cfg for the domain.
Change the Encryption property for the Workstation Listener and the JOLT Listener sections. The default value of 0 does not encrypt.

Authorizing Resource Access Using Cross-Origin Resource Sharing (CORS)
The CORS standard gives web servers cross-domain access controls, which enable secure cross-domain data transfers.

ORACLE

Security Enhancements in PeopleTools 8.55

- Extended Access and Connect ID DB Password Length
- New Cookie Rules
- Implement SHA-2 (SHA-256) Certificate and Hash
- Event Mapping Framework
- Authentication for Cloud File Attachment

ORACLE

 27

New Cookie Rules (and see PeopleTools 8.57)

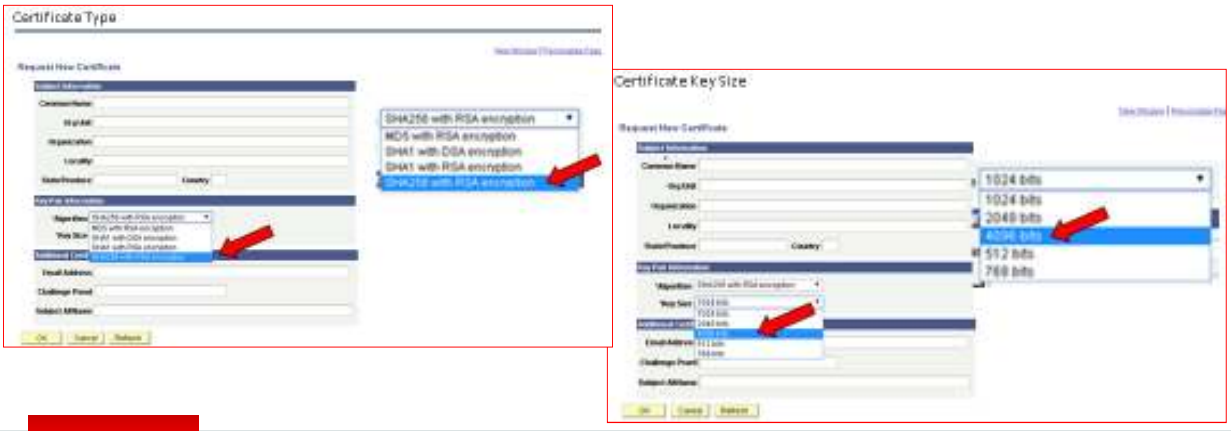
ORACLE

 28

PeopleTools 8.55 Security Features

Implement SHA-2 (SHA-256) Certificate

This feature was initially implemented by patch in:
PeopleTools **8.53.24** and PeopleTools **8.54.11**



 29

PeopleTools 8.55 Security Features

Implement SHA-2 (SHA-256) Hash

- Password in PSOPRDEFN will be SHA-2 hashed with salt
- Two new/modified functions

  `HashSHA256()` - Hash without salt

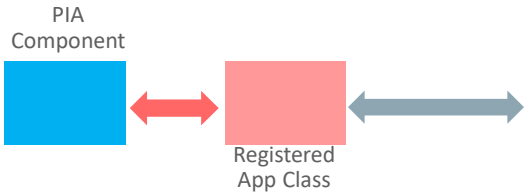
  `HashWithSalt()` - Hash with salt

  By default it is SHA-2 on PeopleTools 8.55, SHA-1 can be optional

Note: PS_TOKEN will continue to use SHA-1 digest. Customers will be recommended to use SHA-2 as Certificate Node Authentication

 30

Mapping Application Class PeopleCode To Component Events – the "PPR Hook" – Event Mapping Framework



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® Web Classification Service**
  https://webroot-cms-cdn.s3.amazonaws.com/4414/5625/1396/BCTI-WCS-WRS-DS_us.pdf
- **BrightCloud® IP Reputation Service**
  https://webroot-cms-cdn.s3.amazonaws.com/1114/5462/0565/BCSS-IPRS-DS.pdf
- **Use the ipinfo.io IP lookup API to integrate IP geolocation into your script or website.**
  http://ipinfo.io/developers
- **IP Location**
  https://www.iplocation.net/

