"Channeling a little Oracle Open World"

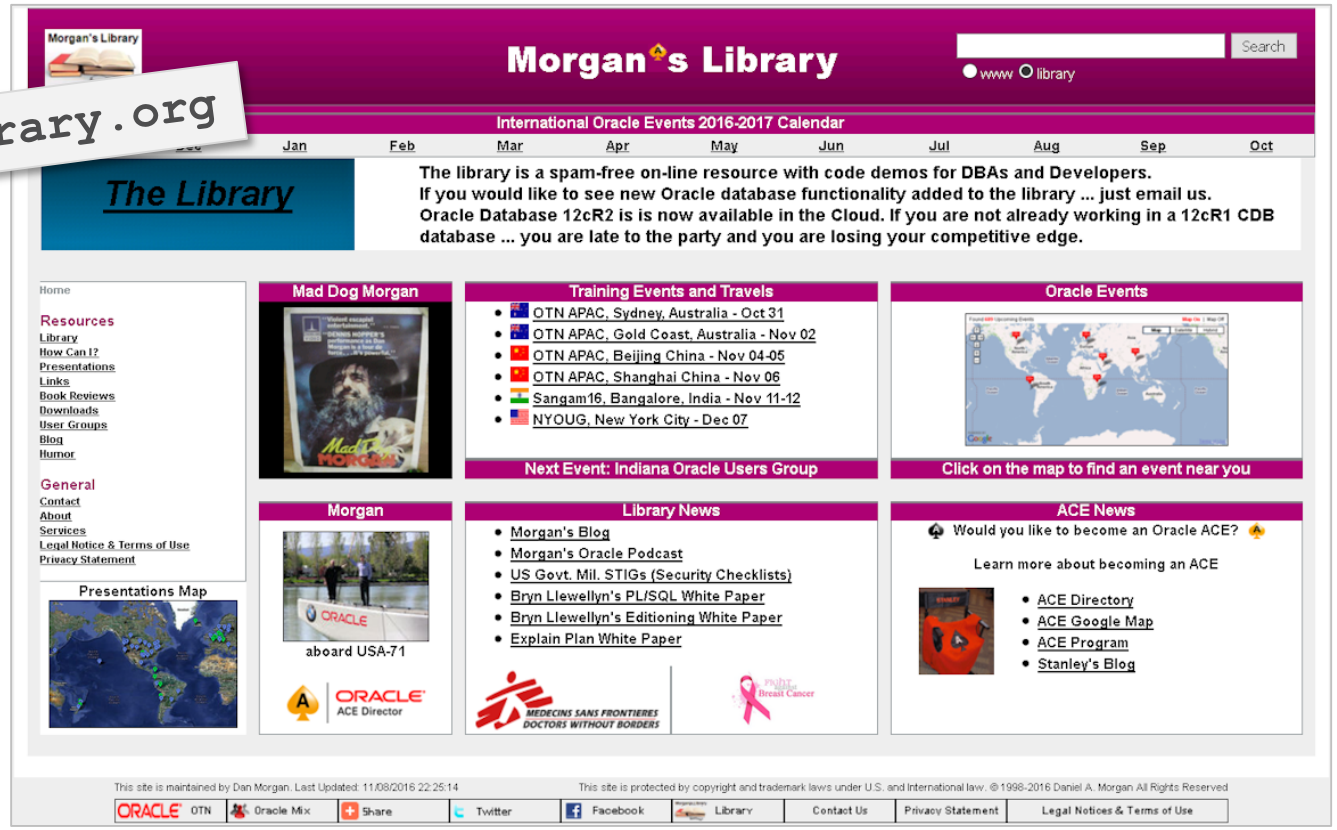
Seattle Training Day 2018

Tuesday: March 6, 2018

A Quick Introduction

- Oracle ACE Director Alumnus
- Curriculum author and primary program instructor at University of Washington
- Consultant: Harvard University
- Principal Adviser: **Meta7** a Sirius Company

www.morganslibrary.org



Meta7 In Forbes Magazine

ForbesBrandVoice® What is this?

JAN 15, 2018 @ 05:00 AM 20,020

3 Essential DBA Career Priorities For 2018

OracleVoice

Simplify IT, Drive Innovation FULL BIO

Jeff Erickson, Oracle

Many database administrators (DBAs) will go into 2018 wondering if "self-driving" databases will weaken their career prospects. More likely, 2018 will be a year that database technology leaps forward and these valuable data experts take on other, more important responsibilities.

"History is repeating itself," says longtime DBA Dan Morgan, founder of Morgan's Library and principal adviser at tech firm Meta7. Morgan has seen the DBA role evolve amid a long series of technical advances in storage, management, and performance. And each advance asked DBAs to adjust the way they work.

When I was growing up my parents taught me to not just pay attention to what was said ...

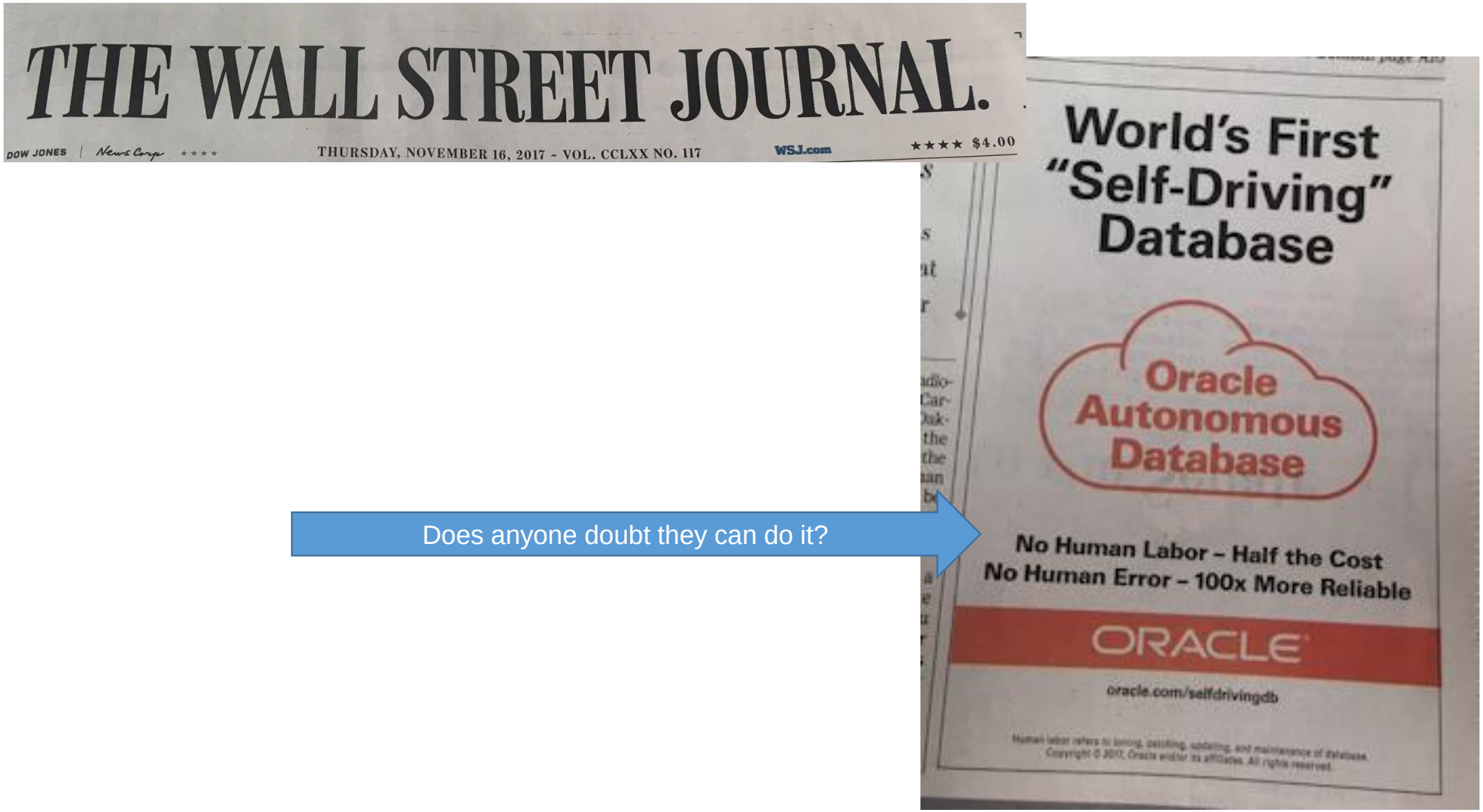
But to pay attention to what was not said

What "should have been said" but was not

If Maxwell House Coffee is "good to the last drop"

Perhaps you shouldn't drink that last drop?

Perhaps We Should Apply That Lesson To Oracle



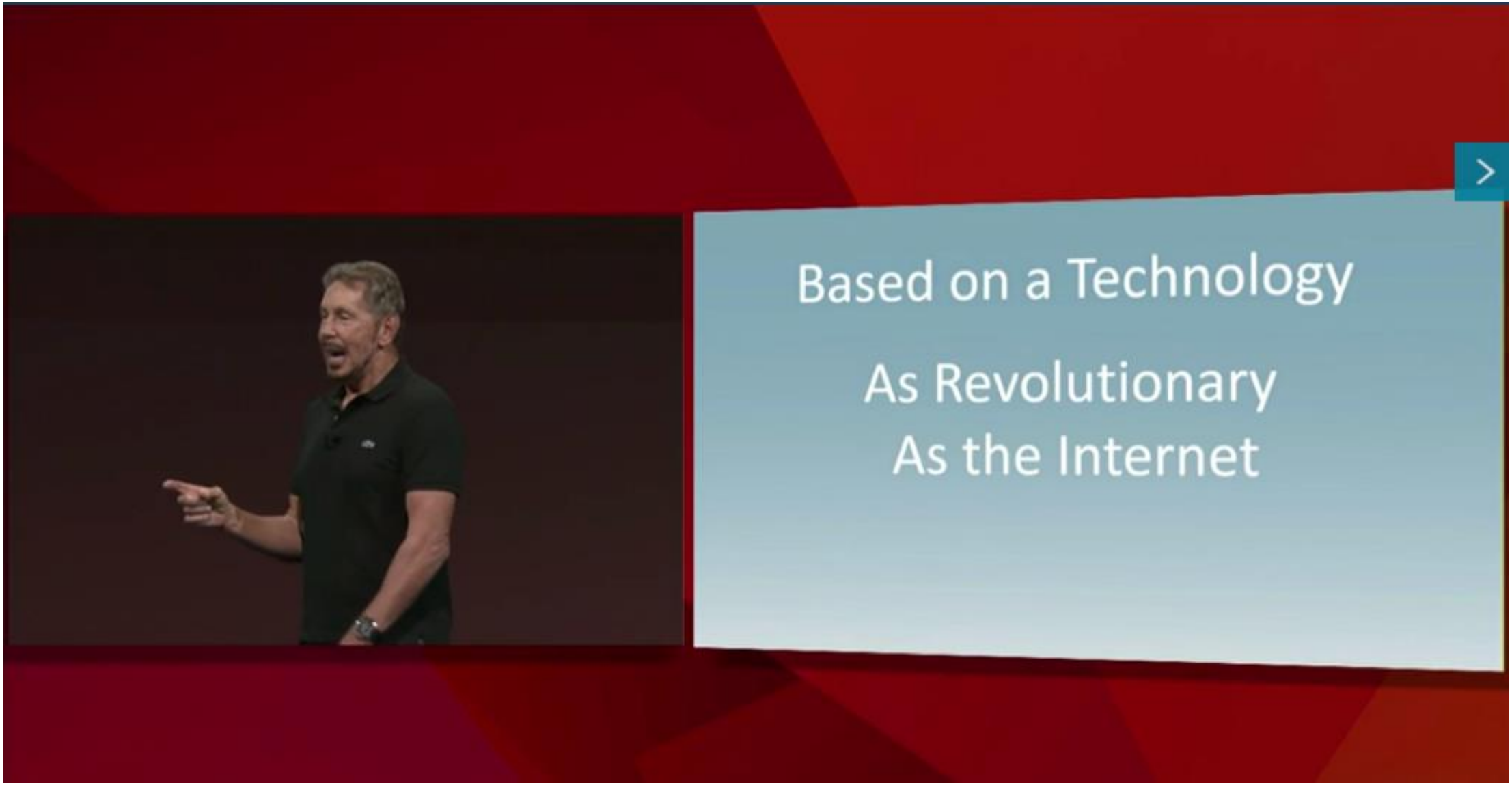
Does anyone doubt they can do it?

