

"Channeling a little Oracle Open World"

Seattle Training Day 2018



A Quick Introduction

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

www.morganslibrary.org

Morgan's Library

International Oracle Events 2016-2017 Calendar

The library is a spam-free on-line resource with code demos for DBAs and Developers. If you would like to see new Oracle database functionality added to the library ... just email us. Oracle Database 12cR2 is now available in the Cloud. If you are not already working in a 12cR1 CDB database ... you are late to the party and you are losing your competitive edge.

Training Events and Travels

- OTN APAC, Sydney, Australia - Oct 31
- OTN APAC, Gold Coast, Australia - Nov 02
- OTN APAC, Beijing China - Nov 04-05
- OTN APAC, Shanghai China - Nov 06
- Sangam16, Bangalore, India - Nov 11-12
- NYOUG, New York City - Dec 07

Next Event: Indiana Oracle Users Group

Oracle Events

Click on the map to find an event near you

Library News

- Morgan's Blog
- Morgan's Oracle Podcast
- US Govt. Mil. STIGs (Security Checklists)
- Bryn Llewellyn's PL/SQL White Paper
- Bryn Llewellyn's Editioning White Paper
- Explain Plan White Paper

ACE News

Would you like to become an Oracle ACE?

Learn more about becoming an ACE

- ACE Directory
- ACE Google Map
- ACE Program
- Stanley's Blog

This site is maintained by Dan Morgan. Last Updated: 11/08/2016 22:25:14

ORACLE OTN | Oracle Mix | Share | Twitter | Facebook | Library | Contact Us | Privacy Statement | Legal Notices & Terms of Use

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.

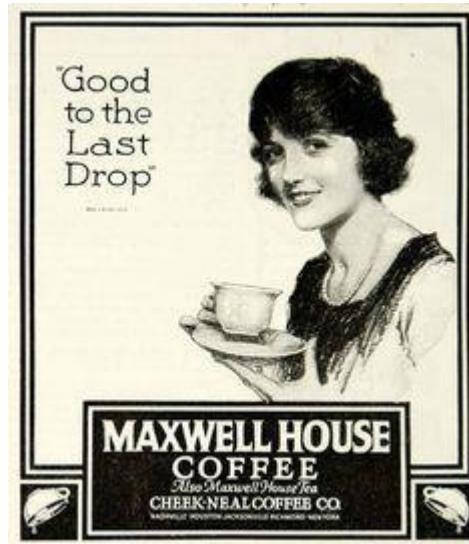
“History is repeating itself,” says longtime DBA Dan Morgan, founder of [Morgan’s Library](#) and principal adviser at tech firm Meta7. Morgan has seen the DBA role evolve amid a long series of technical advances in storage, management, and performance. And each advance asked DBAs to adjust the way they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

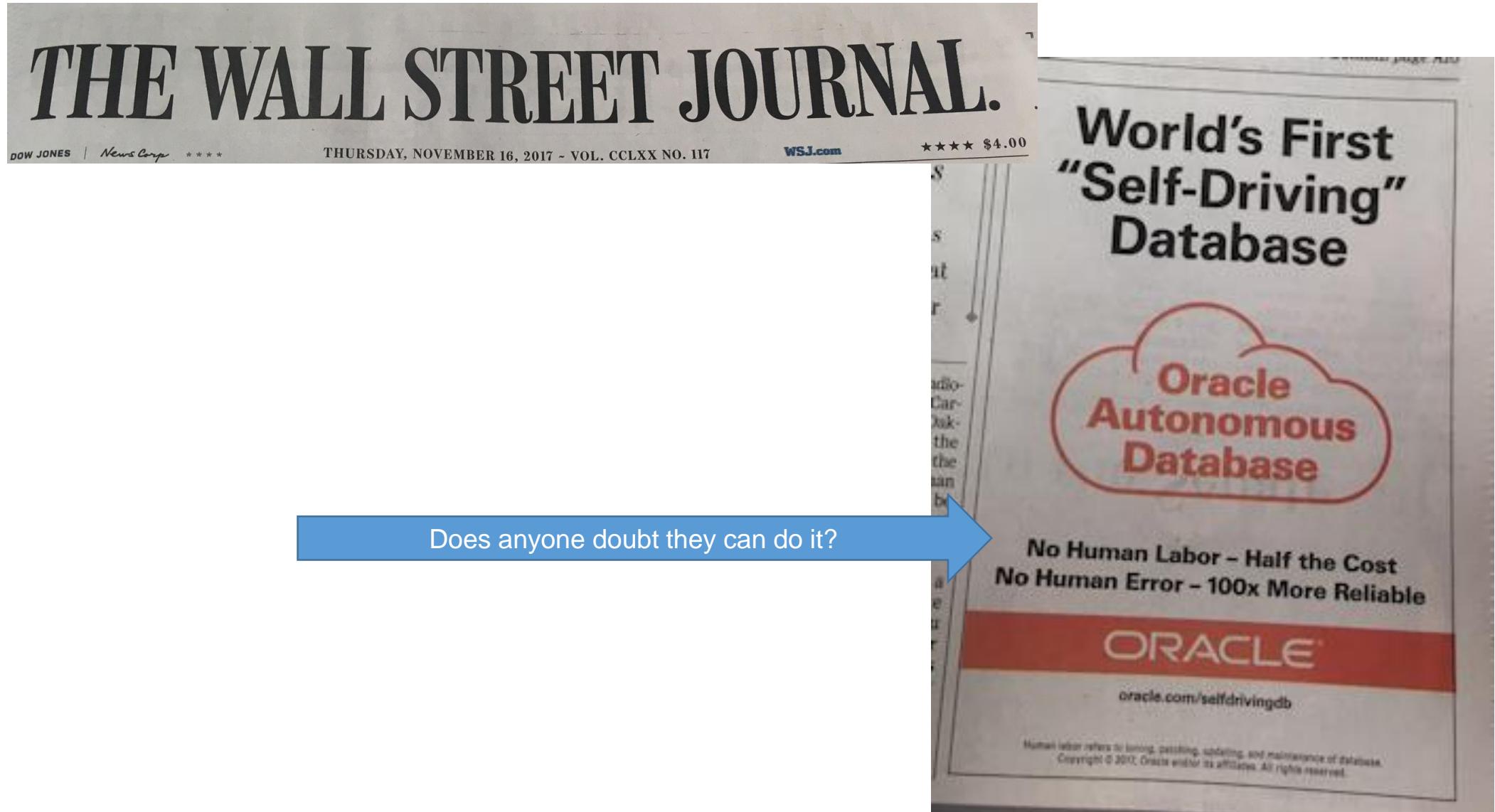
What "should have been said" but was not

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



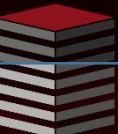
Perhaps you shouldn't drink that last drop?