ORACLE

PeopleTools 8.55 Security Features (not really)

Forwarded IP Addresses

Example

```
=====================================================
$ipaddress = '';
   if (getenv('HTTP_CLIENT_IP'))
      $ipaddress = getenv('HTTP_CLIENT_IP');
   else if(getenv('HTTP_X_FORWARDED_FOR'))
      $ipaddress = getenv('HTTP_X_FORWARDED_FOR');
   else if(getenv('HTTP_X_FORWARDED'))
      $ipaddress = getenv('HTTP_X_FORWARDED');
   else if(getenv('HTTP_FORWARDED_FOR'))
      $ipaddress = getenv('HTTP_FORWARDED_FOR');
   else if(getenv('HTTP_FORWARDED'))
      $ipaddress = getenv('HTTP_FORWARDED');
   else if(getenv('REMOTE_ADDR'))
      $ipaddress = getenv('REMOTE_ADDR');
   else
      $ipaddress = 'UNKNOWN';
=====================================================
```

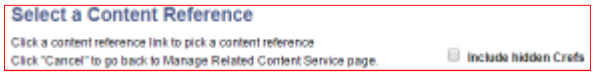
ORACLE

PeopleTools 8.55 Security Features

Mapping Application Class PeopleCode To Component Events – Event Mapping

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

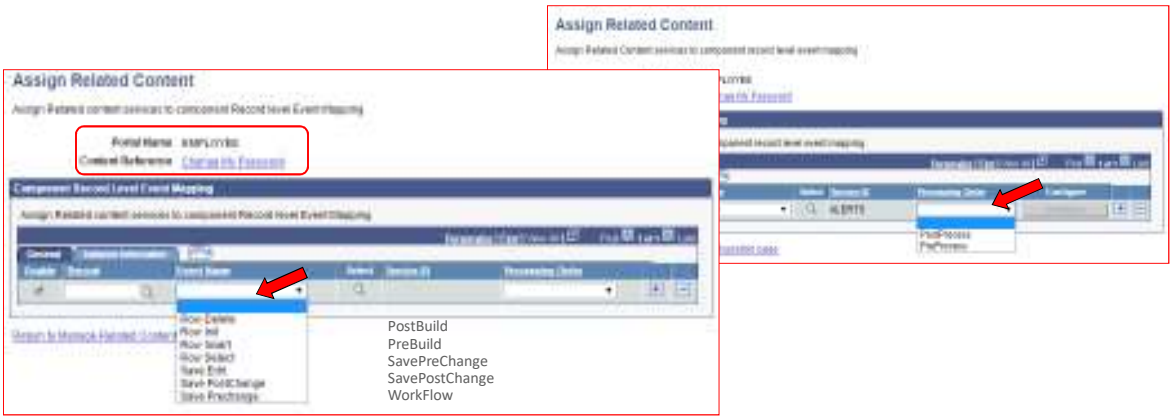
Developer chooses the Content Reference (CREF) from Select content reference page



PeopleTools 8.55 Security Features

Mapping Application Class PeopleCode To Component Events – Assign Related Content

