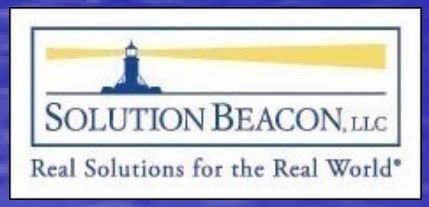
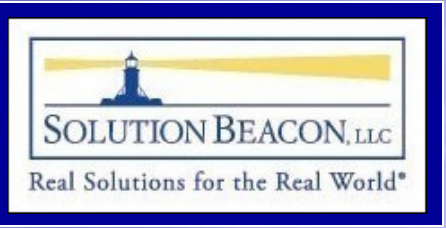
Oracle E-Business Suite Release 11*i* Security

Randy Giefer
Applications DBA and Security Specialist
John Stouffer
Applications DBA

Release 11*i* Workshops
Dallas, TX • San Ramon, CA •
Cincinnati, OH • Denver, CO • Atlanta, GA
Detroit, MI • Las Vegas, NV
www.solutionbeacon.com



Welcome



- Today's Agenda:
  - OAUG Membership Benefits
  - Presenter Introductions
  - Presentation Overview
  - 30 Minute Release 11*i* Security
  - Minute 31 – Your Next Steps
  - Questions and Answers

Are you an OAUG Member?

SOLUTION BEACON, LLC
Real Solutions for the Real World®

OAUG™ oracle applications users group

Global Users. Global Solutions.

Member Benefits include:

- **Advocacy** opportunities to influence Oracle on product enhancements, usability, new features, Oracle support, pricing and quality
- **Knowledge** that showcases the latest trends and techniques used by industry leaders through our national and regional events and our publications, such as OAUG Insight magazine
- **Communication** with other OAUG members worldwide through participation in OAUG committees, leadership positions, interaction with Oracle Corporation's user initiatives, frequent member surveys, and Oracle management briefings
- **Education** through the hundreds of career-enhancing presentations in our conference paper database archive, as well as discounts to conferences and Oracle education
- **Networking** with Oracle customers, industry experts, third-party software firms, and other Oracle Applications specialists through our Member Database and Online Vendor Directory

ORACLE CERTIFIED PARTNER

ROAD TO Las Vegas

Release 11*i* Security

Keeping The Bad (and Badder) Guys Away

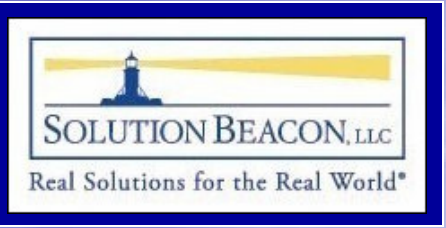
Release 11*i* Workshops

Dallas, TX • San Ramon, CA •
Cincinnati, OH • Denver, CO • Atlanta, GA
Detroit, MI • Las Vegas, NV

www.solutionbeacon.com

SOLUTION BEACON, LLC
Real Solutions for the Real World®

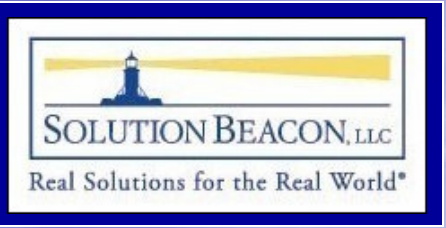
Presenter – Randy Giefer



- 20+ years of IT experience
  - Databases and Applications
  - 10 years Oracle Apps DBA
  - Fortune 1-1000
  - Government
- Founder of Solution Beacon, LLC
- Security Practice
- Email: rgiefer@solutionbeacon.com

ORACLE CERTIFIED PARTNER

Presentation Overview



- ½ Awareness
- ½ Real World Best Practices

ORACLE CERTIFIED PARTNER

30 Minute Release 11*i* Security "Keeping The Bad People Away"

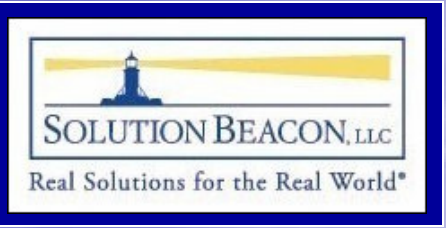
SOLUTION BEACON, LLC
Real Solutions for the Real World®