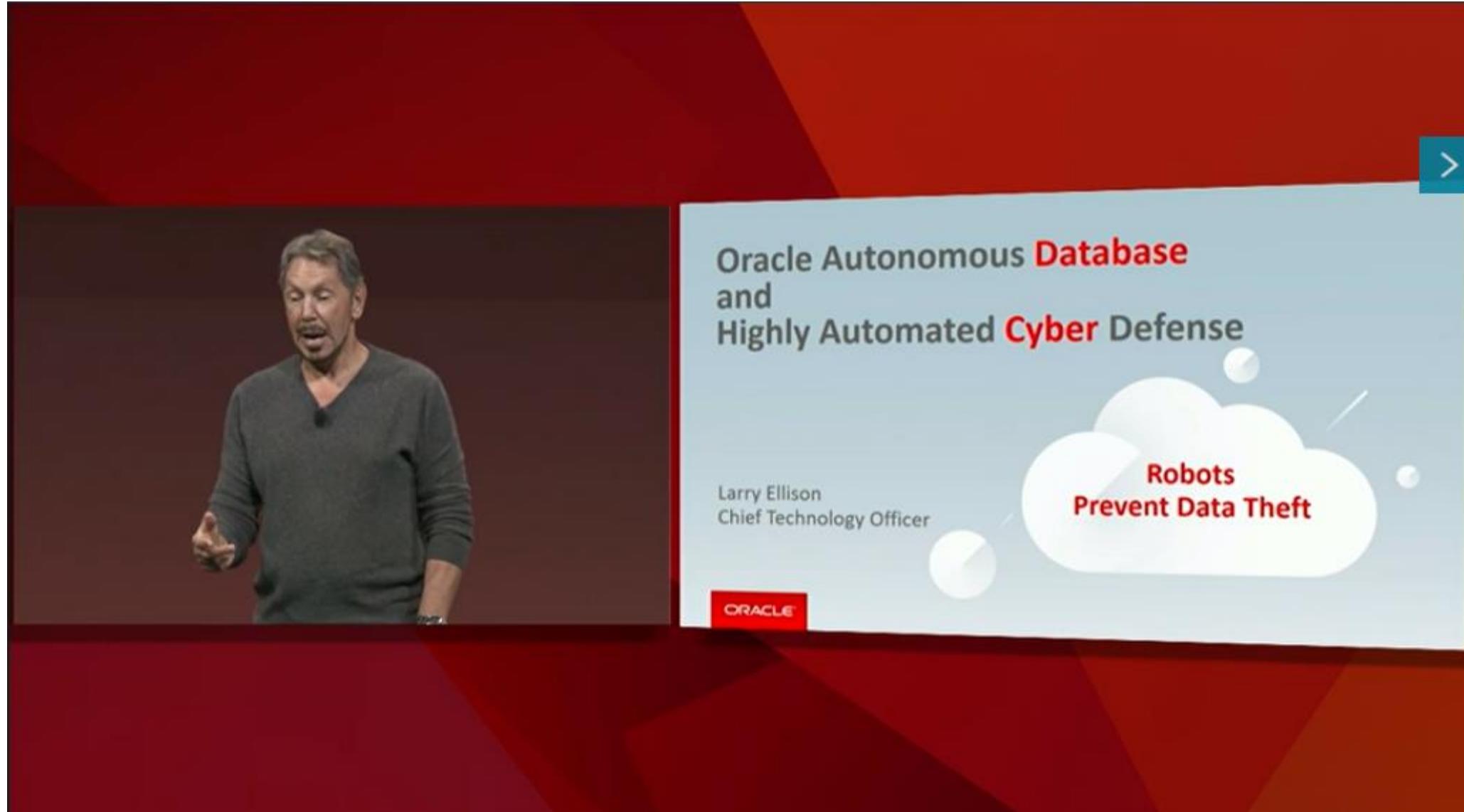
Perhaps We Should Apply That Lesson To Oracle





Channeling Oracle OpenWorld 2017





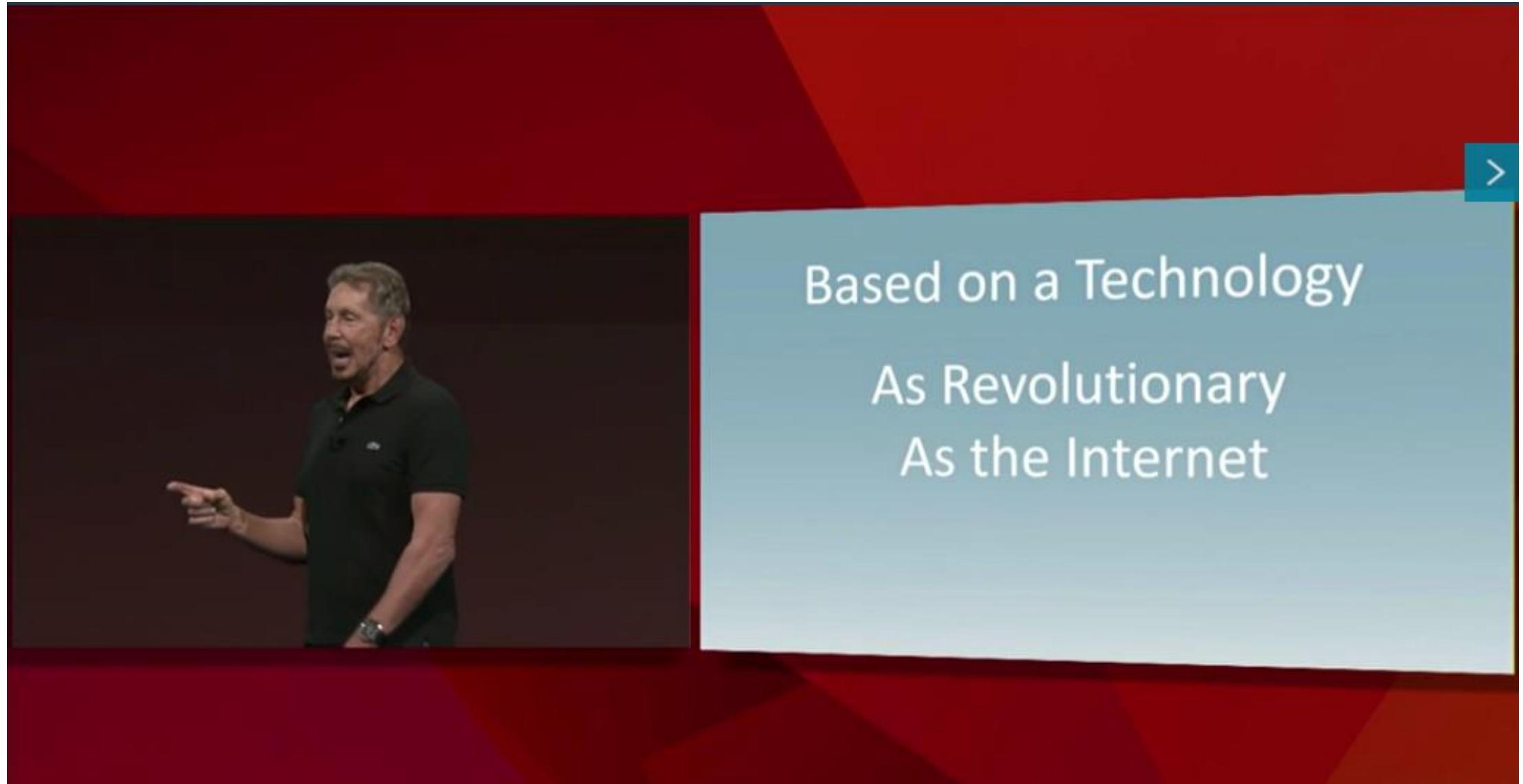
Larry Ellison, Chief Technology Officer, is speaking on stage. To his right is a presentation slide with a red and orange geometric background. The slide features the Oracle logo and the text "Oracle Autonomous Database and Highly Automated Cyber Defense". A white cloud icon contains the text "Robots Prevent Data Theft". A blue navigation arrow is in the top right corner.