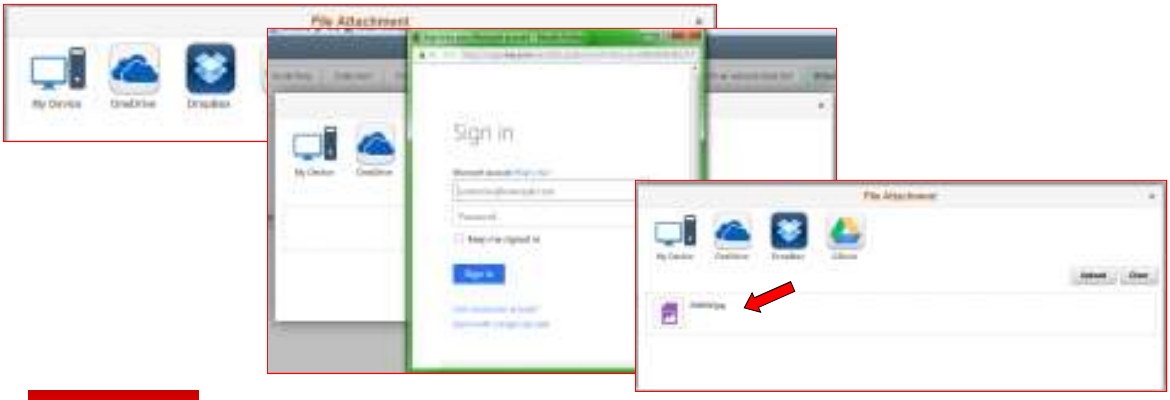
Developer chooses the event from Event name dropdown and processing order



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.



Additional Security Enhancements

- Input Only Field
- Robust Forgotten Password
- Updated OpenSSL Libraries
- Cross Origin Resource Sharing (AJAX request for PeopleSoft)
  - New “Authorized Sites” tab in Web Profile

New reference MOS postings

E-SES: How to enforce a specific TLS version (say TLSv1.2) in Peoplesoft with SES.

DocID 2235616.1: https://support.oracle.com/epmos/faces/DocumentDisplay?id=2235616.1

Useful PeopleSoft Security Links.

DocID 2060772.1: https://support.oracle.com/epmos/faces/DocumentDisplay?id=2060772.1

PeopleTools 8.56 feature updates - Security and Infrastructure Security

While we have established the robustness of PS_TOKEN using long complex node passwords or certificate based, in PeopleTools 8.56 we are adding additional validation to ensure prevention of misuse of the token.

We are extending and reviewing the crypto algorithms available to ensure continued data and authentication integrity.

In PeopleTools 8.56 we will also be introducing changes in the former delivery of hard coded Role and Permission Lists dependencies

PeopleTools 8.56 feature updates - Security and Infrastructure Enterprise Manager plug-in in Application Management Suite

With this release, PeopleSoft supports Enterprise Manager 13.2. The PeopleSoft plug-in is also being re-architected to use JMX as part of the metric gathering functionality. This will significantly reduce JVM overhead. The plug-in will also work with the EM hybrid agent to manage OPC deployment of PeopleSoft.

As part of the OPC deployment in Cloud Manager, PeopleTools 8.56 Enterprise Manager integration will also include automatic provisioning of EM hybrid agent and PeopleSoft plug-in in the deployed PeopleSoft instances.

PeopleTools 8.56 feature updates - Security and Infrastructure

File Processing

In PeopleTools 8.56 we are extending the support for cloud based file attachments to include Oracle Document Cloud as an additional file attachment source.

PeopleSoft integration with LinkedIn using OAuth (limited use case)

PeopleSoft Health Center

Features in the PeopleSoft Health Center are being enhances to support DPK and OPC based deployments.

Event Mapping Framework

The Event Mapping Framework (also called the “PPR Hook”) will be extended to include additional events and an API to programmatically propagate the App Class mapping to multiple components.