Channeling Oracle OpenWorld 2017

META7™


Oracle Autonomous Database
and
Highly Automated Cyber Defense
Larry Ellison
Chief Technology Officer
Robots
Prevent Data Theft
ORACLE

META7™



META7™

The Threat Map (1:3)

There are a variety of threats to our data, our databases, and our organizations

We have been dealing with these issues for decades

- Stability
- Security
- Scalability
- Performance

The Threat Map (2:3)

The solution Oracle has chosen is Machine Learning

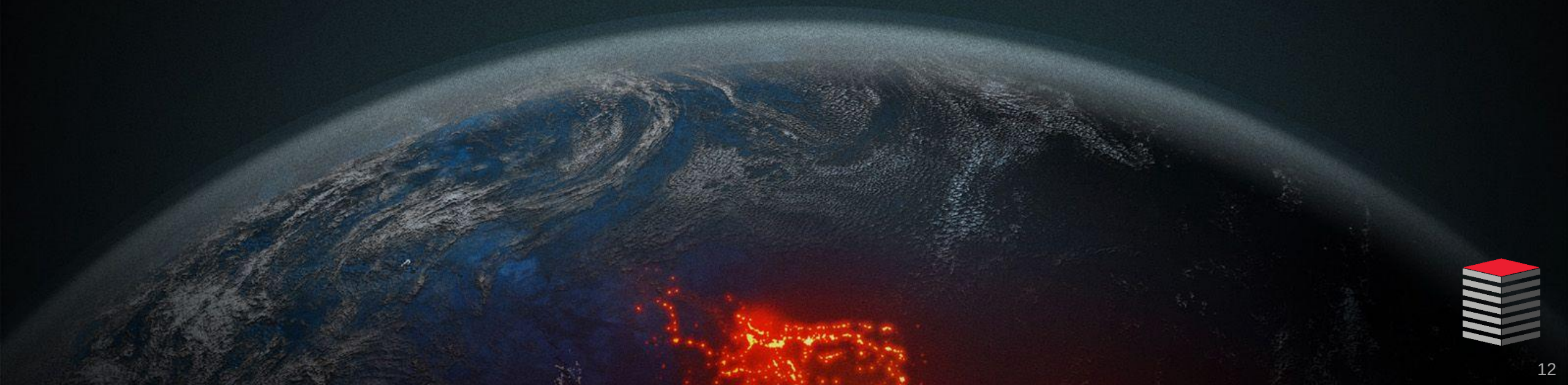
- Not Artificial Intelligence ... but "Machine Learning"
- "We do everything we can to avoid human intervention" (L/E)

The "cold war" has moved from the military to our computers

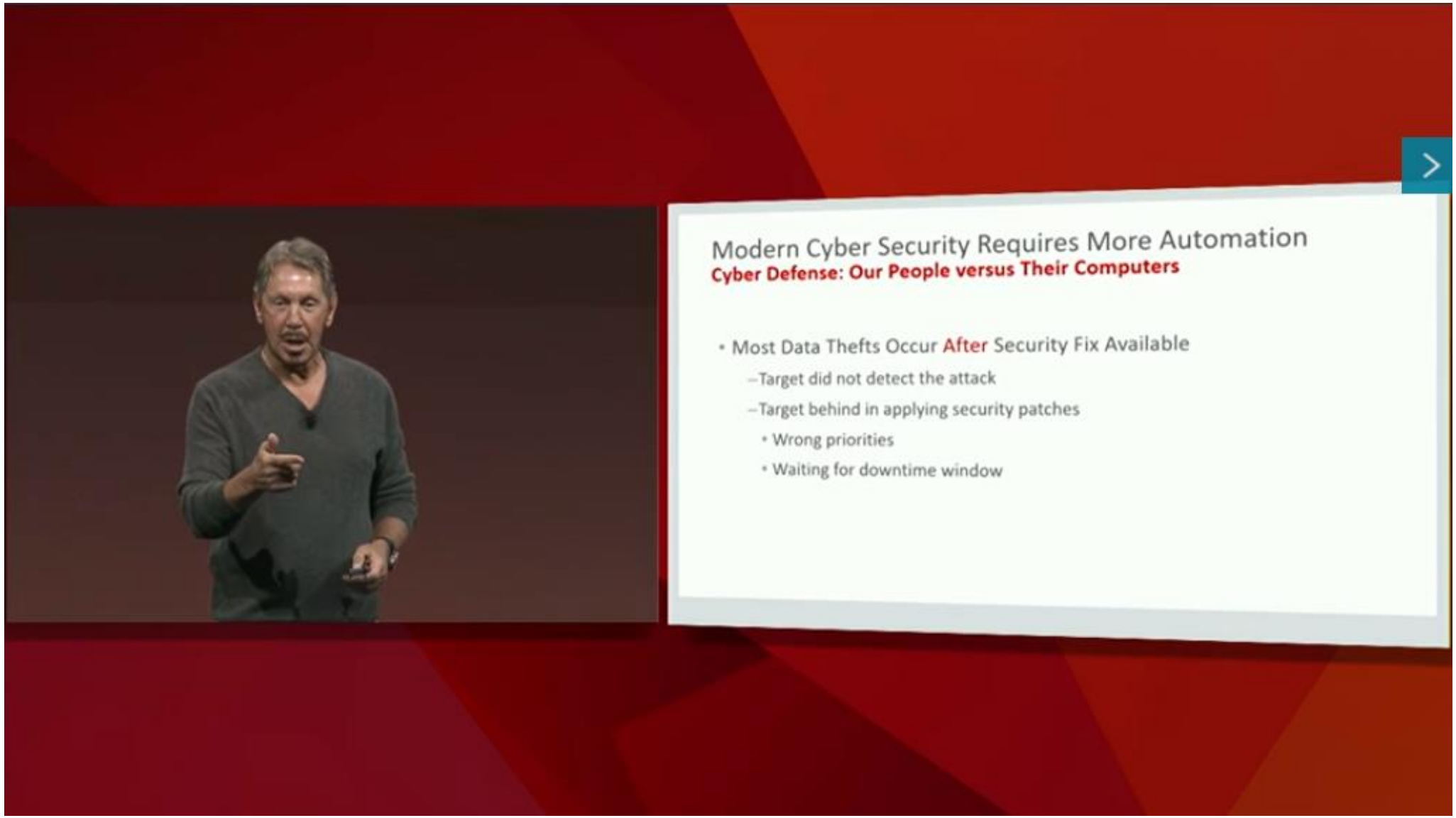
We are the front line ... and while there is no blood and there aren't any burning buildings ... make no mistake about it ... this is escalating, and our ability to pretend that we are not on the front, line is evaporating

CYBER WAR

A conflict without foot soldiers, guns, or missiles



Our People versus Their Computers



It Must Be "Our Computers" vs "Their Computers"

Anyone want to play chess with Deep Blue?

Anyone want to take a shot at AlphaGo?

The Threat Map (3:3)

The threat is not a bunch of 20 year old script kiddies

If the threat is an organized crime family you will find your data being sold on the dark web

If the threat is a nation-state you will find your data being used to attack your country, your community, your family

Pay Attention To What's Not Being Said

Has any organizations that was the target of a major breach failed an audit?

Has any organization that was the target of a major breach configured all default security options?

Has any organization that was the target of a major breach applied all available and relevant security patches?

The Way We Patch Systems is a Guarantee of Failure

Most data thefts have occurred after a patch was available

Because we all know we do not patch quickly

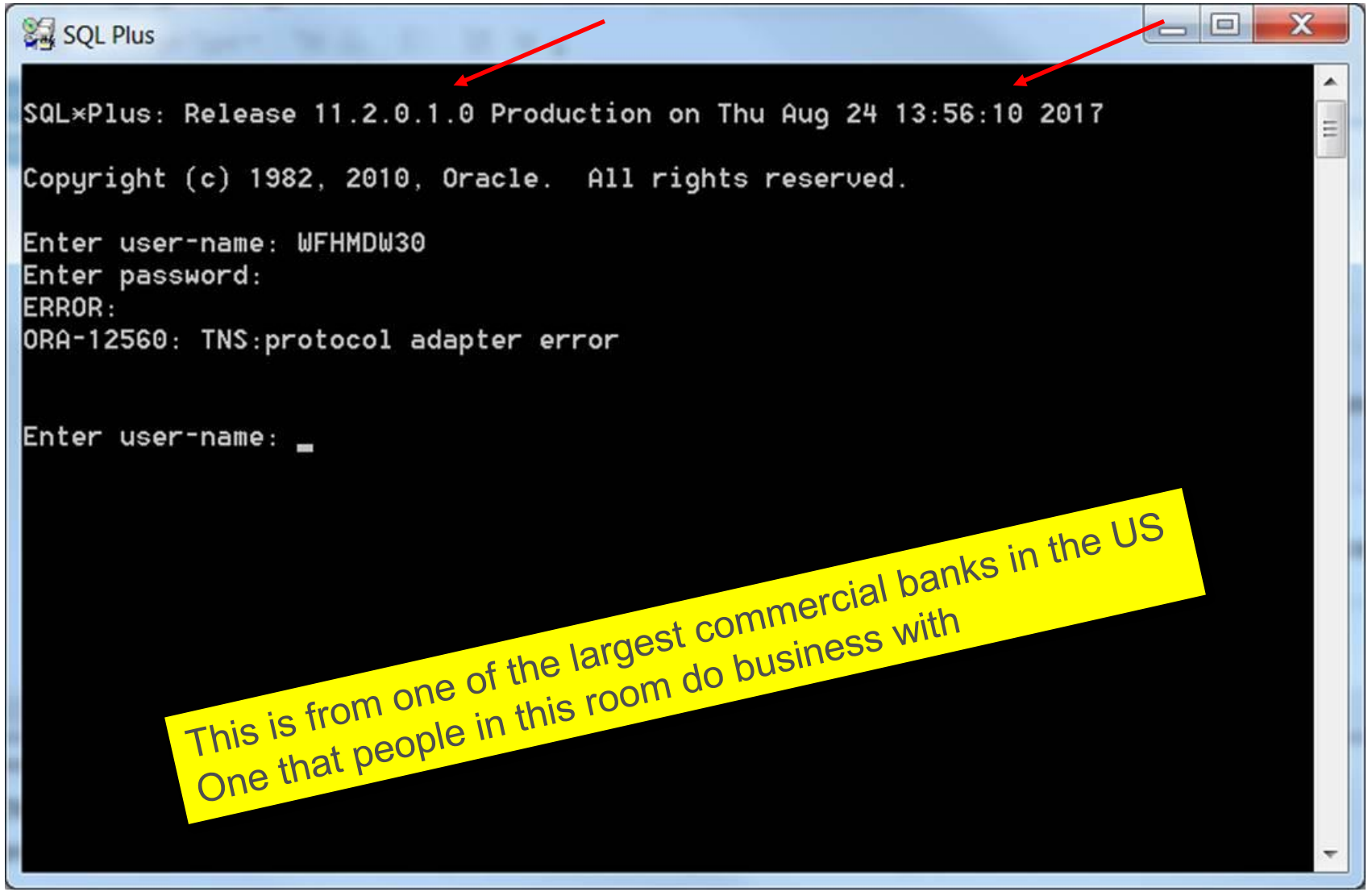
Patching is never a top priority for our employers