Oracle Autonomous Database
and
Highly Automated Cyber Defense

Larry Ellison
Chief Technology Officer

ORACLE

Robots
Prevent Data Theft



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 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



Modern Cyber Security Requires More Automation
Cyber Defense: Our People versus Their Computers

- Most Data Thefts Occur **After** Security Fix Available
 - Target did not detect the attack
 - Target behind in applying security patches
 - Wrong priorities
 - Waiting for downtime window

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 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

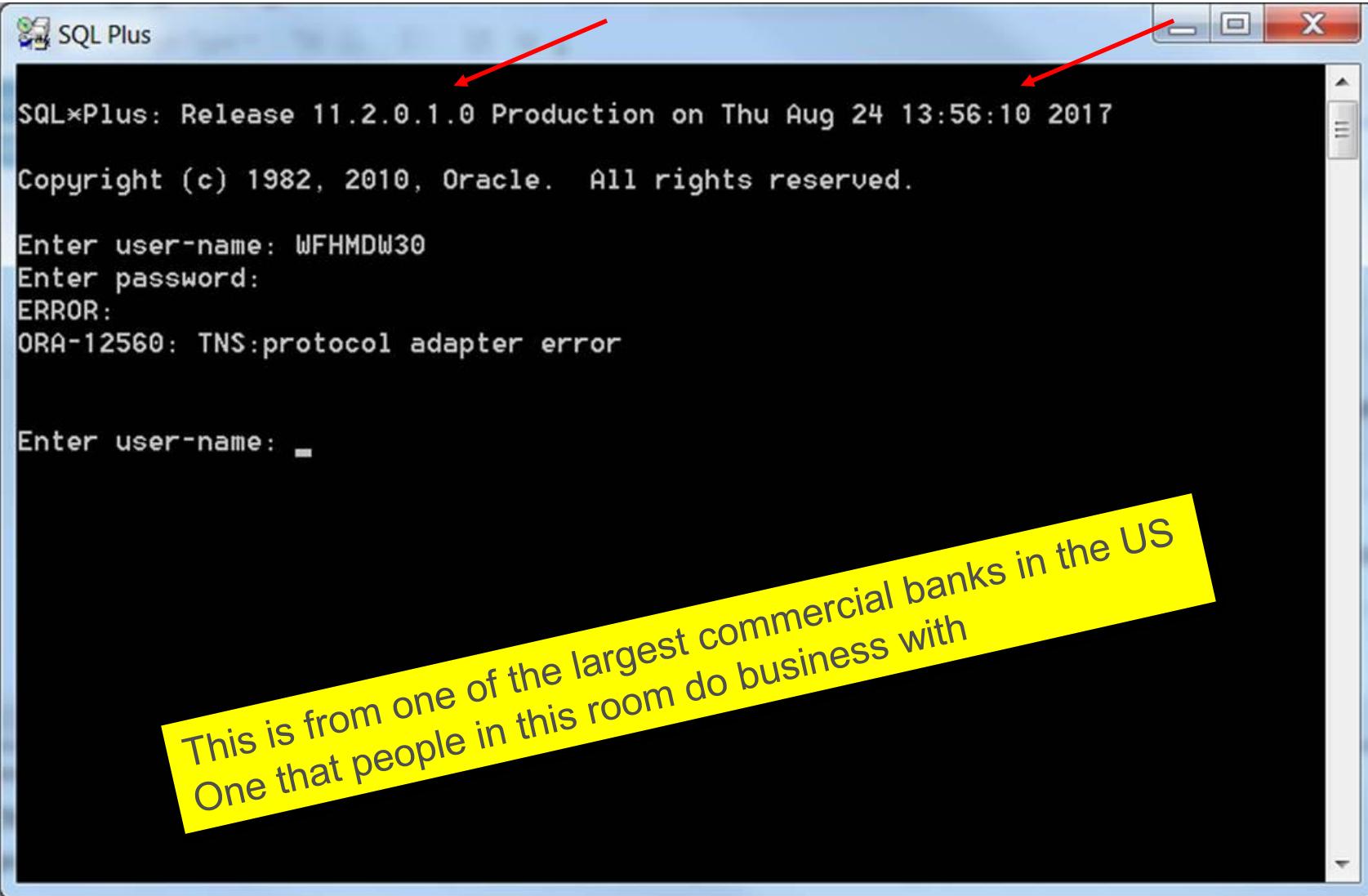
Patching is never a top priority for our employers

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



SQL*Plus: Release 11.2.0.1.0 Production on Thu Aug 24 13:56:10 2017

Copyright (c) 1982, 2010, Oracle. All rights reserved.

Enter user-name: WFHMDW30

Enter password:

ERROR:

ORA-12560: TNS:protocol adapter error

Enter user-name:

This is from one of the largest commercial banks in the US
One that people in this room do business with

Cyber Criminals Are Winning



Cyber Attacks: More Data Stolen Every Year

Cyber Criminals and State Actors are Winning the Cyber War

- Equifax: Records of 143,000,000 Americans plus...
 - Credit Card Numbers, Social Security Numbers, home addresses...
 - Equifax CEO, executives and IT management team resigns
- Office of Personnel Management: Records of 20 Million Federal Employees
 - Security clearance data, finger print data, social security numbers, home addresses
 - White House, Foreign Embassies, State Department, Defense Department...
 - Director of OPM Resigns
- Cyber Criminals and State Actors steal more data every year
 - Formidable and sophisticated adversaries stealing corporate & government data

More Automation is Required

A man with short grey hair, wearing a dark grey V-neck sweater, is speaking on stage. He is gesturing with his hands and holding a small device in his right hand. To his right, a white rectangular box contains text and a list. The background is a dark red gradient stage. In the top right corner of the slide, there is a small blue triangle with a white right-pointing arrow.

Modern Cyber Security Requires More Automation **Security & Database Automation Work Together to Prevent Data Theft**

- **Cyber Defense System:** Automatically Detects Attacks in Real-Time
 - Automated Intrusion Detection
- **Database System:** Automatically and Immediately Secures Your Data
 - Automated database immediately patches itself while running
 - No delay for downtime window, **no manual intervention**
 - Recovers data that's deleted by ransomware, etc.