- Case Studies
  - Disgruntled Worldcom employee posts stolen names, SSN, birth dates of company executives on public website
  - Ex-Employee Steals CRM and Financials Data and Provides to Competitor

ORACLE CERTIFIED PARTNER

ROAD TO Las Vegas

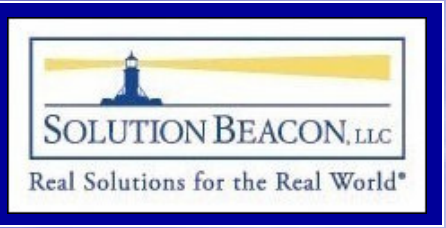
30 Minute Release 11*i* Security "Keeping The Bad People Away"



- Case Studies
  - Employee Sells Credit History Database
  - Employee Manipulates Payroll Data
  - AOL Employee Sells Email Addresses to Spammer
  - Laptops With Sensitive VA Data Stolen

ORACLE CERTIFIED PARTNER

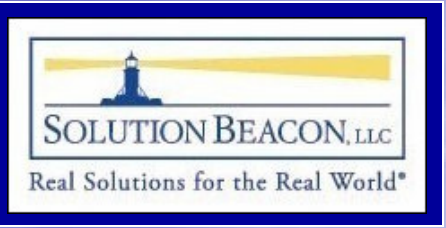
30 Minute Release 11*i* Security "Keeping The Bad People Away"



- Q. What do all of these Case Studies have in common?
  - Disgruntled Employee
  - Ex-Employee Steals CRM and Financials Data
  - Employee Sells Credit History Database
  - Employee Manipulates Payroll Data
  - Employee Sells Email Addresses to Spammer
  - Laptop With Sensitive VA Data Stolen
- A. A firewall didn't help!!!

ORACLE CERTIFIED PARTNER

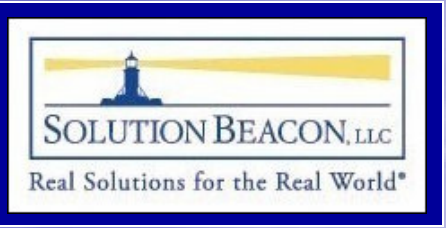
What Is Security?



- What do you think of when someone mentions “security”?
  - Physical Security
    - Three Gs (Guards, Gates, Gizmos)
  - Technology Stack Security
    - Network (e.g. Firewalls, Proxy Servers)
    - Server (e.g. Antivirus)
    - Database (Auditing?)
    - Application (Access Lists?)

ORACLE CERTIFIED PARTNER

What Is Security?



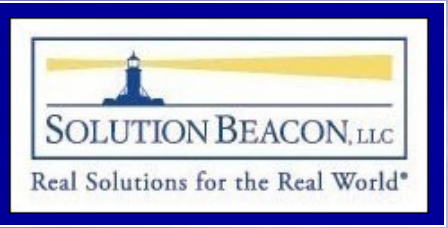
- Most often, Security is focused on trying to keep the *external* bad people out …
- But who is keeping out the *internal* bad people?

ORACLE CERTIFIED PARTNER

Today's Message

- The Internal Threats Are Real!

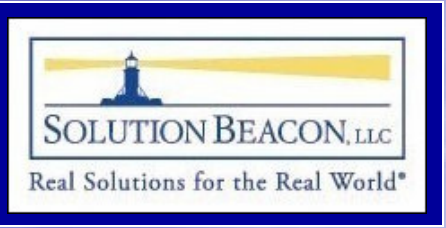
Fact: Internal Threats Are Real



Despite most people's fears that hackers will break into the company and destroy data or steal critical information, *more often than not, security breaches come from the inside*.