To win we must Patch

- The instant the patch is available
- The instant the database detects a threat

Scheduling outages and patching guarantees failure

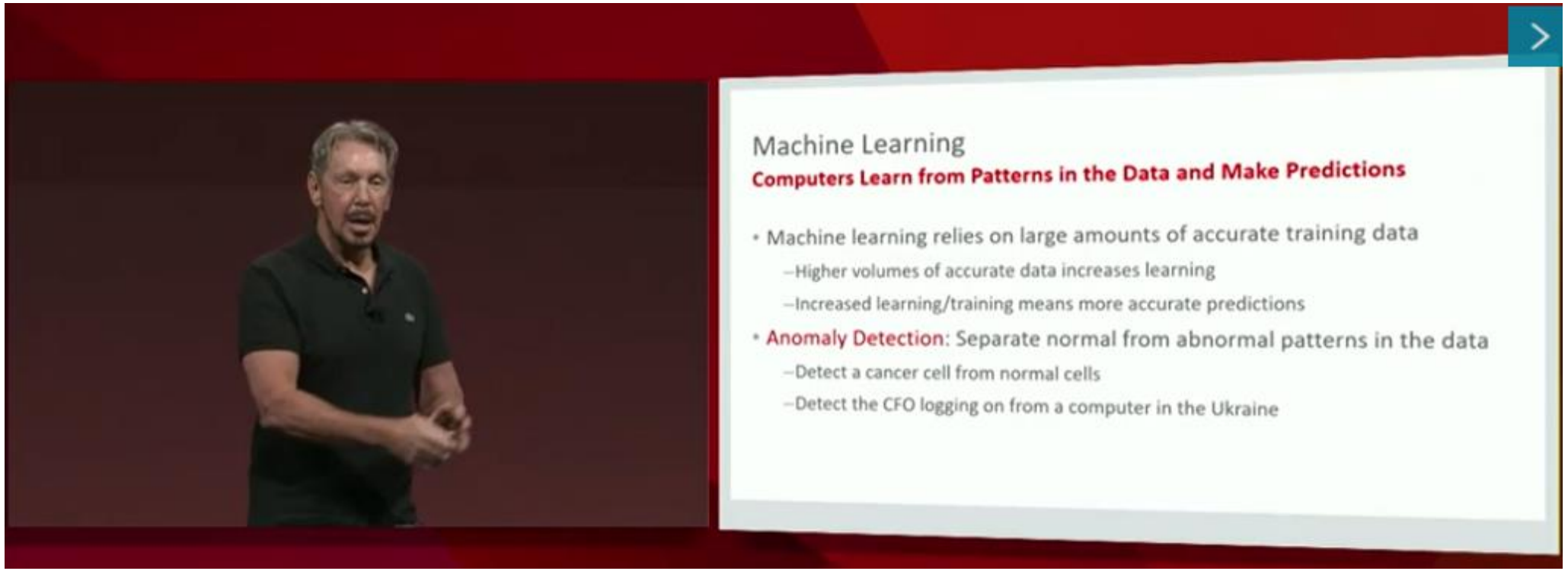
Must I Prove The Point



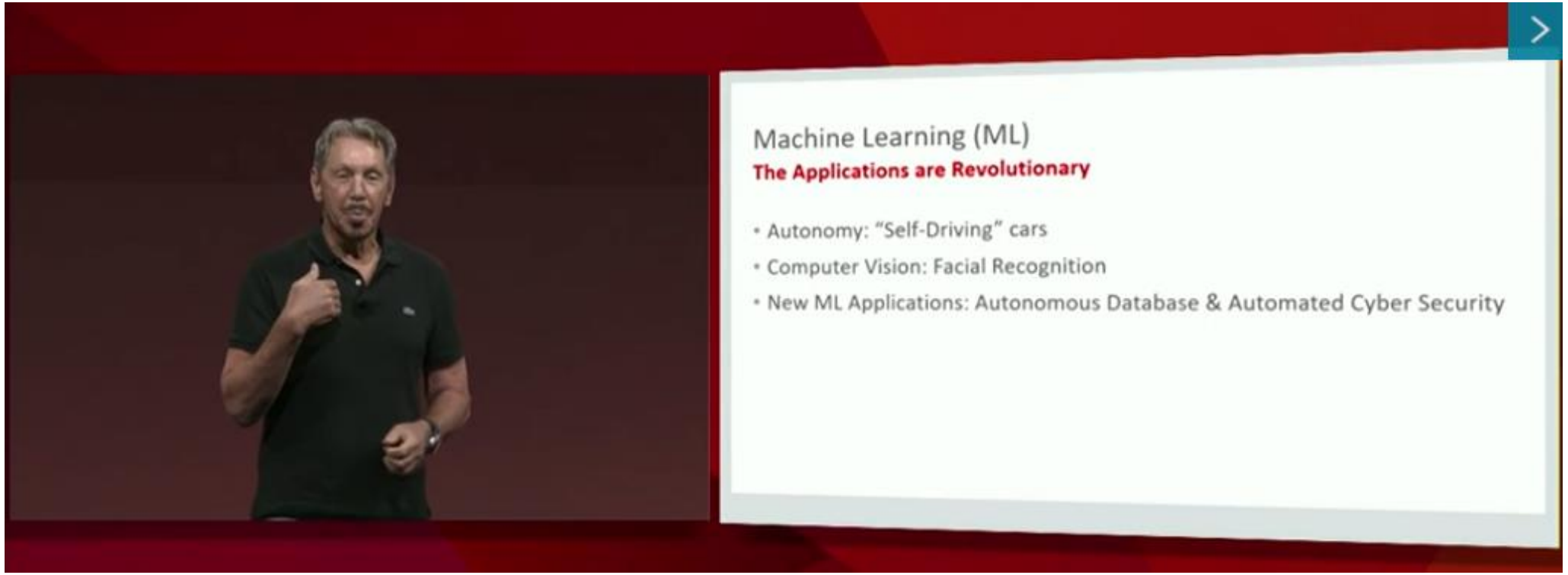
Cyber Criminals Are Winning

More Automation is Required

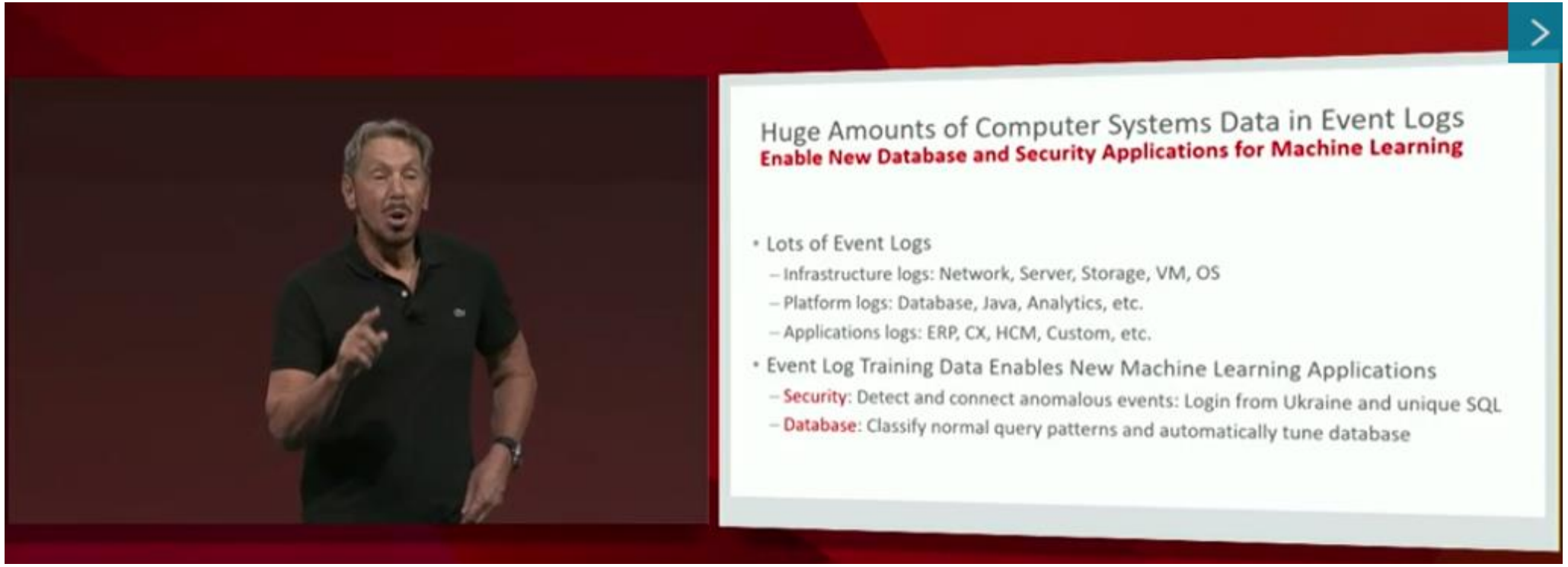
Machine Learning (1:2)



Machine Learning (2:2)

