Safe Harbor Statement

THE INFORMATION CONTAINED IN THIS DOCUMENT IS FOR INFORMATIONAL SHARING PURPOSES ONLY, AND SHOULD BE CONSIDERED IN YOUR CAPACITY AS A CUSTOMER ADVISORY BOARD MEMBER OR PURSUANT TO YOUR BETA TRIAL AGREEMENT ONLY. 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 IN THIS DOCUMENT REMAINS AT THE SOLE DISCRETION OF ORACLE.

THIS DOCUMENT IN ANY FORM, SOFTWARE OR PRINTED MATTER, CONTAINS PROPRIETARY INFORMATION THAT IS THE EXCLUSIVE PROPERTY OF ORACLE. YOUR ACCESS TO AND USE OF THIS CONFIDENTIAL MATERIAL IS SUBJECT TO THE TERMS AND CONDITIONS OF YOUR ORACLE SOFTWARE LICENSE AND SERVICE AGREEMENT, WHICH HAS BEEN EXECUTED AND WITH WHICH YOU AGREE TO COMPLY. THIS DOCUMENT AND INFORMATION CONTAINED HEREIN MAY NOT BE DISCLOSED, COPIED, REPRODUCED OR DISTRIBUTED TO ANYONE OUTSIDE ORACLE WITHOUT PRIOR WRITTEN CONSENT OF ORACLE. THIS DOCUMENT IS NOT PART OF YOUR LICENSE AGREEMENT NOR CAN IT BE INCORPORATED INTO ANY CONTRACTUAL AGREEMENT WITH ORACLE OR ITS SUBSIDIARIES OR AFFILIATES.
Enterprise Communications Innovation Themes

**Service Provider**

- **Public Cloud**
  Viability in market leading public clouds.

- **Price / Performance**
  New platforms with improved price to performance and feature ratios (AP3900, AP4600)

- **Compliance Recording**
  On-premise & Oracle Cloud-based session recording

- **Intelligent Edge**
  SD-WAN (Software Defined WAN) via Oracle Cloud

**Enterprise**

- **Advanced Security & Compliance**
  Government Grade: FIPS (data integrity) and JlTC (admin security); PCI Compliance Solutions

- **Enterprise NFV**
  Improved capacity, Expanded hypervisor support, Orchestration

- **Unified Management**
  Industry leading ease-of-use; cross-product configuration, monitoring and management

- **SMB & Branch Offices**
  AP1100 Features to future proof investments and build platform for IP transformation

- **Fraud Prevention**
  Network pattern detection: black/whitelisting rate limiting, redirection and alerting

**Unified Communications**

- **Microsoft & Skype® for Business**
  Certifications to ensure ease of integration and interoperability; Monitoring of SfB sessions; Hyper-V

- **Communications-as-a-Platform (Omnimodal)**
  “More-than-voice” interworking: presence, video recording, MSRP, screen capture, WebRTC etc.; REST APIs

- **Oracle Communications**
  Customer Advisory Board

**Oracle NFV**

- **Improved capacity, Expanded hypervisor support, Orchestration**

**Oracle Compliance to ensure ease of integration and interoperability; Monitoring of SfB sessions; Hyper-V**

**Oracle Communications**

- **Customer Advisory Board**
Skype for Business
Microsoft Initiatives

• Release R1 will officially be certified with Skype for Business
• Cloud Connect Edition (CCE)
  – Transition from on premise to Office 365
  – Formal certification
• Hyper-V support
PCI Compliance
Business Drivers For PCI

- 169 Million: Reported records exposed in US from data breaches in 2015
- 69%: of consumers would be less inclined to do business with a breached organization
- 45%: of Americans have been notified that their credit card info has possible been stolen
- 72%: of organizations that suffer a major data loss shut down within 24 months.
- No. 1: 25.5% of Worldwide data attacks occur in the US.
- 47: out of 50 states require organizations to notify their potentially impacted customers following a data breach.

Oracle Communications
Customer Advisory Board
Role Of Oracle ESBC In PCI

- DTMF suppression support
- DTMF format conversion that is necessary for 3rd party processing system like Semafone
  - Fully validated by Oracle & Semafone and interop tech note now available
Enterprise Network Function Virtualization (ENFV)
## Market Analyst Data on NFV

<table>
<thead>
<tr>
<th>Year</th>
<th>Key Event</th>
<th>NFV Use Cases</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015</td>
<td>Live Network Trials</td>
<td>Enterprise <strong>Collaboration</strong> and <strong>Unified Communications</strong> are among the top NFV use cases*</td>
</tr>
<tr>
<td>2016</td>
<td>Proof of Concept</td>
<td></td>
</tr>
<tr>
<td>2017</td>
<td>Deployed VNFs*</td>
<td></td>
</tr>
</tbody>
</table>

86% of medium to large Enterprises will deploy NFV in some aspect of their network*  
34% within the next 1-2 yrs  
62% within the next 2-5 yrs

*HEAVY READING’S NFV Survey, January 2016  
*INFONETICS RESEARCH SDN and NFV Strategies, March 2016
Virtualization

• Additional Hypervisor support
• Improved performance using Intel DPDK libraries
• Oracle Next Generation Contact Center (NGCC)
Network Wide Licensing (NWL) Model