ORACLE CERTIFIED PARTNER

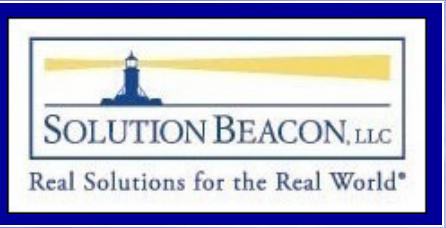
Fact: Internal Threats Are Real



- Gartner estimates that more than 70% of unauthorized access to information systems is committed by employees, as are more than 95% of intrusions that result in significant financial losses ...
- The FBI is also seeing rampant insider hacking, which accounts for 60% to 80% of corporate computer crimes

ORACLE CERTIFIED PARTNER

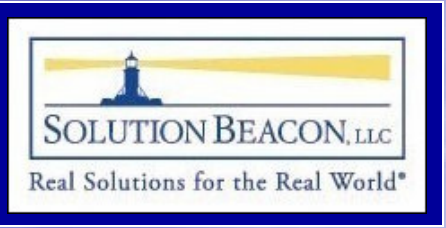
Fact: It may Happen To You



- In 2005, 20 Percent of Enterprises Will Experience a Serious Internet Security Incident – Gartner
- In 2005, 60 percent of security breach incident costs incurred by businesses will be financially or politically motivated – Gartner

ORACLE CERTIFIED PARTNER

Quotes From Industry Experts



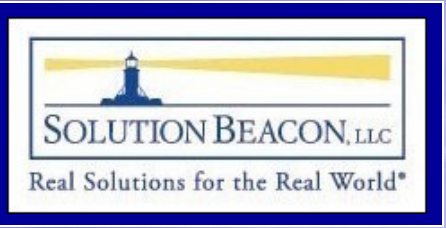
- "Insider attacks are where most of the money's lost, where most of the vulnerabilities are."

  Frank Huerta, Vice President Intrusion-Detection Product Delivery, Symantec

- "Technological protection from external threats is indeed important, but human problems cannot be solved with [only] technological solutions."

  Eric D. Shaw, Keven G. Ruby, & Jerrold M. Post, Security Awareness Bulletin / RAND

Quotes From Industry Experts

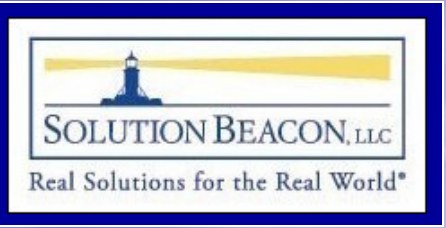


- "In the Banking and Finance sector, fraud is typically perpetrated by a non-technical current or former employee. Sabotage, on the other hand, is typically led by a technical disgruntled employee, usually a former employee."

  Dawn Cappelli, Carnegie Mellon University / CERT / Software Engineering Institute

ORACLE CERTIFIED PARTNER

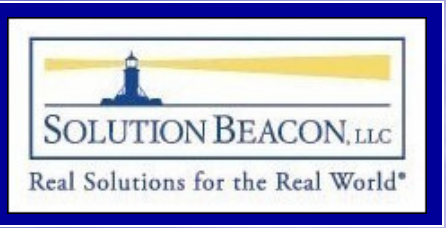
Fact: It may Happen To You



- Are you prepared?
- Can you prevent becoming a statistic?

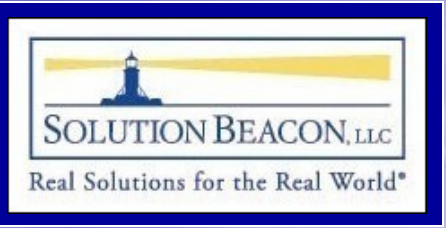
ORACLE CERTIFIED PARTNER

What Is Security?