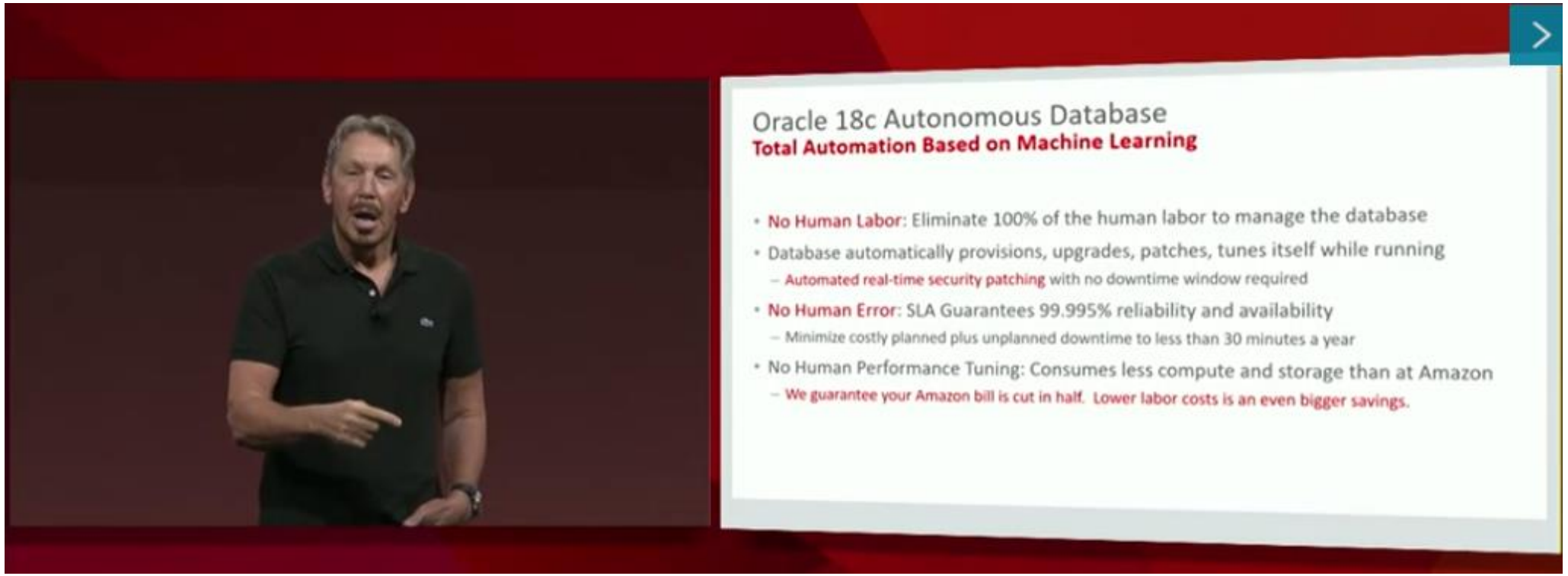


Log File Mining



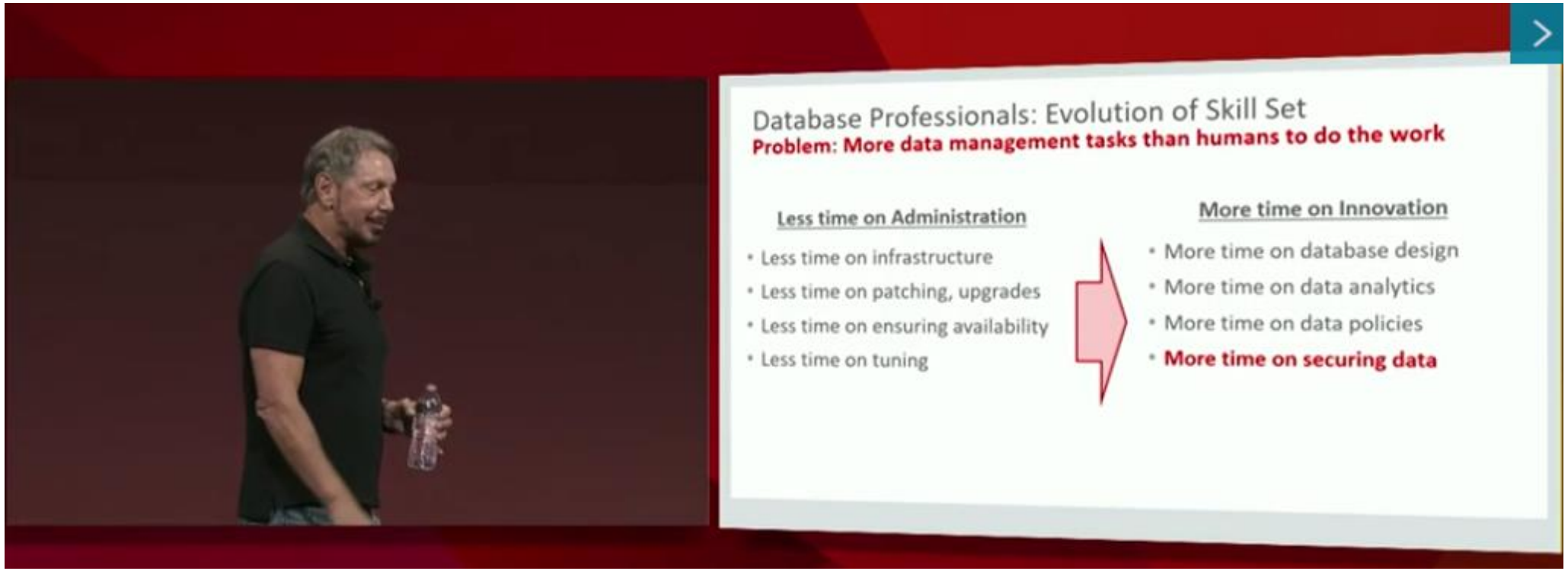
Automated Attack Remediation

Our Careers (1:3)

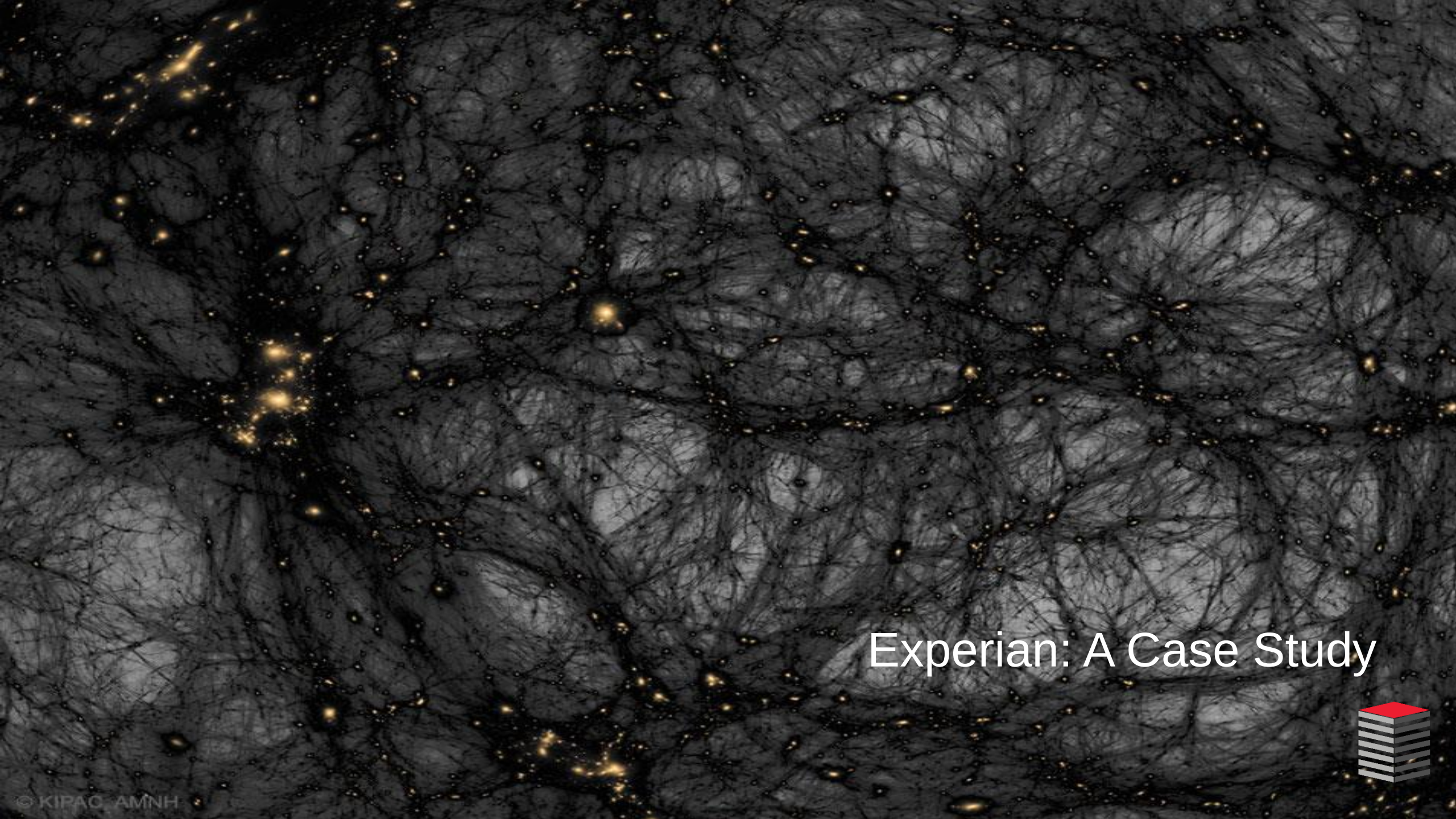


Our Careers (2:3)

Our Careers (3:3)