Machine Learning
Computers Learn from Patterns in the Data and Make Predictions

- Machine learning relies on large amounts of accurate training data
 - Higher volumes of accurate data increases learning
 - Increased learning/training means more accurate predictions
- **Anomaly Detection:** Separate normal from abnormal patterns in the data
 - Detect a cancer cell from normal cells
 - Detect the CFO logging on from a computer in the Ukraine



Machine Learning (ML)
The Applications are Revolutionary

- Autonomy: "Self-Driving" cars
- Computer Vision: Facial Recognition
- New ML Applications: Autonomous Database & Automated Cyber Security



Huge Amounts of Computer Systems Data in Event Logs
Enable New Database and Security Applications for Machine Learning

>

- Lots of Event Logs
 - Infrastructure logs: Network, Server, Storage, VM, OS
 - Platform logs: Database, Java, Analytics, etc.
 - Applications logs: ERP, CX, HCM, Custom, etc.
- Event Log Training Data Enables New Machine Learning Applications
 - **Security**: Detect and connect anomalous events: Login from Ukraine and unique SQL
 - **Database**: Classify normal query patterns and automatically tune database

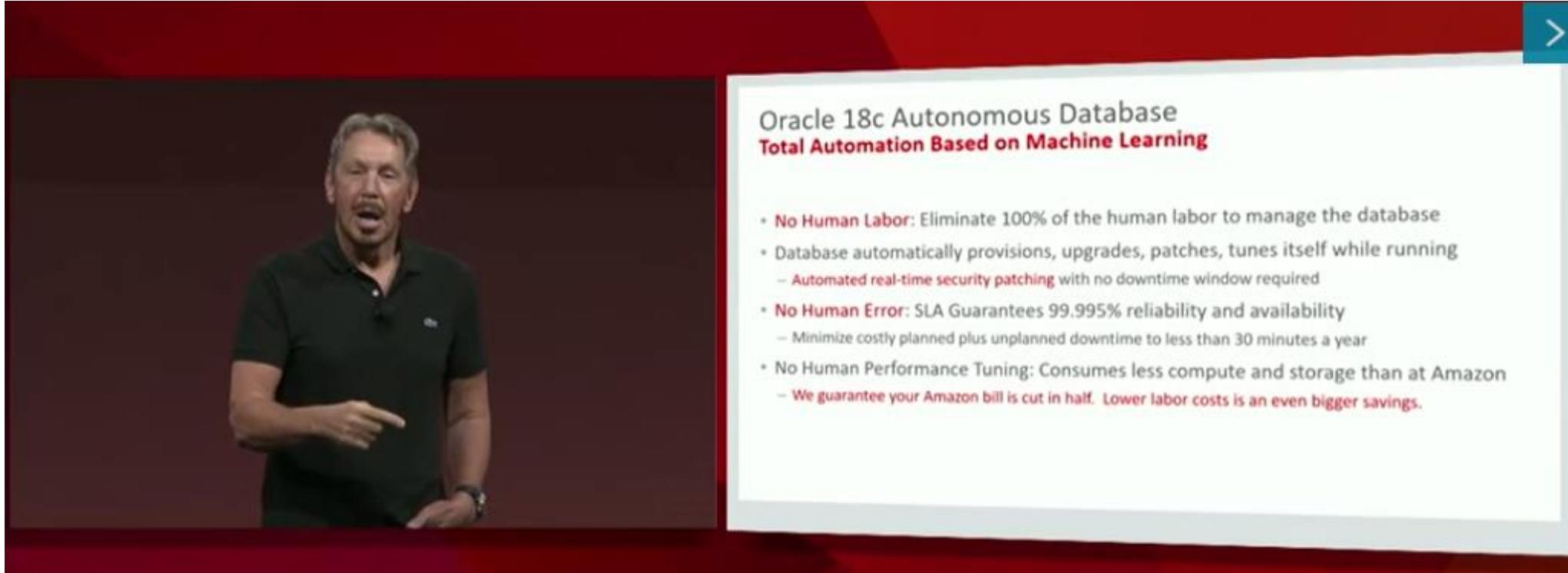


>

Database Autonomy & Highly Automated Cyber Security

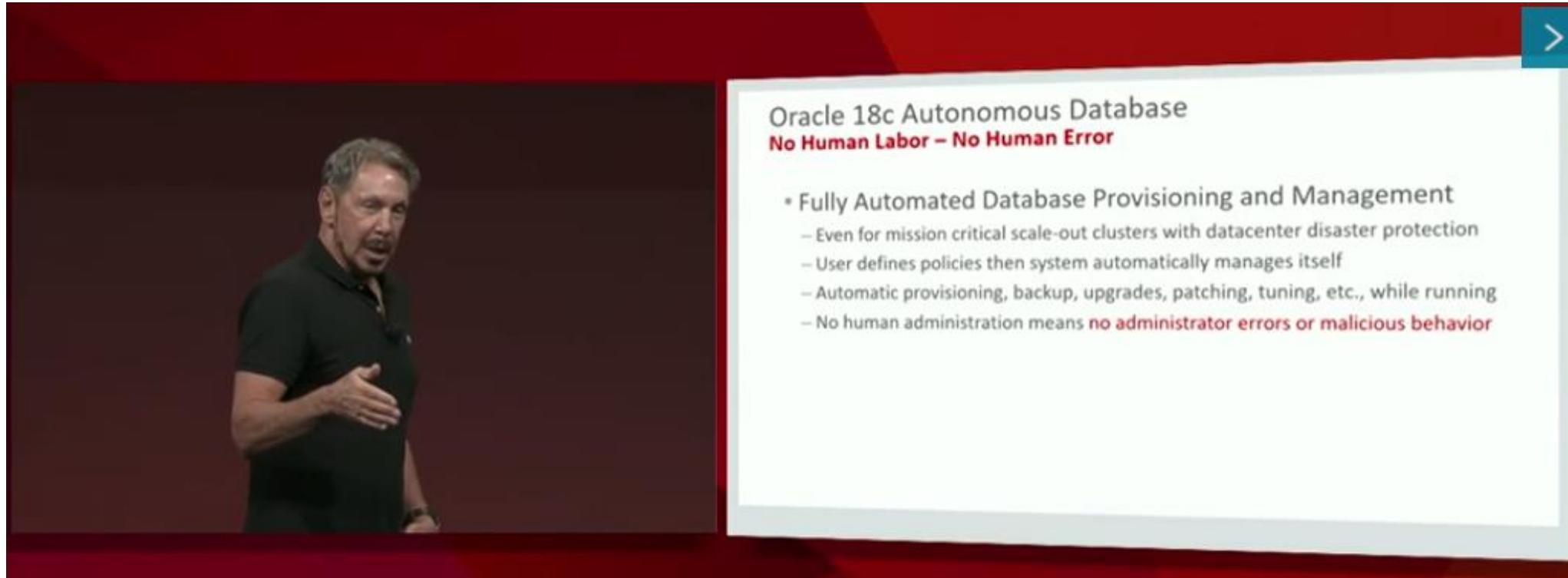
- Database Autonomy: Fully automated 100% “self-driving” database
- Automated Cyber Defense: Detect & remediate attacks in real-time
- They Work Together:
 - Discover attack: Real time ML log processing detects security anomaly in data
 - Remediate: Database automatically patches itself while running

Lots of Other Benefits Come with Total Database Automation



Oracle 18c Autonomous Database
Total Automation Based on Machine Learning

- **No Human Labor:** Eliminate 100% of the human labor to manage the database
 - Database automatically provisions, upgrades, patches, tunes itself while running
 - **Automated real-time security patching** with no downtime window required
- **No Human Error:** SLA Guarantees 99.995% reliability and availability
 - Minimize costly planned plus unplanned downtime to less than 30 minutes a year
- **No Human Performance Tuning:** Consumes less compute and storage than at Amazon
 - **We guarantee your Amazon bill is cut in half. Lower labor costs is an even bigger savings.**