- Security is a PROCESS that occurs (or doesn't occur) at multiple levels
- Security awareness at organizations varies due to:
  - Business Core Function
  - Organizational Tolerance (e.g. SOX)
  - Prior Incidents

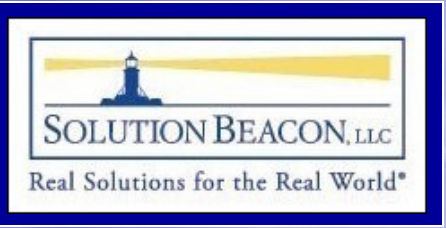
Security Is A Process



- "Process" means it occurs more than once!
  - Policies, Processes and Procedures
  - Internal and External Checks and Balances
  - Regular Assessments (Focus = Improve)
    - Internal
    - Third Party
  - Audits (Focus = $ for Auditors)
    - Necessary Evil
    - Many Don't Understand the Apps

ORACLE CERTIFIED PARTNER

What Is Applications Security?

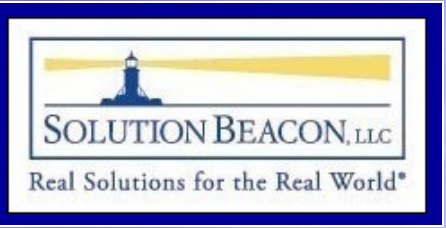


In an Oracle Applications environment, it's protection of information from:

- Accidental Data Loss
- Employees
- Ex-Employees
- Hackers
- Competition

ORACLE CERTIFIED PARTNER

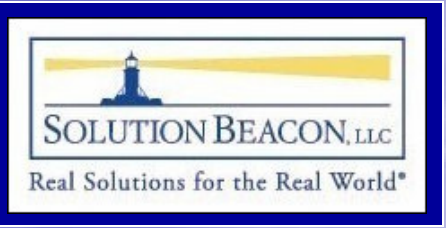
Application Security



- Part Technology, Mostly User Access
- User Security
  - Authentication
  - Authorization
  - Audit Trail

ORACLE CERTIFIED PARTNER

Application Security



- Authentication – Who are you?
- Authorization – What privileges do you have?
- Audit Trail – Effectiveness is almost useless if you can't ensure:
  - Individual accounts are used
  - Individuals are who they say they are

ORACLE CERTIFIED PARTNER

What is "30 Minute Release 11*i* Applications Security"?

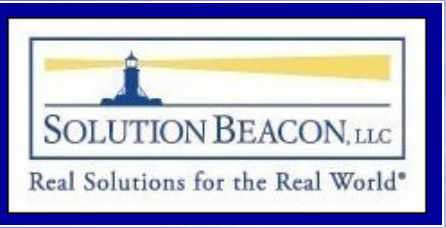
SOLUTION BEACON, LLC
Real Solutions for the Real World®

- Guide to Easily Implement Select Security Controls Consisting Of:
  - User Account Policies
  - Profile Options
- Quick and Easy to Implement
- Low Investment / High Return Value
- "Big Bang for the Buck"
- Required Foundation for other Security Controls

ORACLE CERTIFIED PARTNER

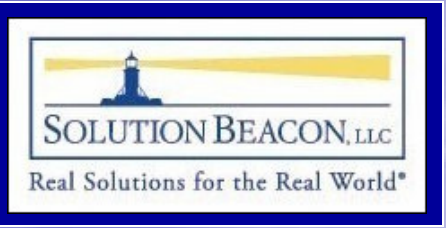
ROAD TO Las Vegas

Best Practice: No Shared Accounts



- Difficult or Impossible to Properly Audit
- How Hard Is It To Guess A Username?
- Release 11*i* Feature to Disallow Multiple Logins Under Same Username
- Uses WF Event/Subscription to Update ICX_SESSIONS Table
- 11.5.8 MP
- Patches 2319967, 2128669, WF 2.6

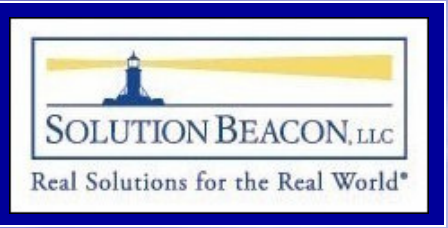
Best Practice: No Generic Passwords



- Stay Away From ‘welcome’!!!
- 11.5.10 Oracle User Management (UMX)
  - User Registration Flow
    - Select Random Password
    - Random Password Generator