- The Network-wide licensing model allows customers to share licenses across multiple Oracle Enterprise Session Border Controllers (OESBC).
- These licenses are perpetual and hence can be moved to newer platforms beyond the end of life of the existing platforms.
- The customers can share these licenses across different type of platforms for e.g. VME, 1100, 3900, 4600 and 6300.
- The customers can mix and match ISO and NWL on the same box.
- No ‘Base’ license required with Network-wide licensing model.
Session Mobility & Base Impact Across License Models

ISO MODEL

<table>
<thead>
<tr>
<th>ENT Base ($7500)</th>
<th>SMB Base ($500)</th>
</tr>
</thead>
<tbody>
<tr>
<td># Sessions (non transferable)</td>
<td># Sessions (non transferable)</td>
</tr>
</tbody>
</table>

- 12% Support – 4600/6300
- 12% Support – 3900
- 5% Support – 4600/6300

- 12% Support – 4600/6300
- 12% Support – 1100/3900
- 5% Support – 4600/6300

NETWORK WIDE

<table>
<thead>
<tr>
<th>Platform</th>
<th>Platform</th>
</tr>
</thead>
</table>

- 22% Support
- # Sessions
- 22% Support
- # Sessions

- 5% Support – 4600/6300
- 12% Support – 1100/3900
- 12% Support – 1100/3900

Oracle Communications
Customer Advisory Board
REST APIs

Fraud
- Real-time detection
- Dynamic call to actions

Contact Centre
- 3rd party call control
- Call reconnect

Others
- Real time communications on Service cloud

Oracle Communications
Customer Advisory Board
Advanced Security

March 2017

Madhu Mathiyalagan
Enterprise Product Management & Strategy
Session Delivery Products
Safe Harbor Statement

THE INFORMATION CONTAINED IN THIS DOCUMENT IS FOR INFORMATIONAL SHARING PURPOSES ONLY, AND SHOULD BE CONSIDERED IN YOUR CAPACITY AS A CUSTOMER ADVISORY BOARD MEMBER OR PURSUANT TO YOUR BETA TRIAL AGREEMENT ONLY. 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 IN THIS DOCUMENT REMAINS AT THE SOLE DISCRETION OF ORACLE.

THIS DOCUMENT IN ANY FORM, SOFTWARE OR PRINTED MATTER, CONTAINS PROPRIETARY INFORMATION THAT IS THE EXCLUSIVE PROPERTY OF ORACLE. YOUR ACCESS TO AND USE OF THIS CONFIDENTIAL MATERIAL IS SUBJECT TO THE TERMS AND CONDITIONS OF YOUR ORACLE SOFTWARE LICENSE AND SERVICE AGREEMENT, WHICH HAS BEEN EXECUTED AND WITH WHICH YOU AGREE TO COMPLY. THIS DOCUMENT AND INFORMATION CONTAINED HEREIN MAY NOT BE DISCLOSED, COPIED, REPRODUCED OR DISTRIBUTED TO ANYONE OUTSIDE ORACLE WITHOUT PRIOR WRITTEN CONSENT OF ORACLE. THIS DOCUMENT IS NOT PART OF YOUR LICENSE AGREEMENT NOR CAN IT BE INCORPORATED INTO ANY CONTRACTUAL AGREEMENT WITH ORACLE OR ITS SUBSIDIARIES OR AFFILIATES.
Key Drivers of Government Grade Security

Federal Information Processing Standard (FIPS) 140-2
- Compliant implementations of SIP-TLS, IPsec, SSH and SFTP

DISA Joint Interoperability Test Command (JITC)
- Security across all external interfaces sufficient for operation as a standalone network border device

Data Integrity

Admin Security
Data Integrity

- Crypto Validation
- Image Integrity
- Physical Security
- Conditional Test
- Power on Self Test

FIPS 140-2 Cert
Cryptography Validation

- U.S. government standard that describes the encryption and related security requirements that IT products should meet for sensitive, but unclassified use.
- Approved for protecting classified information.
- Suite B algorithms were designed to resist all known cryptographic attacks.
  - AES-256, SHA-384, 384-bit ECDH, 384-bit ECDSA.
Self Tests

• Power on self test are performed when cryptographic module powers up
  • AES
  • HMAC
  • 3DES
  • Hashing
• Conditional self test are performed when RSA or RNG operation is required
• Non-compatible mode
• TLS and SSH connections are failed
• Security related ACLI config elements are not available
• Security related ACLI commands are not allowed
Software Integrity Test

• This verifies the bootable software image
• Software image cannot be bootable externally
FIPS 140-2 Levels of Security

- The FIPS 140-2 standard provides four increasing, qualitative levels of security, from 1 to 4 (1 being the lowest) – Oracle Enterprise SBC is compliant with level 2
- Level 2: Tamper evident physical security or pick resistant locks. Level 2 also provides for role-based authentication
Administrative Security

Password Policy
- Strengthen length, history
- Re-use policy
- Expiration

Audit Log
- Permission to access logs
- Logs are pushed out at regular interval

Login Policy
- Concurrent System access
- Lockout interval
- Authentication mode

Refined User Roles
- TACACS+ Authentication
- RADIUS Authentication

Deny any Insecure Access
- No shell access
- Any insecure ports like telnet, ftp, http are all locked
Enterprise SBC Advanced Security

FIPS 140-2

Data Integrity

Admin Security

Platinum Suite

JITC