Oracle 18c Autonomous Database
No Human Labor – No Human Error

- Fully Automated Database Provisioning and Management
 - Even for mission critical scale-out clusters with datacenter disaster protection
 - User defines policies then system automatically manages itself
 - Automatic provisioning, backup, upgrades, patching, tuning, etc., while running
 - No human administration means **no administrator errors or malicious behavior**



Database Professionals: Evolution of Skill Set

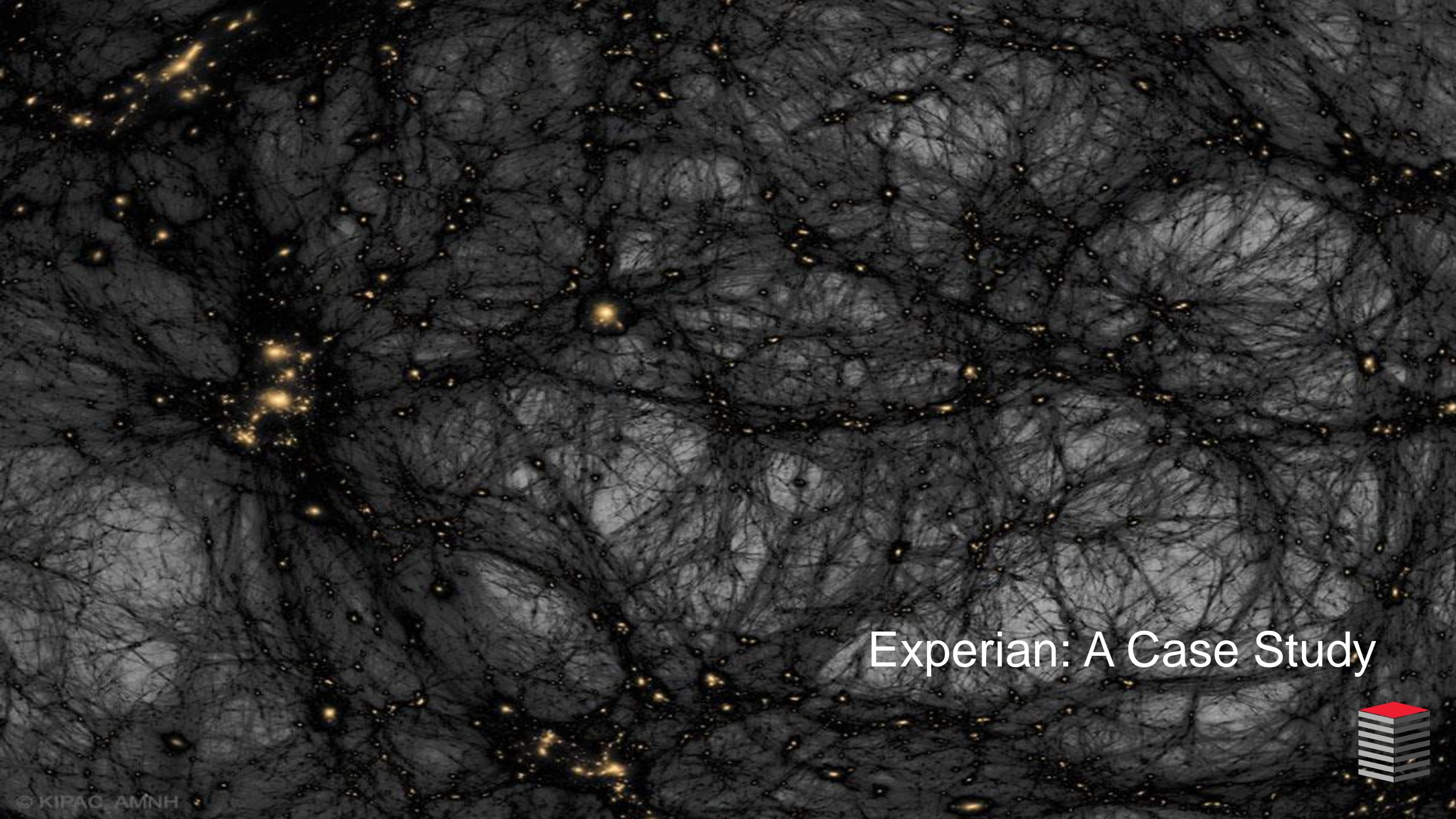
Problem: More data management tasks than humans to do the work

Less time on Administration

- Less time on infrastructure
- Less time on patching, upgrades
- Less time on ensuring availability
- Less time on tuning

More time on Innovation

- More time on database design
- More time on data analytics
- More time on data policies
- **More time on securing data**



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?



Are You The Next Experian? (2:5)

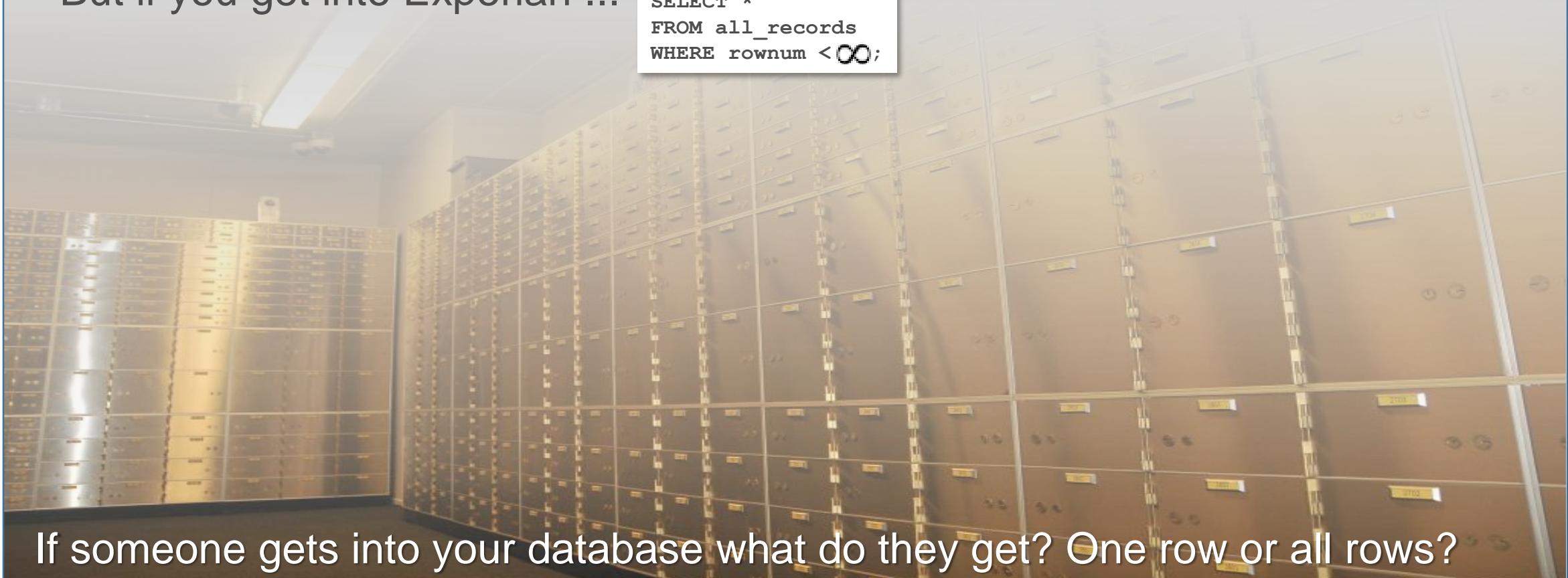
- According to Experian an Apache Struts patching failure allowed the theft of data from 145,000,000 people some of whom are sitting in this room
- Do you believe Experian?
- I don't
- Security is not "I put a lock on the front door"