 39

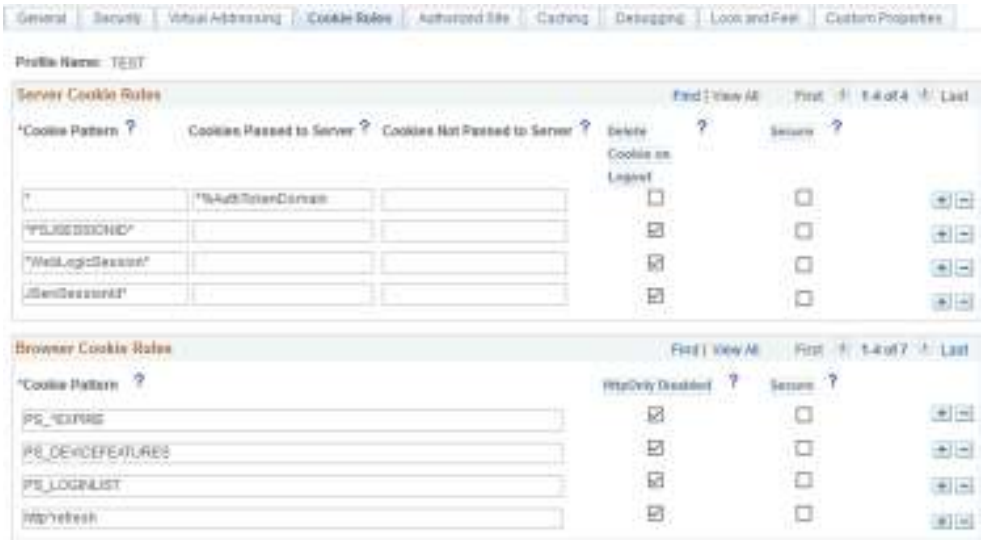
PeopleTools 8.57 feature updates - Security and Infrastructure

PeopleSoft PeopleTools 8.57 PeopleBooks

https://docs.oracle.com/cd/E99483_01/pt857pbr1/eng/pt/index.html

 40

Cookie Rules



Non-Root DPK deploy

PeopleSoft PeopleTools 8.57 Deployment Packages Installation document introduces a new optional procedure, task 2-2. It outlines the steps required to perform an install as a non-root user for those customer shops where the PeopleSoft administrator is not allowed to have root access. There is still a pre-requisite step that root must perform, but that is the case with other products as well.

Contents

Task 2-2: Deploying as a Non-Root User on Linux, AIX, HP-UX, or Solaris

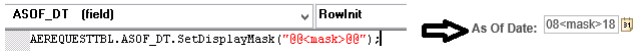
This section discusses:

- Preparing to Run the DPK Setup Script as a Non-Root User on Linux, AIX, HP-UX, or Solaris
- Running the DPK Setup Prerequisite for Linux, AIX, HP-UX, or Solaris
- Running the DPK Setup Script as a Non-Root User on Linux, AIX, HP-UX, or Solaris

PeopleCode Masking API

- The functionality is brand new and can only be accessed by writing new PeopleCode.
- The new Field Object API is called SetDisplayMask().
- SetDisplayMask was delivered in 8.57 GA requiring 2 parameters.
  - The First Parameter is a Single Char, which will be used as the masking character. No matter what length of string is provided in the parameter only the first Character will be used.
  - The Second Parameter is a Numeric which indicates how many right-most Characters are to remain unmasked.

- SetDisplayMask is being updated in the 8.57.03 patch.
  - The second parameter will now be optional. When present the above functionality will be used.
  - When the second parameter is not supplied the First parameter will be processed as a Mask Pattern. The Mask Pattern will only be applied if the length of the Mask Pattern matched the length of the Displayed Value. The @ symbol means do not mask this position in the data.



AUDIT TABLES FOR MANAGED OBJECTS IN SECURITY

Delivered Changes

- Audit Tables for Security Objects
  - Delivered as a convenience to customers
  - audit tables are clones of the original Security tables
  - No Code changes are delivered with the tables
  - Customers can create DB triggers that execute on the DB platform they are running
  - Customers can create views to select the fields they want to audit

PeopleTools Security : Cryptography

- upgrade the encryption strength to AES-128bits.
- stronger encryption function using stronger encryption algorithm