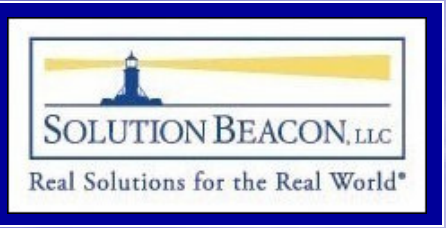
ORACLE CERTIFIED PARTNER

11.5.10 Oracle User Management (UMX)



- UMX leverages workflow to implement business logic around the registration process
- Raising business events
- Provide temporary storage of registration data
- Identity verification
- Username policies
- Include the integration point with Oracle Approval Management
- Create user accounts and release usernames
- Assign Access Roles
- Maintain registration status in the UMX schema
- Launch notification workflows

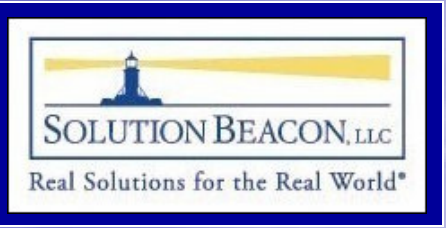
Profile: Signon Password Length



- Signon Password Length sets the minimum length of an Oracle Applications password value
- Default Value = 5 characters
- Recommendation: At least 7 characters

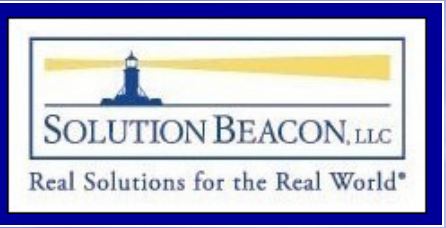
ORACLE CERTIFIED PARTNER

Profile: Signon Password Hard to Guess



- The Signon Password Hard to Guess profile option sets internal rules for verifying passwords to ensure that they will be "hard to guess"
- Oracle defines a password as hard-to-guess if it follows these rules:
  - The password contains at least one letter and at least one number
  - The password does not contain repeating characters
  - The password does not contain the username
- Default Value = No
- Recommendation = Yes

Profile: Signon Password No Reuse



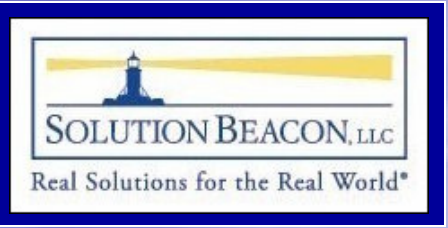
- This profile option is set to the number of days that must pass before a user is allowed to reuse a password
- Default Value = 0 days
- Recommendation = 180 days or greater

ORACLE CERTIFIED PARTNER

Profile: Signon Password Failure Limit

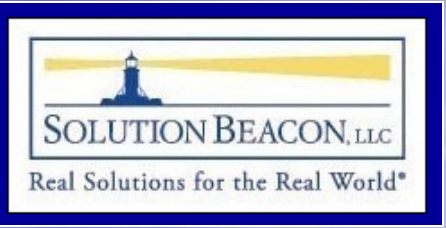
- Default Value = 0 attempts
- Recommendation = 3
- By default, there is no lockout after failed login attempts: This is just asking to be hacked!
- Additional Notes:
  - Implement an alert (periodic), custom workflow or report to notify security administrators of a lockout
  - FND_UNSUCCESSFUL_LOGINS
  - 11.5.10 raises a security exception workflow

Profile: Password Case Option (RUP3)



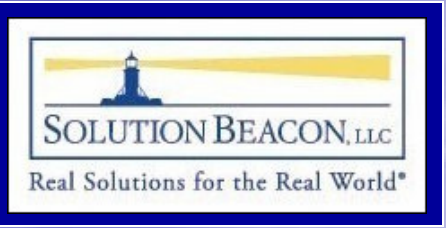
- Enforces case sensitivity for password values:
  - Insensitive
  - Sensitive
  - Mixed
- Introduced in 11i ATG_PF_H RUP3
- 11i ATG_PF_H RUP4 deprecated 'Mixed'