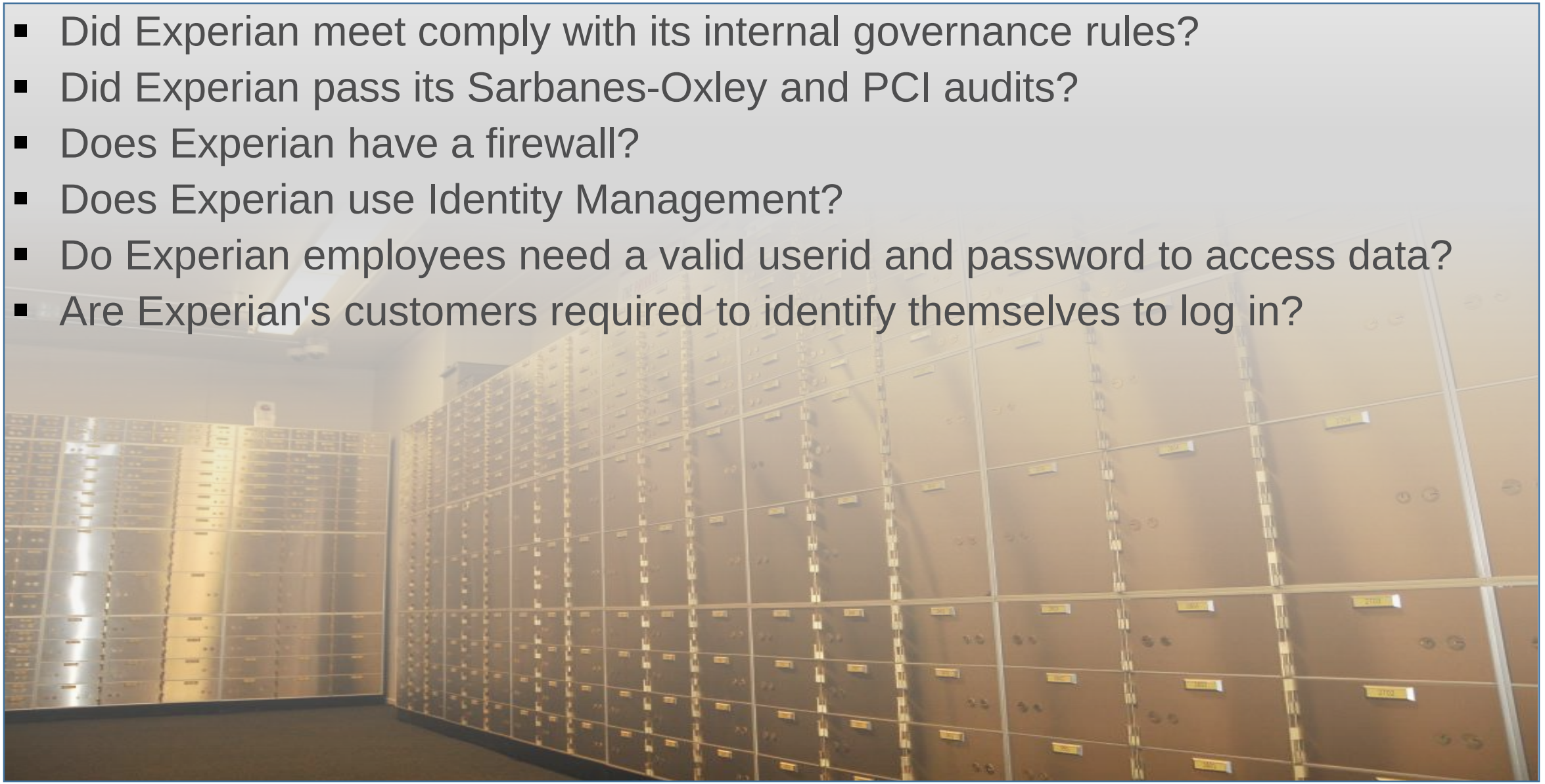


Experian: A Case Study



Are You The Next Experian? (1:5)

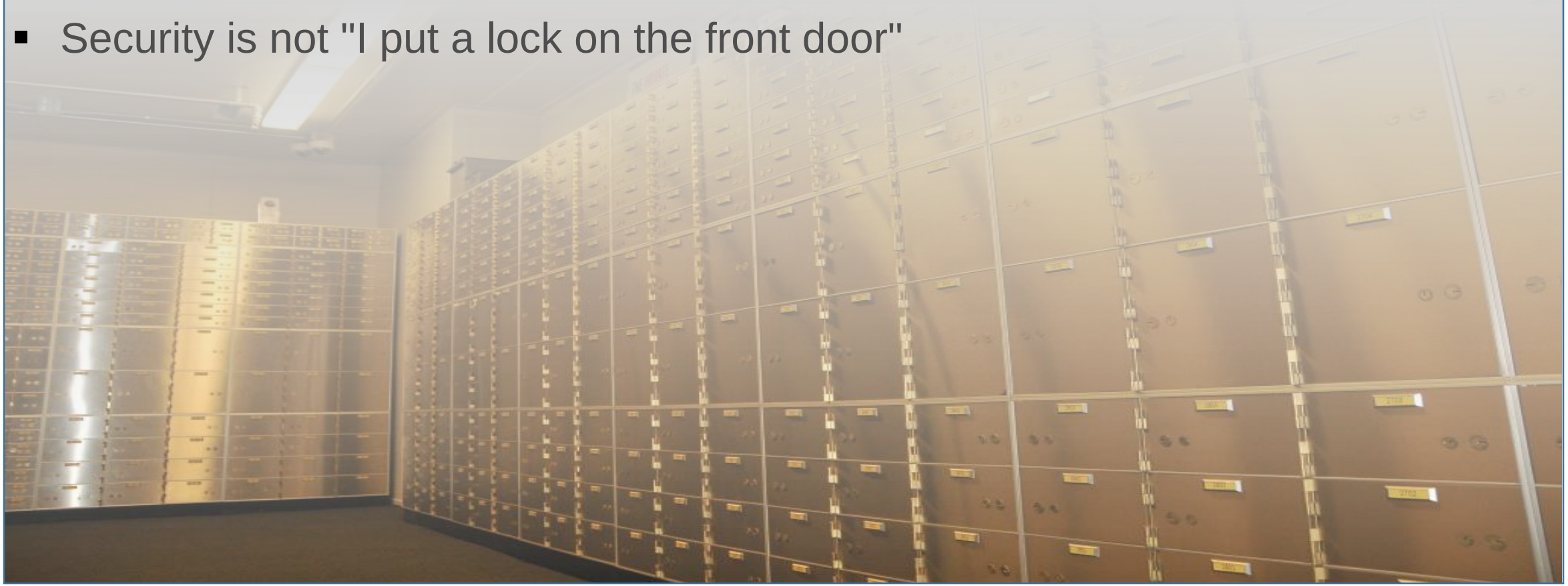
- Did Experian meet comply with its internal governance rules?
- Did Experian pass its Sarbanes-Oxley and PCI audits?
- Does Experian have a firewall?
- Does Experian use Identity Management?
- Do Experian employees need a valid userid and password to access data?
- Are Experian's customers required to identify themselves to log in?



META7™

Are You The Next Experian? (2:5)

- According to Experian an Apache Struts patching failure allowed the theft of data from 145,000,000 people some of whom are sitting in this room
- Do you believe Experian?
- I don't
- Security is not "I put a lock on the front door"

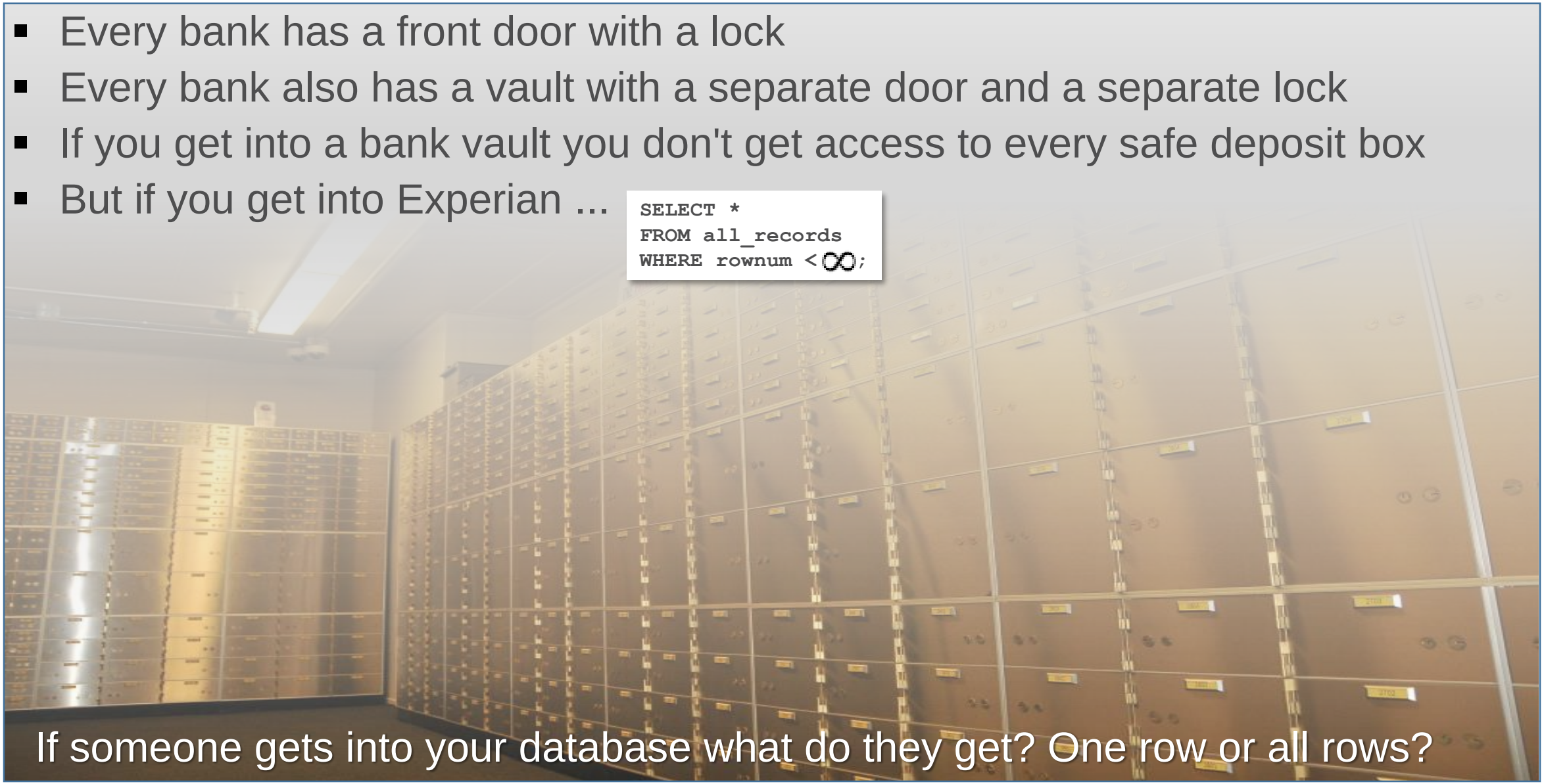


META7™

Are You The Next Experian? (3:5)

- Every bank has a front door with a lock
- Every bank also has a vault with a separate door and a separate lock
- If you get into a bank vault you don't get access to every safe deposit box
- But if you get into Experian ...

```
SELECT *
FROM all_records
WHERE rownum <∞;
```