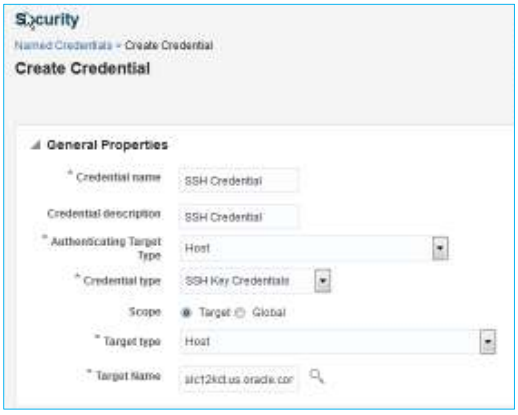
ORACLE

ORACLE

Enhancement: Improved Logging with Log4j 2

Discovery Plug-in	
%AGENT_HOME%/plugins/oracle.apps.psft.discovery.plugin_13.3.1.1.0/config/psemdiscoveryllogging.properties	**%AGENT_HOME%/plugins/oracle.apps.psft.discovery.plugin_13.3.1.1.0/config/discoveryLogging.xml**
Agent Plug-in	
%AGENT_HOME%/plugins/oracle.apps.psft.agent.plugin_13.2.1.1.0/config/psemagentlogging.properties	%AGENT_HOME%/plugins/oracle.apps.psft.agent.plugin_13.2.1.1.0/config/agentLogging.xml
%AGENT_HOME%/plugins/oracle.apps.psft.agent.plugin_13.2.1.1.0/config/psemmetricslogging.properties	%AGENT_HOME%/plugins/oracle.apps.psft.agent.plugin_13.2.1.1.0/config/metricLogging.xml

Enhancement: SSH Credential Support



Agenda

- Threat Architecture
- Hardening
- Security Considerations for a Security Strategy
- Security Considerations for Cloud
- Prevent PeopleSoft Becoming Collateral Damage
- Past Cases Discussion

Security Considerations for a Security Strategy

IT Security Is Not Just For The IT Department

The consequences of the loss of security doesn't have to be discussed at a technical level in the board room, but should be a topic.

- The effect on Brand
- Loss of consumer (even user) confidence in your ability to protect data
- Diminished value (share price) of the organization

Security Considerations for a Security Strategy

Real Consequences for Loss of Security

Data loss has a real effect on the bottom line, through loss of business and reparation expense.

Security Considerations for a Security Strategy

All Hackers are not Blackhats

- Criminal Organizations
- "Hacktivists" and Whistle Blowers
- Deliberate and Inadvertent insider abuse

Security Considerations for a Security Strategy

Each new technology opens new Attack Vectors

Regardless of company size, it's likely you've been attacked, even if you don't realize it. As well as virus's, malware and malicious software, consider the risks imposed by use of smartphone/tablets and cloud computing.

Security Considerations for a Security Strategy

Compliance Does Not Equal Security

Compliance Certification is point in time. Typically a certification is engaged for the project, possibly on an annual basis.
Security is an ongoing effort.

Security Considerations for a Security Strategy

Balancing the Need for Security With the Need for Productivity

Smart phones and tablets have forever changed the way we work. How can you be sure these efficiency-boosting tools aren't introducing security risks and/or leaving with data they shouldn't?

Security Considerations for a Security Strategy

Security is NOT Just a Technology Problem

Often the biggest risk to an organization is the behavior of the people inside. How do you encourage and build an environment that leverages strong company-wide employee education on top of effective technology leadership within IT?

Agenda

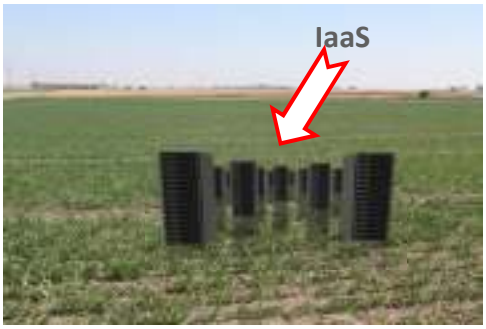
- Threat Architecture
- Hardening
- Security Considerations for a Security Strategy
- Security Considerations for Cloud
- Prevent PeopleSoft Becoming Collateral Damage
- Past Cases Discussion

ORACLE

"Cloud"