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 < 100;
```



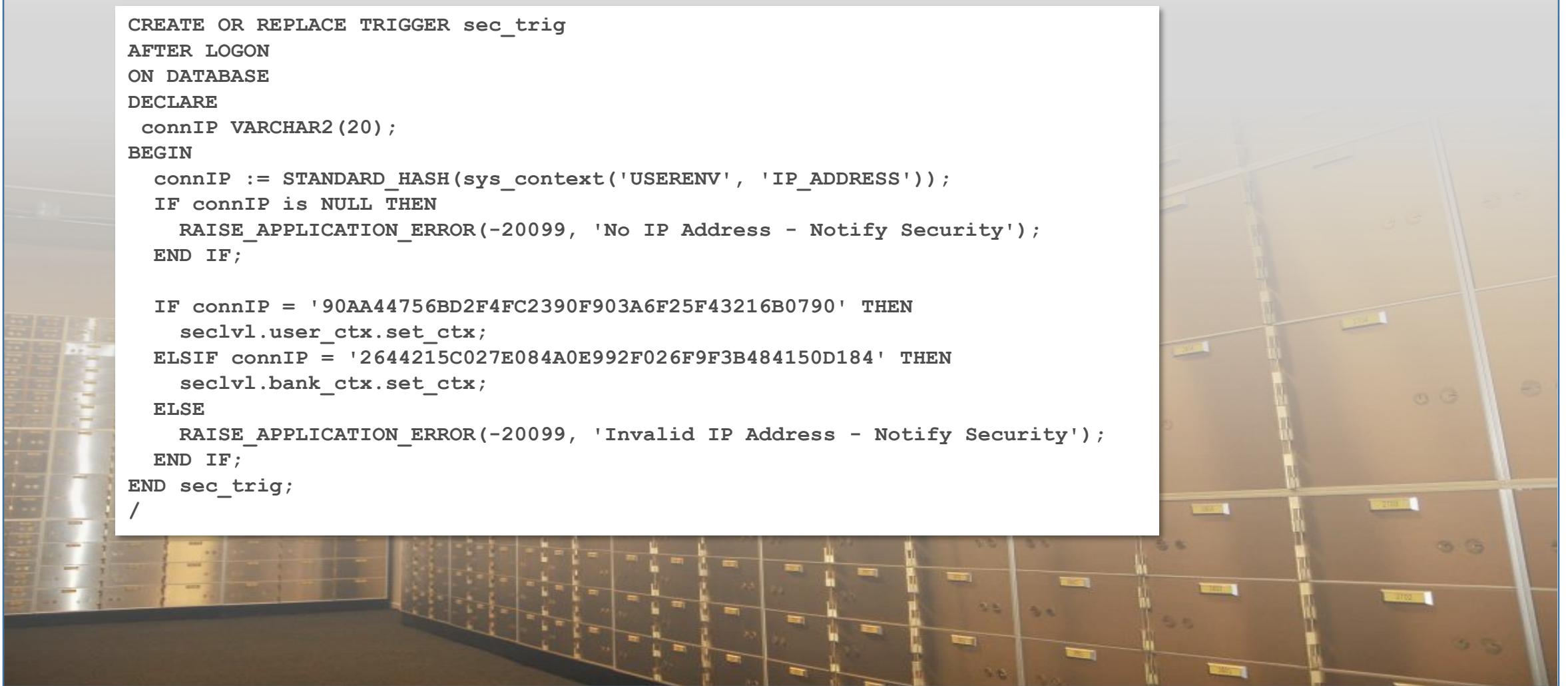
If someone gets into your database what do they get? One row or all rows?

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;
/
```



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;
/
```

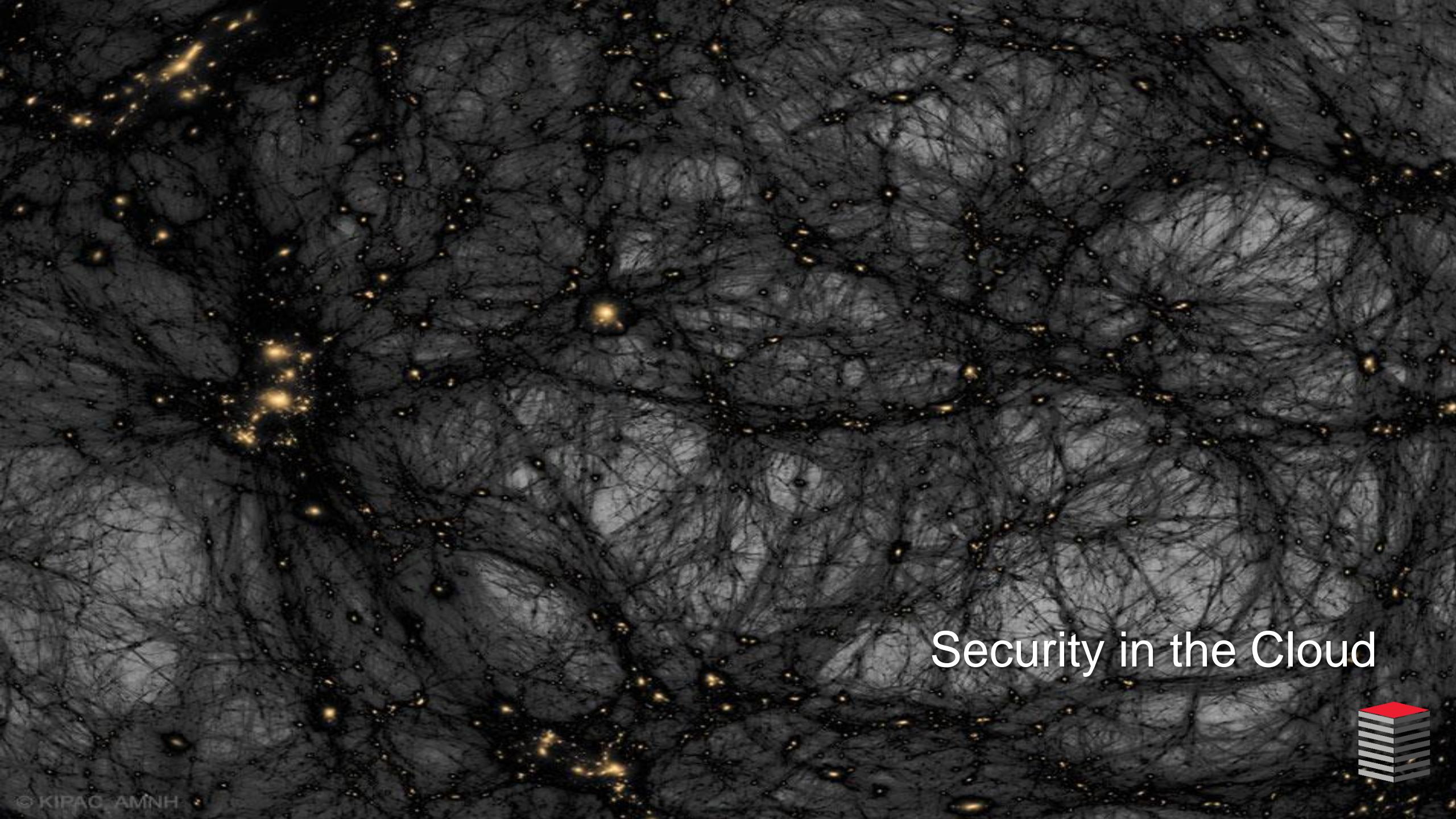
- And the user_sec function did this

```
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?