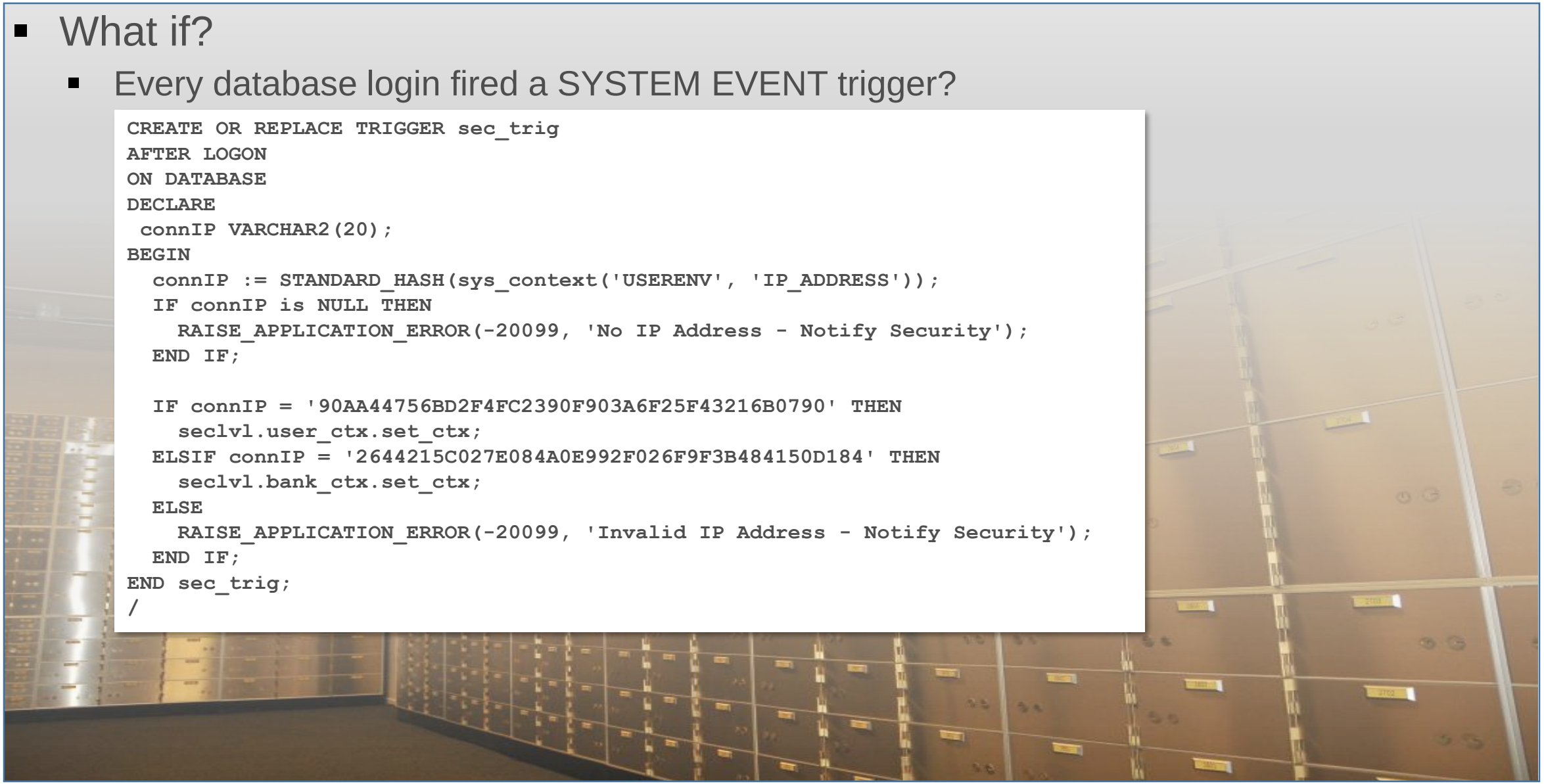


Are You The Next Experian? (4:5)

- What if?
  - Every database login fired a SYSTEM EVENT trigger?

```
CREATE OR REPLACE TRIGGER sec_trig
AFTER LOGON
ON DATABASE
DECLARE
 connIP VARCHAR2(20);
BEGIN
  connIP := STANDARD_HASH(sys_context('USERENV', 'IP_ADDRESS'));
  IF connIP is NULL THEN
    RAISE_APPLICATION_ERROR(-20099, 'No IP Address - Notify Security');
  END IF;

  IF connIP = '90AA44756BD2F4FC2390F903A6F25F43216B0790' THEN
    seclvl.user_ctx.set_ctx;
  ELSIF connIP = '2644215C027E084A0E992F026F9F3B484150D184' THEN
    seclvl.bank_ctx.set_ctx;
  ELSE
    RAISE_APPLICATION_ERROR(-20099, 'Invalid IP Address - Notify Security');
  END IF;
END sec_trig;
/
```



META7™

Are You The Next Experian? (5:5)

- And every user access had a Row Level Security policy?

```
exec dbms_rls.add_policy(USER, 'CREDIT_RPT_VIEW', 'USER_VIEW_POLICY', USER, 'credit_sec.user_sec', 'SELECT');
exec dbms_rls.add_policy(USER, 'CREDIT_RPT_VIEW', 'BANK_VIEW_POLICY', USER, 'credit_sec.bank_sec', 'SELECT');
```

- And every access request was row limited by the context?

```
CREATE OR REPLACE PACKAGE credit_sec AS
 FUNCTION user_sec(owner VARCHAR2, objname VARCHAR2) RETURN VARCHAR2;
 FUNCTION bank_sec(owner VARCHAR2, objname VARCHAR2) RETURN VARCHAR2;
END credit_sec;
/
```

- And the user_sec function did this

```
 IF (sys_context('credit_rpt', 'user_role') = 'USER') THEN
    predicate := 'rownum <= 1';
  ELSE
    predicate := '1 = 2';
  END IF;
  RETURN predicate;
```

- Or this

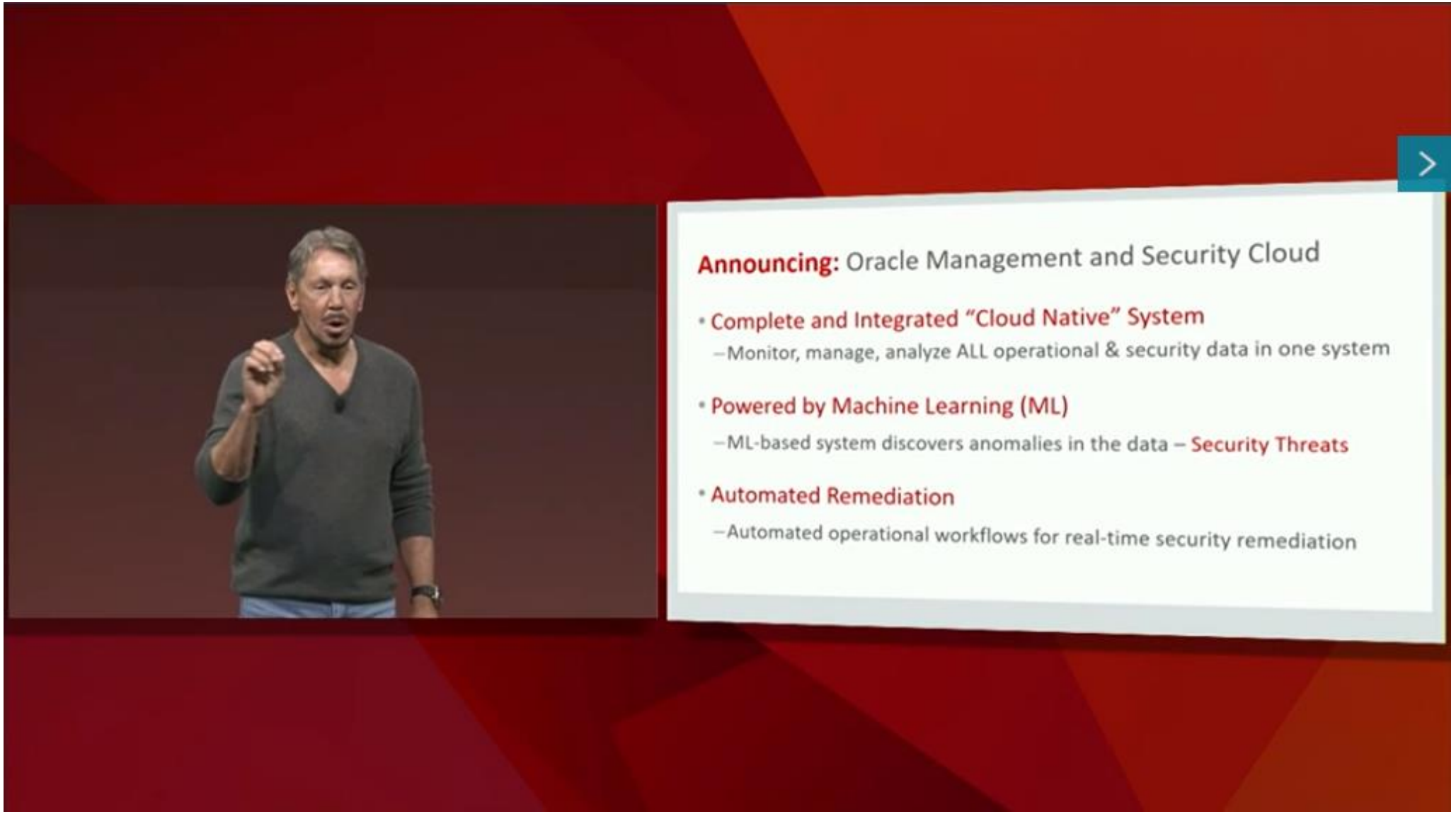
```
 IF (sys_context('credit_rpt', 'user_role') = 'BANK') THEN
    predicate := 'rownum <= 10001';
  ELSE
    predicate := '1 = 2';
  END IF;
  RETURN predicate;
```

Could someone steal 145,000,000 rows?