SaaS

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



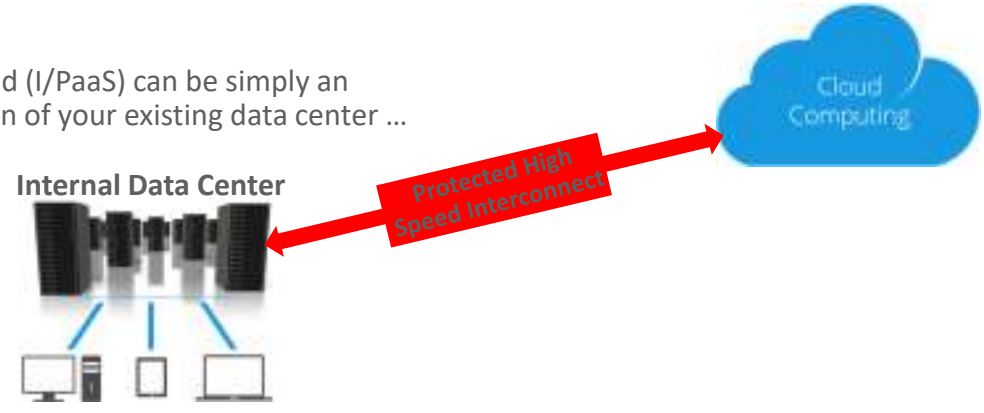
Bring Your Own License - BYOL

- 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
- . . .

ORACLE

Cloud Deployment

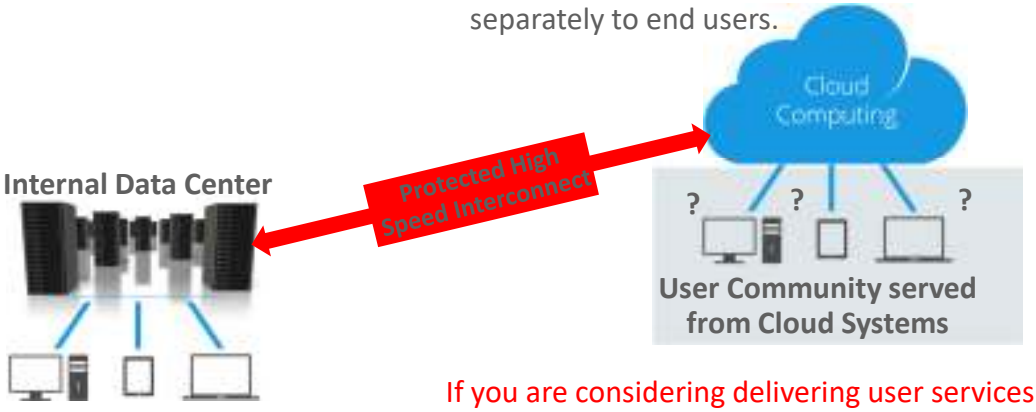
The cloud (I/PaaS) can be simply an extension of your existing data center …