Profile: Signon Password Case (RUP4)



- Enforces case sensitivity for password values:
  - Insensitive
  - Sensitive
  - Mixed
- Introduced as 'Password Case Option' in ATG_PF_H RUP3
- 11i ATG_PF_H RUP4 deprecated 'Mixed'

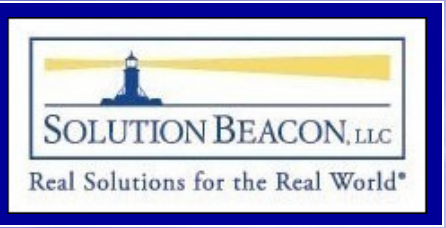
Force Apps User Passwords To Expire



- By default, passwords do not expire
- Define User screen – Password Expiration
  - Days
  - Accesses
  - None (Default)

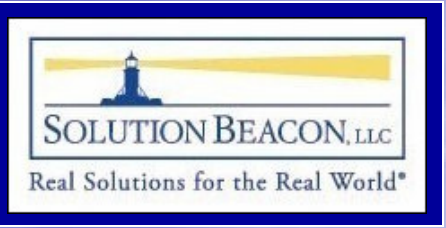
ORACLE CERTIFIED PARTNER

Profile: ICX:Session Timeout



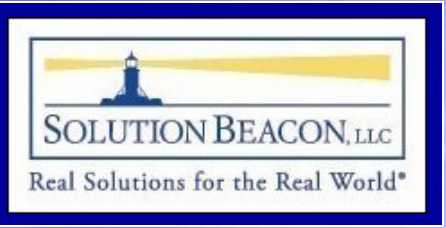
- The length of time (in minutes) of inactivity in a user's form session before the session is *disabled*.
- Default value = none
- Recommendation = 30 (minutes)
- Also set *session.timeout* in *zone.properties*
- Available via Patch 2012308
  (Included in 11.5.7, FND.E)

Change Your System PWs Frequently!



- apps, applsys, gl, ap, ar, etc.
- FNDCPASS - MetaLink Note: 159244.1
- 'ALLORACLE' mode – 11i.ATG_PF.H RUP4
  - Changes all E-Biz Oracle passwords
  - Exception: apps and applsys
  - I don't encourage its use

Notes On Oracle DB Password Values



- If the password is not enclosed in quotes then it can include any letter, any digit, or any of the three following special characters: "_", "#" or "$".
- Only a letter can be used in the first character, the other characters can be used after that.
- It is important to remember that Oracle passwords are not case sensitive so the valid alphabet is reduced by 26 characters. That is "a" is the same as "A".

Release 11*i* Security

Keeping The Badder Guys Away

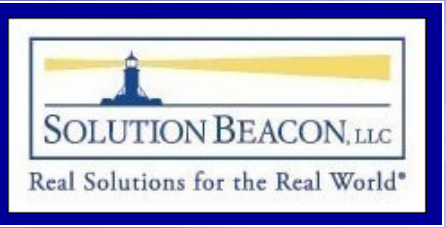
Release 11*i* Workshops

Dallas, TX • San Ramon, CA •
Cincinnati, OH • Denver, CO • Atlanta, GA
Detroit, MI • Las Vegas, NV

www.solutionbeacon.com

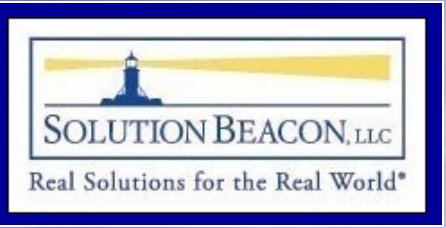
SOLUTION BEACON, LLC
Real Solutions for the Real World®

Minute 31 – Your Next Steps



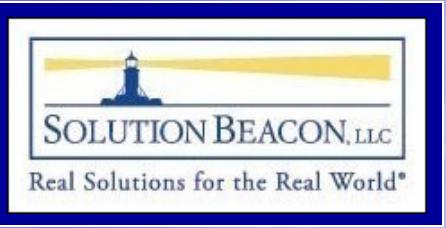
- Be Paranoid!
- Review/Update/Create Security Processes, Procedures and Policies
- Be Proactive – Monitor Security Sources
  - CERT (OS, products, and more)
  - Oracle
- Apply Oracle Critical Patch Updates
  - Quarterly Releases
  - Not Cumulative!