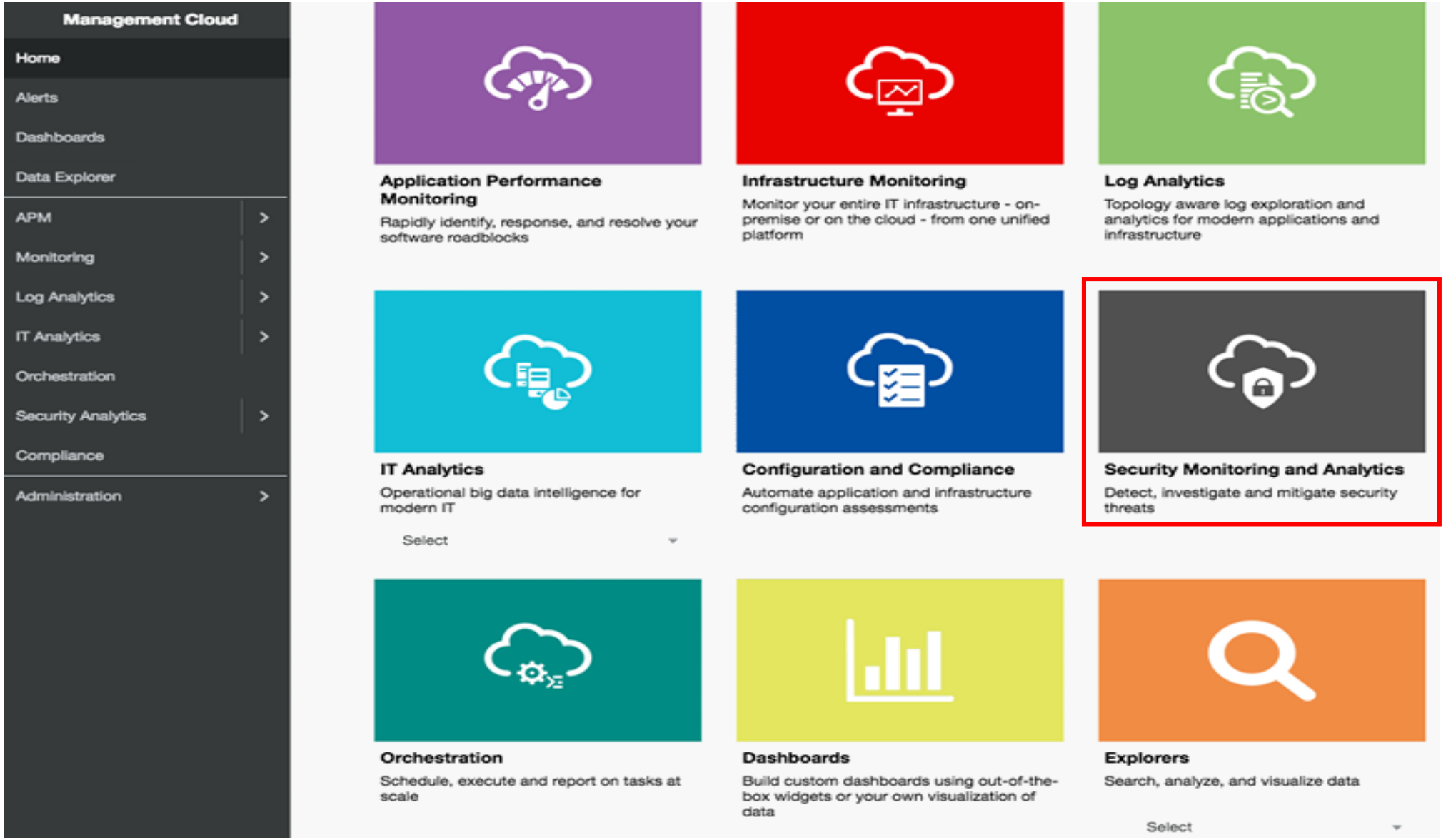
META7™

Security in the Cloud

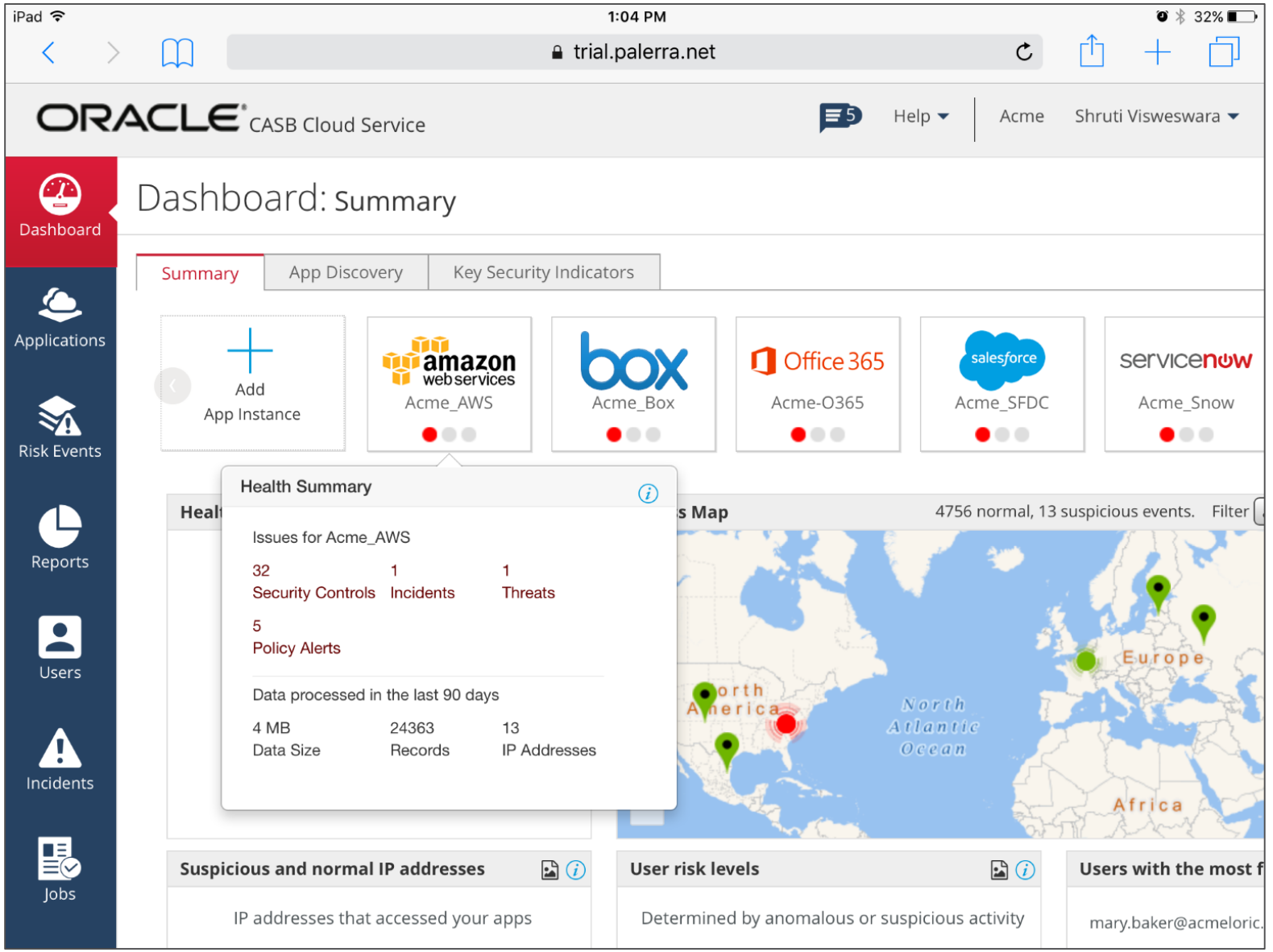
Oracle Management & Security Cloud



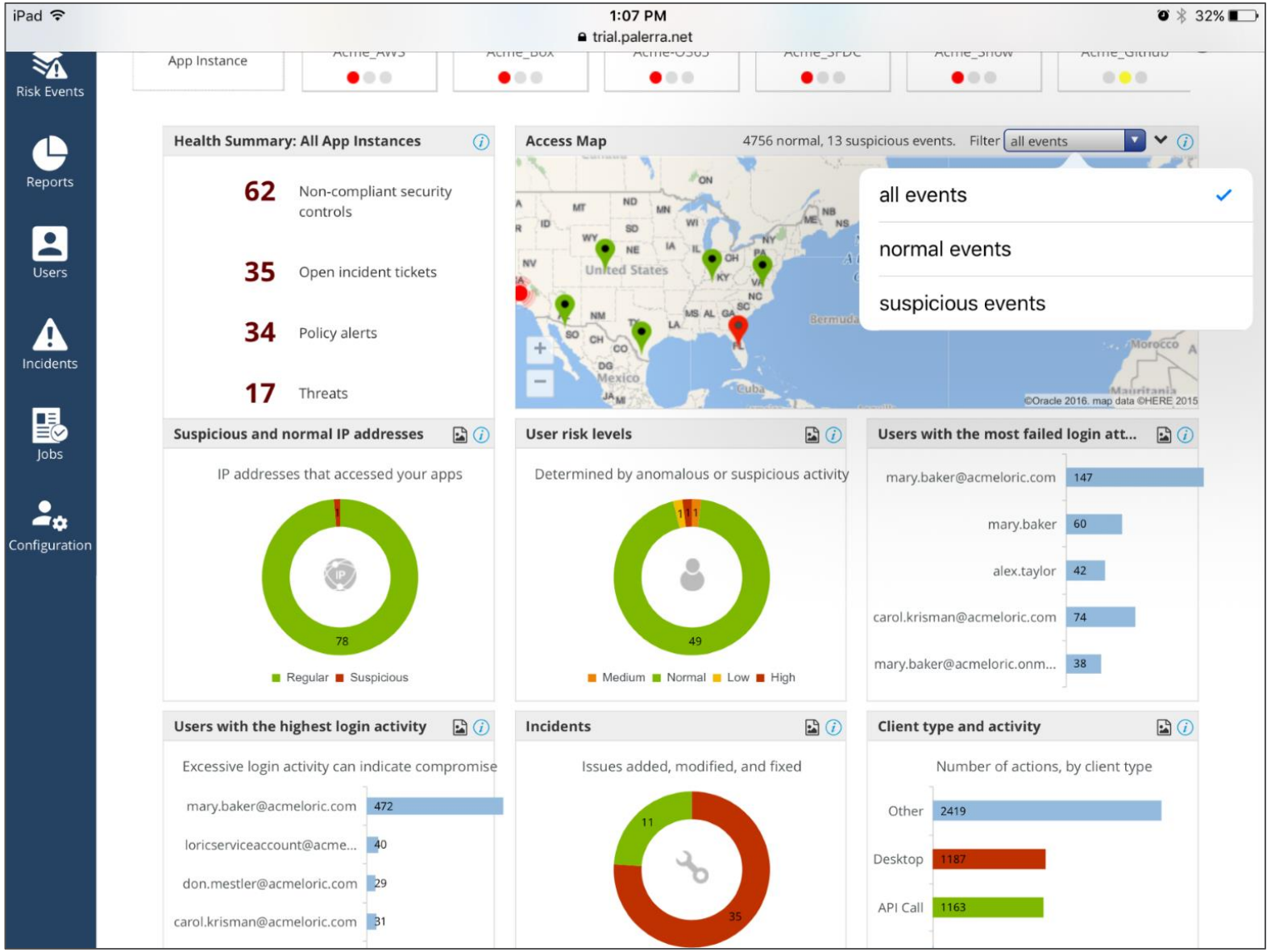
Oracle Management Cloud



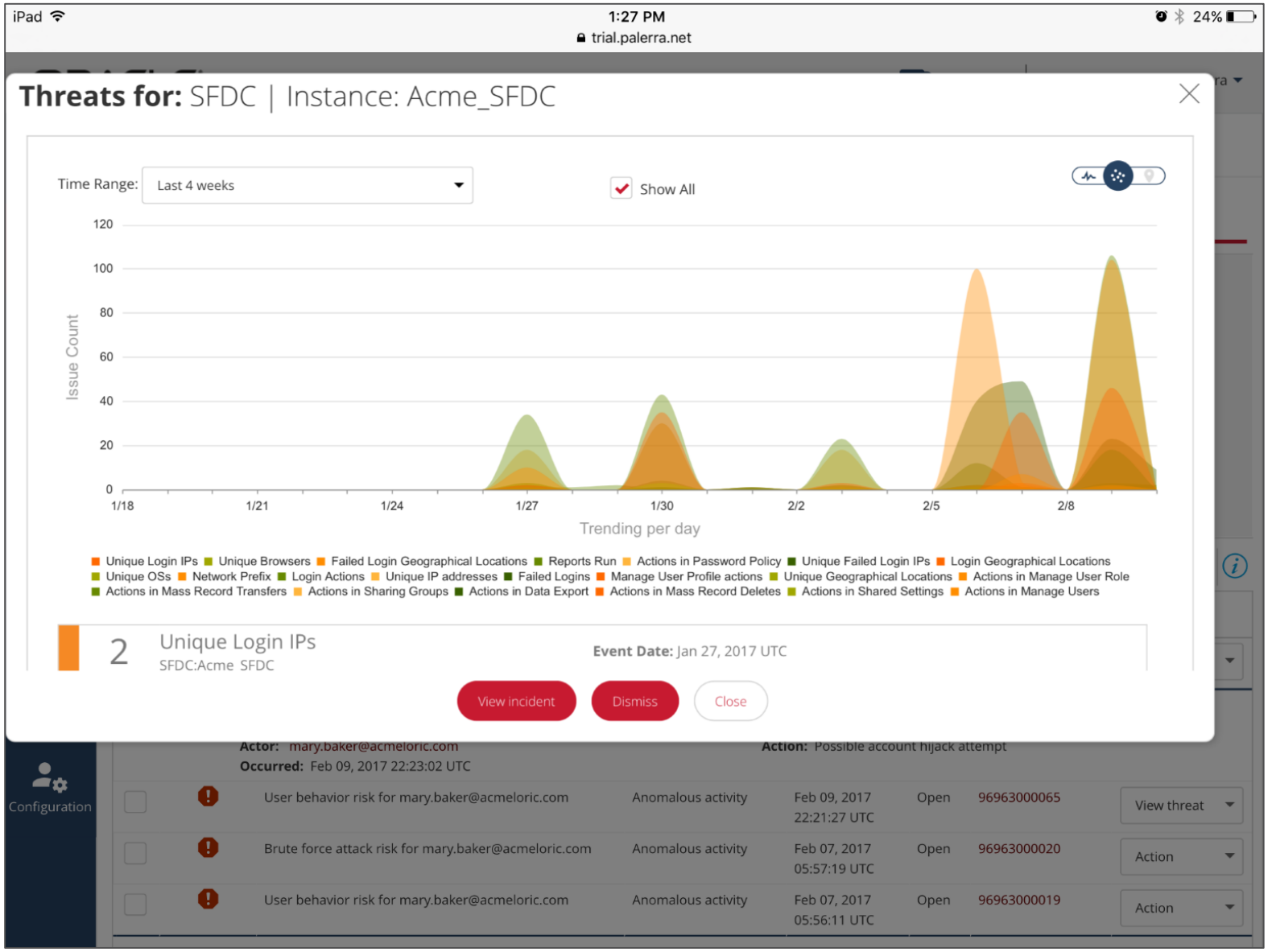
CASB (1:3)


iPad
1:04 PM
32%
trial.palerra.net
ORACLE CASB Cloud Service
Help
Acme
Shruti Visweswara
Dashboard
Applications
Risk Events
Reports
Users
Incidents
Jobs
Dashboard: Summary
Summary
App Discovery
Key Security Indicators
Add App Instance
Acme_AWS
Acme_Box
Acme-O365
Acme_SFDC
Acme_Snow
Health Summary
Issues for Acme_AWS
32 Security Controls
1 Incidents
1 Threats
5 Policy Alerts
Data processed in the last 90 days
4 MB Data Size
24363 Records
13 IP Addresses
s Map
4756 normal, 13 suspicious events.
Filter
Europe
North Atlantic Ocean
Africa
Suspicious and normal IP addresses
IP addresses that accessed your apps
User risk levels
Determined by anomalous or suspicious activity
Users with the most f
mary.baker@acmeloric.

CASB (2:3)


iPad
1:07 PM
trial.palerra.net
32%
App Instance
Risk Events
Reports
Users
Incidents
Jobs
Configuration
Health Summary: All App Instances
62 Non-compliant security controls
35 Open incident tickets
34 Policy alerts
17 Threats
Access Map
4756 normal, 13 suspicious events.
Filter
all events
all events
normal events
suspicious events
©Oracle 2016. map data ©HERE 2015
Suspicious and normal IP addresses
IP addresses that accessed your apps
78
Regular
Suspicious
User risk levels
Determined by anomalous or suspicious activity
111
49
Medium
Normal
Low
High
Users with the most failed login att...
mary.baker@acmeloric.com 147
mary.baker 60
alex.taylor 42
carol.krisman@acmeloric.com 74
mary.baker@acmeloric.onm... 38
Users with the highest login activity
Excessive login activity can indicate compromise
mary.baker@acmeloric.com 472
loricserviceaccount@acme... 40
don.mestler@acmeloric.com 29
carol.krisman@acmeloric.com 31
Incidents
Issues added, modified, and fixed
11
35
Client type and activity
Number of actions, by client type
Other 2419
Desktop 1187
API Call 1163

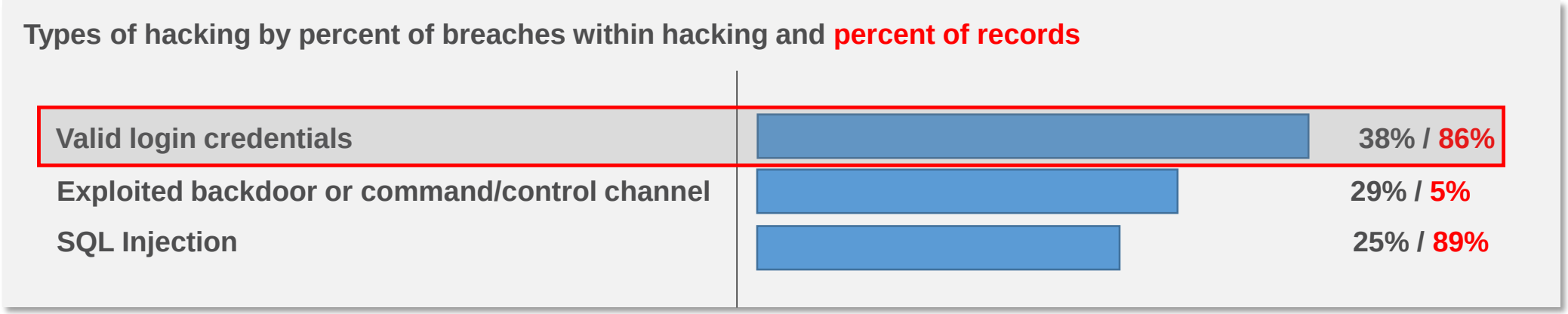
CASB (3:3)


iPad
1:27 PM
trial.palerra.net
24%
Threats for: SFDC | Instance: Acme_SFDC
Time Range: Last 4 weeks
Show All
120
100
80
60
40
20
0
Issue Count
1/18
1/21
1/24
1/27
1/30
2/2
2/5
2/8
Trending per day
Unique Login IPs
Unique Browsers
Failed Login Geographical Locations
Reports Run
Actions in Password Policy
Unique Failed Login IPs
Login Geographical Locations
Unique OSs
Network Prefix
Login Actions
Unique IP addresses
Failed Logins
Manage User Profile actions
Unique Geographical Locations
Actions in Manage User Role
Actions in Mass Record Transfers
Actions in Sharing Groups
Actions in Data Export
Actions in Mass Record Deletes
Actions in Shared Settings
Actions in Manage Users
2
Unique Login IPs
SFDC:Acme SFDC
Event Date: Jan 27, 2017 UTC
View incident
Dismiss
Close