ORACLE

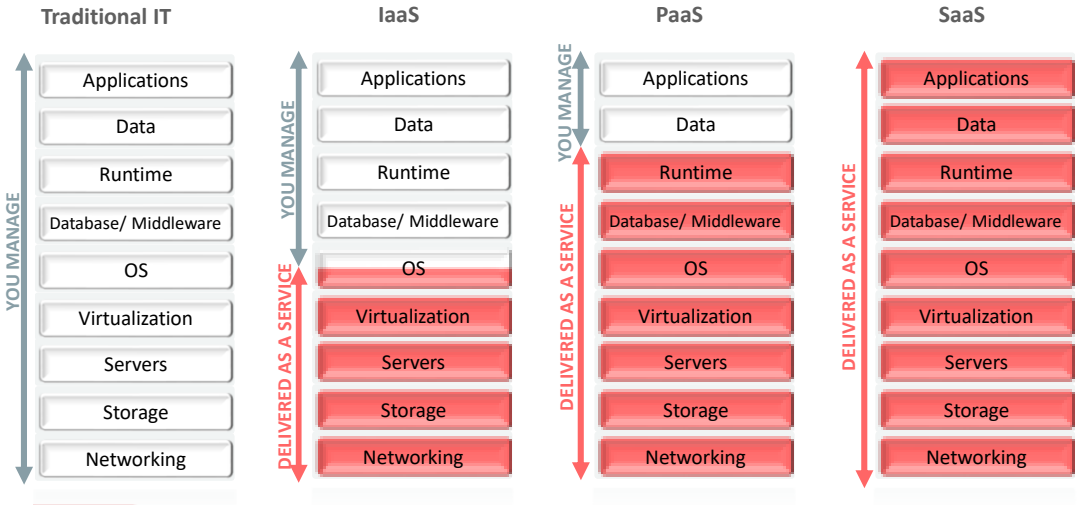
Cloud Deployment

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

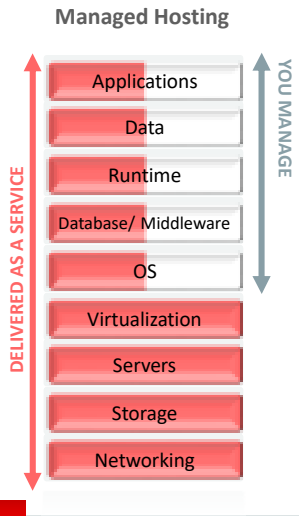


If you are considering delivering user services directly from the cloud and you do not have your on-premise system security in place, you are unlikely to be successfully secure in the cloud.

Operational Differences in Cloud Models



Other Cloud Models



- Overlapping trust boundaries
- Customer-specific deployments
- Many bespoke integration points
- Often requires additional
  - Technical Controls
  - Detective Controls
  - Administrative Controls
  - Contractual Controls

Agenda

- Threat Architecture
- Hardening
- Security Considerations for a Security Strategy
- Security Considerations for Cloud
- Prevent PeopleSoft Becoming Collateral Damage
- Past Cases Discussion

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**
- **Review PCI DSS v3 (Why?)**

ORACLE

Agenda

- Threat Architecture
- Hardening
- Security Considerations for a Security Strategy
- Security Considerations for Cloud
- Prevent PeopleSoft Becoming Collateral Damage
- Past Cases Discussion

ORACLE

Case #1

$4.5M office supply scheme inside Las Vegas water district draws FBI inquiry
http://www.reviewjournal.com/news/las-vegas/45m-office-supply-scheme-inside-las-vegas-water-district-draws-fbi-inquiry

... The scheme, which unfolded over three years, involved an employee in the district's purchasing division who fraudulently ordered office supplies through the water utility's vendor, then sold the items to a company in New Jersey and kept the money.

Case #2

Target settles for $39 million over data breach
http://money.cnn.com/2015/12/02/news/companies/target-data-breach-settlement/

Target agreed to a $39 million settlement with several U.S. banks on Wednesday over a data breach that affected roughly 40 million customers.

The banks lost millions when they were forced to reimburse customers who lost money in the massive 2013 hack of Target's database.

Case #3

The Trusted Grown-Ups Who Steal Millions From Youth Sports
http://www.nytimes.com/2016/07/10/sports/youth-sports-embezzlement-by-adults.html
Prosecutors in several states say embezzlement investigations involving youth sports have become common.

... Across the country, people who volunteered as treasurers and other officers for Little Leagues and sports clubs have been prosecuted for pilfering gobs of money from the coffers: $220,000 in Washington, $431,000 in Minnesota, $560,000 in New Jersey, and so on, according to law enforcement authorities, league officials, experts on nonprofit organizations and news reports.