E-Business Suite Critical Patch Update Note 372931.1



- For the October 2006 Critical Patch Update (CPUOct2006), the minimum supported baseline for Oracle E-Business Suite Release 11.5.10.x will be Oracle Applications Technology 11*i*.ATG_PF.H **RUP3** (4334965).
- The 11.5.10 CU2 for ATG Product Family will **not** be a supported baseline for CPUOct2006.
- The minimum supported baseline for all other 11i releases, including 11.5.7, 11.5.8, and 11.5.9, will remain at the patch levels listed in Note 363827.1

E-Business Suite Critical Patch Update Note 372931.1



- Oracle recommends that all Release 11*i* customers uptake Oracle Applications Technology 11*i*.ATG_PF.H Rollup 4 (4676589).
- Beginning with the July 2007 Critical Patch Update (CPUJul2007), Oracle Applications Technology will support only the current and previous production rollups (RUP N and RUP N-1) as patching baselines for all 11*i* releases.

Minute 31 – Your Next Steps (CPU)

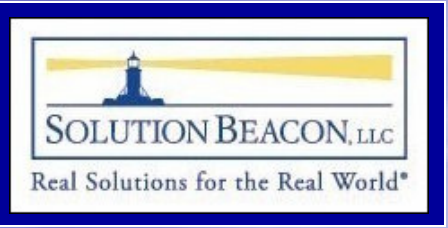
SOLUTION BEACON, LLC
Real Solutions for the Real World®

- Rebaselined ATG Components - 11.5.7 thru .10 (363827.1)
- Prior E-Business Suite Security Alerts (315713.1)
- E-Business Suite Critical Patch Update Note (372931.1)
- Oracle ATG Newsletter - August 2006, Volume 2 (387436.1)
- Old? FAQ Documents (237007.1 and 360470.1)

ORACLE CERTIFIED PARTNER

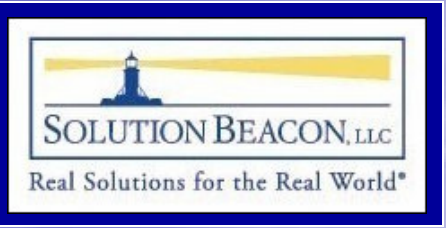
ROAD TO Las Vegas

Minute 31 – Your Next Steps (continued)



- Protect Your Data!
- No Direct Access to Database
  - Only Allowed Via An Application
  - Does not mean that people can't do their job!
  - Reduces the number of attack vectors
  - Implemented via tcp.invited_nodes in sqlnet.ora
  - Oracle's Recommendation
  - MetaLink Note: 277535.1

Minute 31 – Your Next Steps (continued)

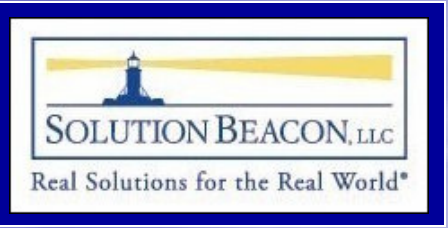


- No Direct Access Example (sqlnet.ora)

```
tcp.validnode_checking = YES
tcp.invited_nodes = (192.168.1.91)
tcp.excluded_nodes = (192.168.1.89, 192.168.1.90)
```

- In a multi-node/server configuration, the E-Business Web Node, Admin Node, Forms Node and Concurrent Processing Node servers would be included in the list of invited nodes, as well as any other administrative or monitoring servers (e.g. Oracle Enterprise Manager).