Security in the Cloud





>

Announcing: Oracle Management and Security Cloud

- **Complete and Integrated “Cloud Native” System**
 - Monitor, manage, analyze ALL operational & security data in one system
- **Powered by Machine Learning (ML)**
 - ML-based system discovers anomalies in the data – **Security Threats**
- **Automated Remediation**
 - Automated operational workflows for real-time security remediation

Oracle Management Cloud

Management Cloud

- Home
- Alerts
- Dashboards
- Data Explorer**
 - APM
 - Monitoring
 - Log Analytics
 - IT Analytics
 - Orchestration
 - Security Analytics
 - Compliance
- Administration



Application Performance Monitoring
Rapidly identify, response, and resolve your software roadblocks



Infrastructure Monitoring
Monitor your entire IT infrastructure - on-premise or on the cloud - from one unified platform



Log Analytics
Topology aware log exploration and analytics for modern applications and infrastructure



IT Analytics
Operational big data intelligence for modern IT



Configuration and Compliance
Automate application and infrastructure configuration assessments



Security Monitoring and Analytics
Detect, investigate and mitigate security threats



Orchestration
Schedule, execute and report on tasks at scale



Dashboards
Build custom dashboards using out-of-the-box widgets or your own visualization of data



Explorers
Search, analyze, and visualize data

Select

Select

Select

iPad 1:04 PM trial.palerra.net

ORACLE CASB Cloud Service 5 Help Acme Shruti Visweswara

Dashboard: Summary

Summary

Add App Instance

Acme_AWS

Acme_Box

Acme_O365

Acme_SFDC

Acme_Snow

Health Summary

Issues for Acme_AWS

32	1	1
Security Controls	Incidents	Threats

5 Policy Alerts

Data processed in the last 90 days

4 MB	24363	13
Data Size	Records	IP Addresses

Events Map 4756 normal, 13 suspicious events.

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.

iPad  1:07 PM trial.palerra.net



Risk Events

- App Instance
- Acme_AWS
- Acme_Box
- Acme_Podus
- Acme_SFDC
- Acme_Snow
- Acme_GitHub

Health Summary: All App Instances

- 62 Non-compliant security controls
- 35 Open incident tickets
- 34 Policy alerts
- 17 Threats

Suspicious and normal IP addresses

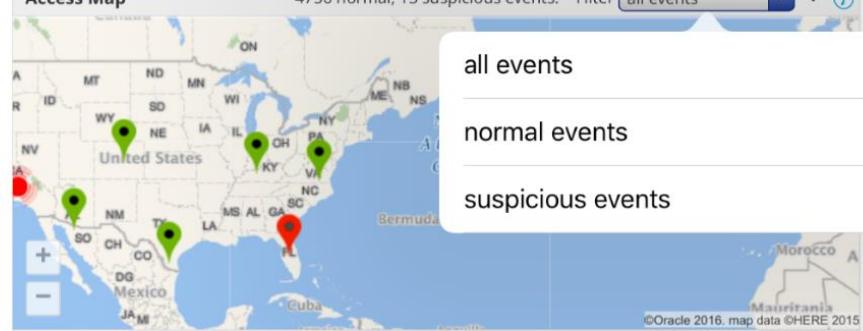
IP addresses that accessed your apps



■ Regular ■ Suspicious

Access Map

4756 normal, 13 suspicious events. Filter



User risk levels

Determined by anomalous or suspicious activity



■ Medium ■ Normal ■ Low ■ High

Users with the most failed login attempts

User	Attempts
mary.baker@acmeloric.com	147
mary.baker	60
alex.taylor	42
carol.kisman@acmeloric.com	74
mary.baker@acmeloric.onm...	38

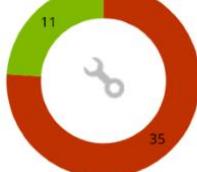
Users with the highest login activity

Excessive login activity can indicate compromise

User	Activity
mary.baker@acmeloric.com	472
loricserviceaccount@acme...	40
don.mestler@acmeloric.com	29
carol.kisman@acmeloric.com	31