ORACLE

Remember –
Fluid, VPN, (T)OTP, HTTPS are not alone sufficient security for Smartphone/Tablet access, other protection has to be considered

ORACLE

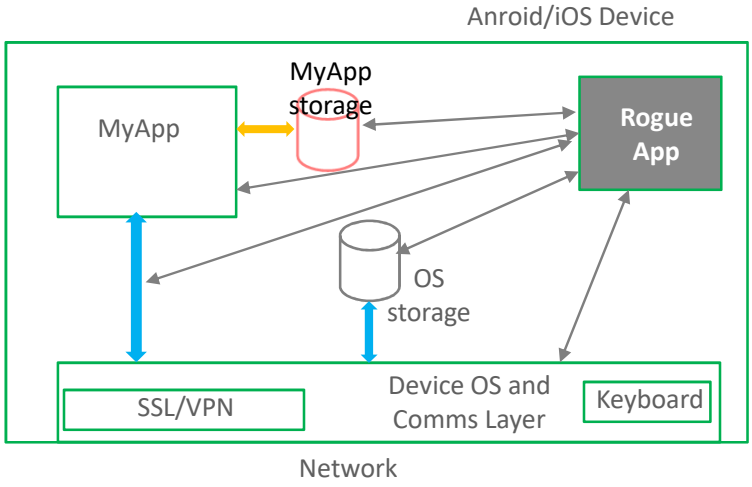
Considerations for BYOD Security

- Leaky operating systems
- Rogue applications
- Where is the Perimeter? (DMZ)
- Device Secure Transport demarcation
- Ability to distinguish trusted and untrusted networks
- Mobile Device Management (MDM)
  Mobile Application Management (MAM)
- Oracle Mobile Security Suite(OMSS)
  http://www.oracle.com/technetwork/middleware/id-mgmt/overview/omss-data-sheet-2104764.pdf

ORACLE

BYOD (Android/iOS) Device Considerations

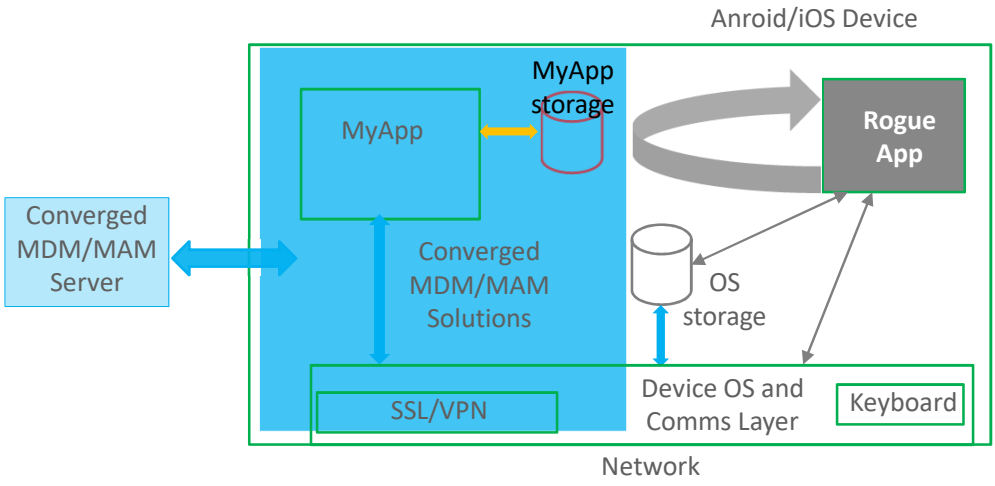
Unprotected



ORACLE

BYOD (Android/iOS) Device Considerations

Protected – including Oracle Access Manager Mobile & Social



ORACLE

Some Additional Useful Links

The insidious threat - the hacker behind the firewall
https://blogs.oracle.com/peopletools/entry/the_insidious_threat_the_hacke

Why are we concerned about a "sniffer" behind the firewall?
https://blogs.oracle.com/peopletools/entry/why_are_we_concerned_about_a_s

PeopleTools CPU analysis and supported versions of PeopleTools
https://blogs.oracle.com/peopletools/entry/peopletools_cpu_analysis_and_supported

Open the following URL in MS IE which seems to format the output best:
http://www.oracle.com/ocom/groups/public/@otn/documents/webcontent/3432537.xml

ORACLE

ORACLE