Actor: mary.baker@acmeloric.com
Occurred: Feb 09, 2017 22:23:02 UTC
Action: Possible account hijack attempt
Configuration
User behavior risk for mary.baker@acmeloric.com
Anomalous activity
Feb 09, 2017 22:21:27 UTC
Open
96963000065
View threat
Brute force attack risk for mary.baker@acmeloric.com
Anomalous activity
Feb 07, 2017 05:57:19 UTC
Open
96963000020
Action
User behavior risk for mary.baker@acmeloric.com
Anomalous activity
Feb 07, 2017 05:56:11 UTC
Open
96963000019
Action

Wrap Up

How Database Breaches Really Occur

- 48% involve privilege misuse
- 40% result from hacking



- 38% utilized malware
- 28% employed social engineering
- 15% physical attacks

Percentages do not add up to 100% because many breaches employed multiple tactics in parallel or were outliers

SQL Injection

Both Of These Train Wrecks Were Avoidable

```
DIR=/opt/oracle/scripts
. /home/oracle/.profile_db

DB_NAME=hrrpt
ORACLE_SID=$DB_NAME"1"
export ORACLE_SID

SPFILE=`more $ORACLE_HOME/dbs/init$ORACLE_SID.ora | grep -i spfile`
PFILE=$ORACLE_BASE/admin/$DB_NAME/pfile/init$ORACLE_SID.ora
LOG=$DIR/refresh_$DB_NAME.log
RMAN_LOG=$DIR/refresh_$DB_NAME"_rman".log

PRD_PWD=sys_pspr0d
PRD_SID=hrprd1
PRD_R_UNAME=rman_pshrprd
PRD_R_PWD=pspr0d11
PRD_BK=/backup/hrprd/rman_bk
SEQUENCE=`grep "input archive log thread" $PRD_BK/bk.log | tail -1 | awk '{ print $5 }'`
THREAD=`grep "input archive log thread" $PRD_BK/bk.log | tail -1 | awk '{ print $4 }'`

BK_DIR=/backup/$DB_NAME/rman_bk
EXPDIR=/backup/$DB_NAME/exp
DMPFILE=$EXPDIR/exp_sec.dmp
IMPLOG=$EXPDIR/imp_sec.log
EXPLOG=$EXPDIR/exp_sec.log
EXP_PARFILE=$DIR/exp_rpt.par
IMP_PARFILE=$DIR/imp_rpt.par

uname=rman_pshrprd
pwd=pspr0d11

rman target sys/$PRD_PWD@$PRD_SID catalog $PRD_R_UNAME/$PRD_R_PWD@catdb auxiliary / << EOF > $RMAN_LOG
  run{
     set until $SEQUENCE $THREAD;
     ALLOCATE AUXILIARY CHANNEL aux2 DEVICE TYPE DISK;
     duplicate target database to $DB_NAME;
  }
EOF
```

Conclusions

- You can't dig yourself out of a hole after the sides have fallen in
- Few organizations have the skill set required to secure their databases and operational environments
- Less than 1% of DBA "training" involves security
- If we, as a nation keep doing security the way we've been doing it up to now
  - Our employer are at risk
  - Our careers are at risk

Sirius: The Second Largest Security Integrator in North America

FORSYTHE

Forbes AMERICA'S BEST MANAGEMENT CONSULTING FIRMS 2016

Forbes | 2017 AMERICA'S BEST MANAGEMENT CONSULTING FIRMS Powered by Statista

7th straight year CRN Top 50 Providers

THE CHANNEL CO. CRN SOLUTION PROVIDER 500 2017

THE CHANNEL CO. CRN TECH ELITE 250 2017

THE CHANNEL CO. CRN MSP 500 2017

ORACLE Platinum Partner

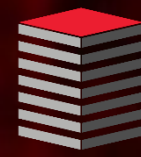
This Is Our New Reality

- A reality that you must embrace


F9
W
F2
F12
E
R
D
F3
T
G
Y
J

Thank You

Seattle Training Day 2018



Daniel A. Morgan
dmorgan@forsythe.com
+1 206-669-2949