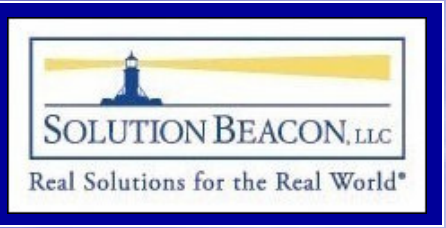
Minute 31 – Your Next Steps (continued)



- Harden Operating System
- Harden Database
- Harden E-Business Suite Tech Stack
- Internal Assessment
- Third Party Assessment
- Continuous Process Improvement

ORACLE CERTIFIED PARTNER

Questions and Answers



Thank you!

Randy Giefer
rgiefer@solutionbeacon.com

www.solutionbeacon.com

Real Solutions for the Real World.®

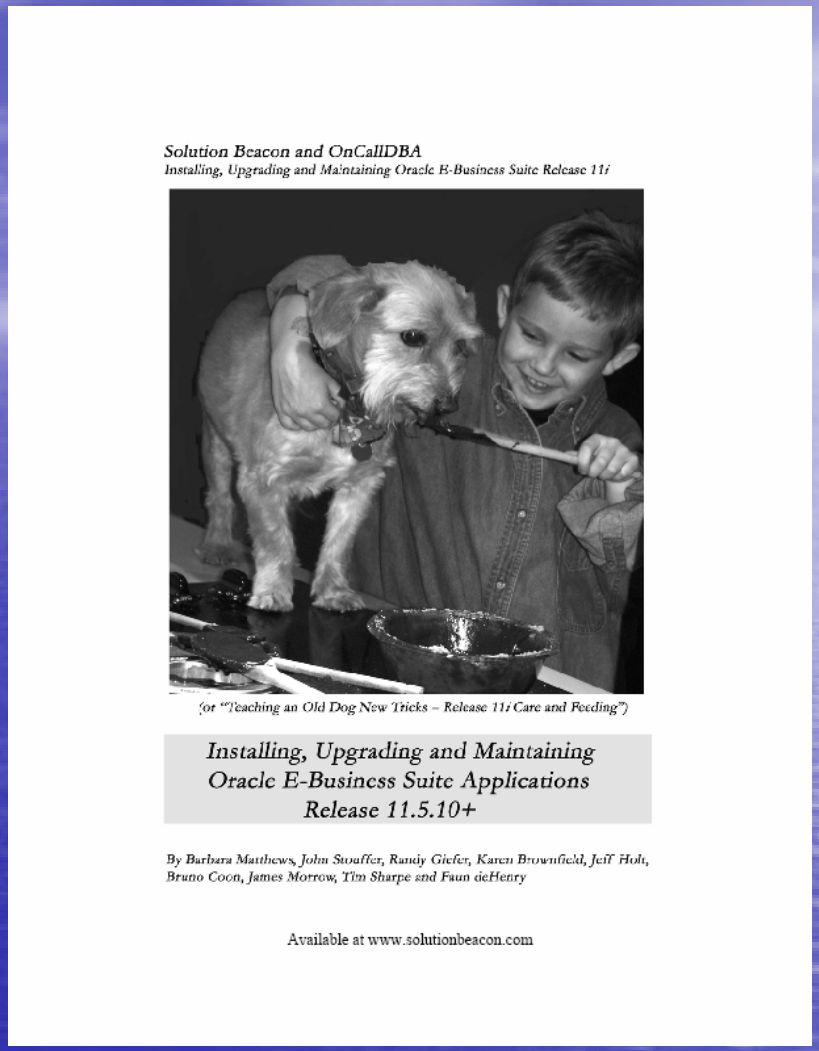
ORACLE CERTIFIED PARTNER

Watch for our new book:

Installing, Upgrading and Maintaining Oracle E-Business Suite Applications 11.5.10.2

It's coming THIS YEAR!

Sign Up For the Solution Beacon Newsletter at www.solutionbeacon.com so you'll be notified when it's available!



Release 11*i* Workshops

Dallas, TX • San Ramon, CA •
Cincinnati, OH • Denver, CO • Atlanta, GA
Detroit, MI • Las Vegas, NV

www.solutionbeacon.com

SOLUTION BEACON, LLC
Real Solutions for the Real World®

ROAD TO Las Vegas