Incidents

Issues added, modified, and fixed

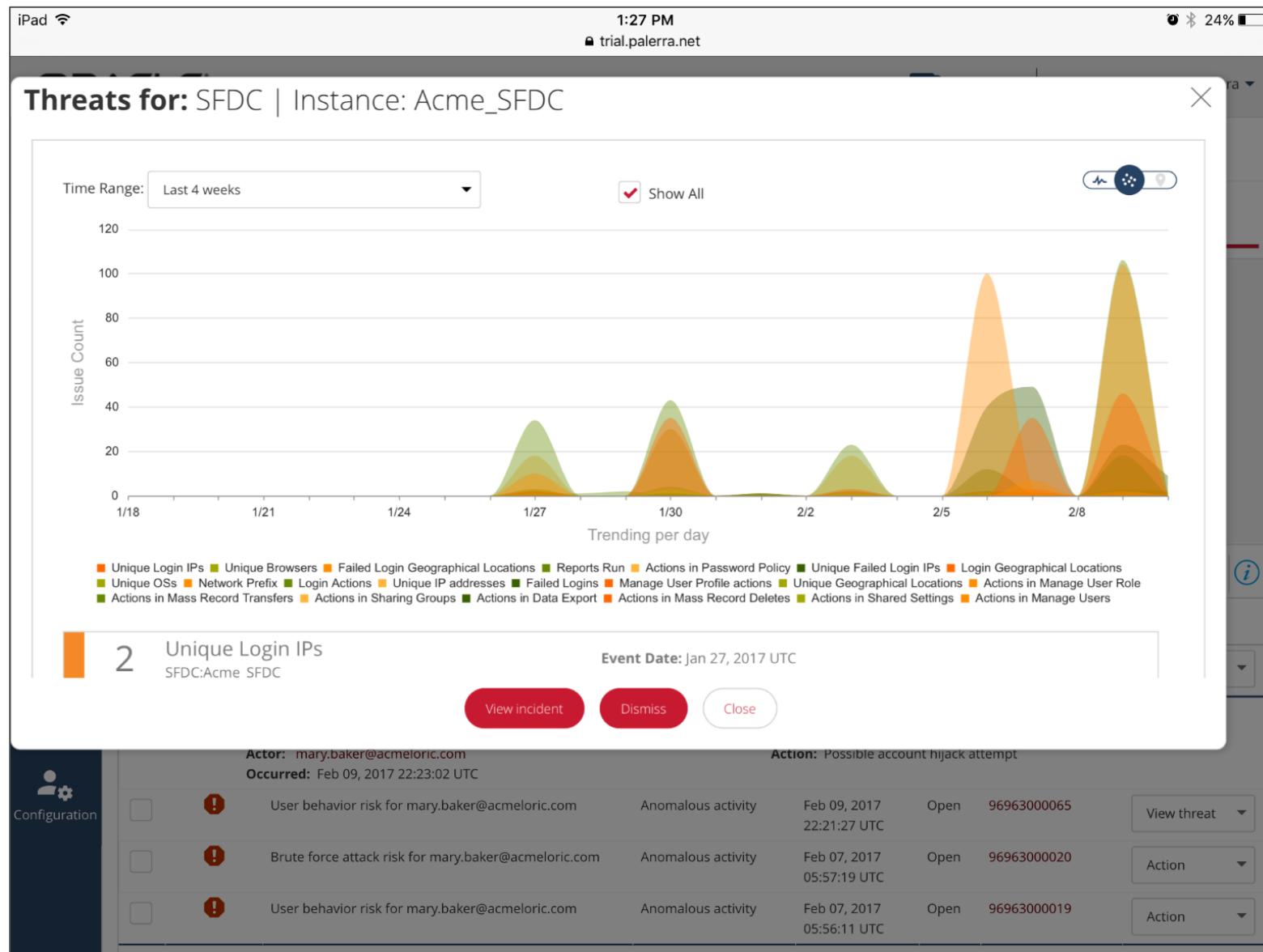


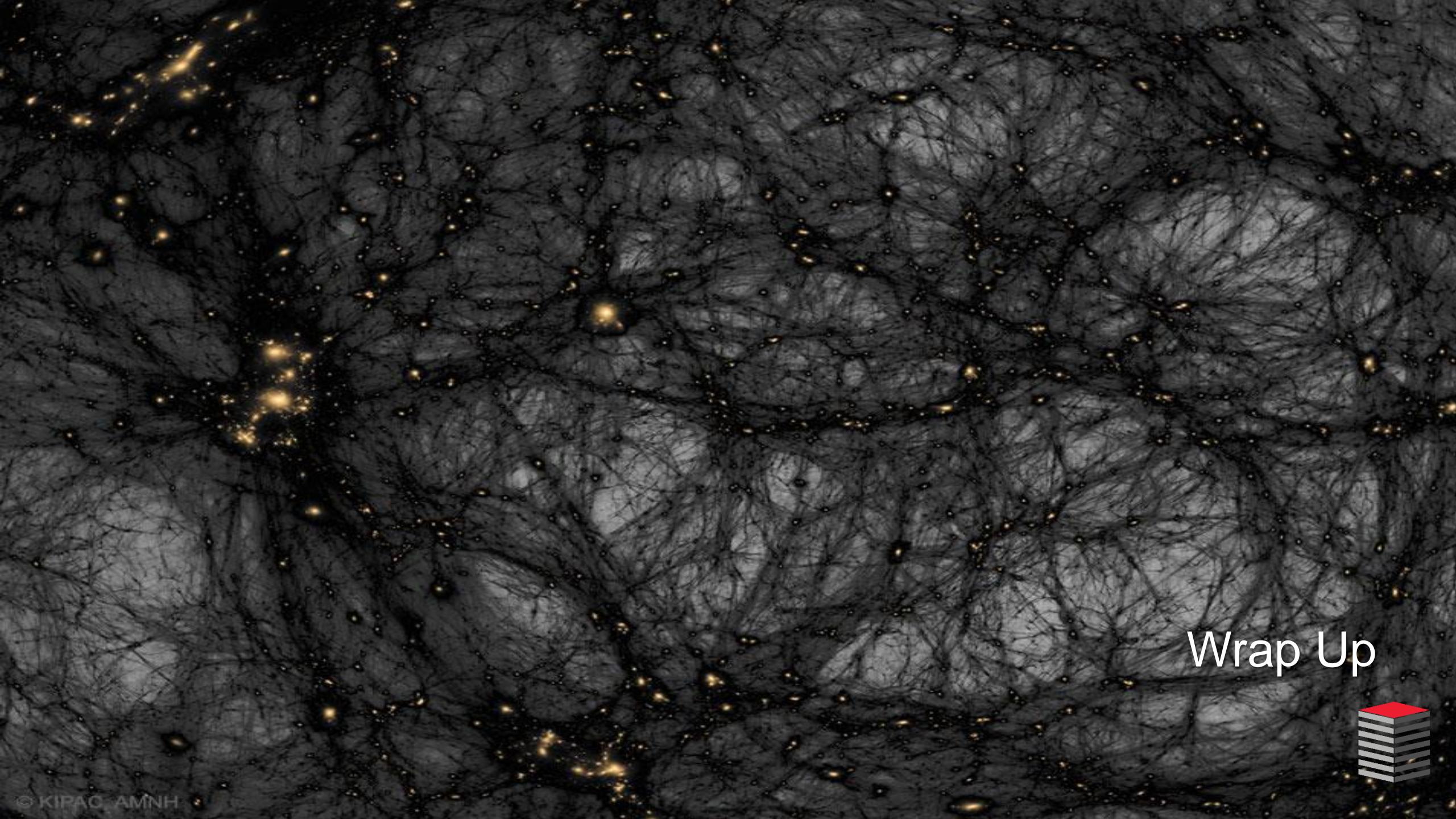
■ 11 ■ 35

Client type and activity

Number of actions, by client type

Client Type	Actions
Other	2419
Desktop	1187
API Call	1163



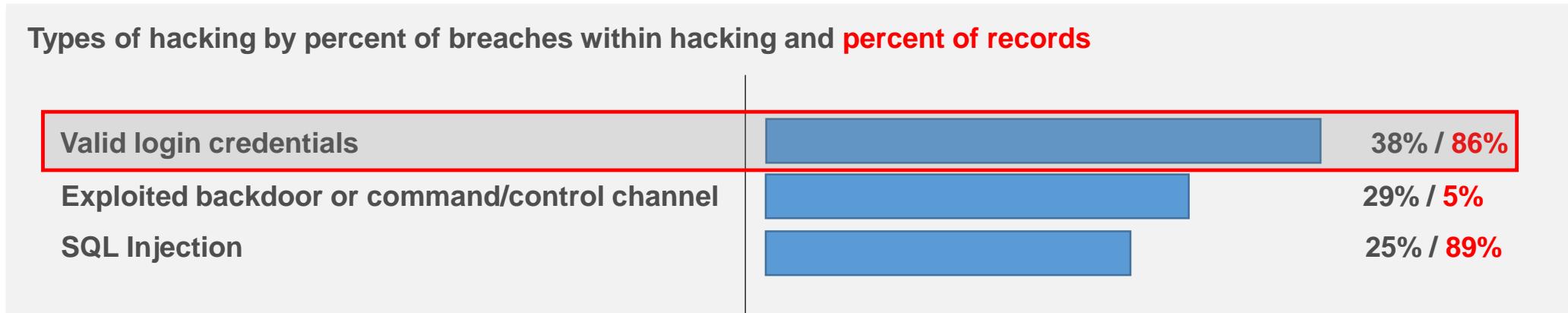


Wrap Up



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_pshprd
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 }'`  
THREADE=`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_pshprd
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 $THREADE;
  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



7th straight year CRN Top 50 Providers



This Is Our New Reality

- A reality that you must embrace







Thank You

Seattle Training Day 2018

