Protect the Data at All Costs

Success is about people, it's never about technology

March 29, 2016

Robert Murray, INL Oracle Business Systems Architect

UT Oracle Users Group Conference

Salt Lake City, UT

www.inl.gov

Idaho National Laboratory

Anyone wanting a copy of this slide deck, please email me at robert.murray@inl.gov

ENSURING THE NATION'S ENERGY SECURITY

- INL is the nation’s leading center for nuclear energy research and development. INL is part of the U.S. Department of Energy’s complex of national laboratories.

- The laboratory performs work in each of the strategic goal areas of DOE: energy, national security, science and environment.

- INL is the nation’s lead laboratory for nuclear energy research, development, demonstration and deployment and we are engaged in the mission of ensuring the nation’s energy security with safe, competitive and sustainable energy systems and unique national and homeland security capabilities.

- Please visit https://www.inl.gov/about-inl/general-information

Abstract

To protect the data at all costs

My advice – keep your security policy simple. Be proactive, not reactive. Don't strive to get it right using some "big bang" technical solution – instead, outline a series of doable steps to "make it better".

Focus on the access points. Limit the number of "front doors" and "back doors". Know how the "bad guys" will be able to access the data. Know your data's sensitivity and where it lives – visually map it out.

Know who the "bad guys" are – your team, your department, other employees and contractors, your end users, and finally, the hackers. If the bad guys do manage to steal it – you better make sure it is encrypted.

My presentation highlights recent data breaches, common attack routes, and the strategies my team at the INL is using to safeguard the data.

WHY STEAL DATA?

Data is Valuable

- Health information that is individually identifiable and held or transmitted by a covered entity is protected by HIPAA (Health Information Portability and Accountability Act). Examples include health records, patient treatment information, health insurance billing information.
- Credit cards numbers, names, and other information used for payment processing are regulated through a trade association agreement with the "Payment Card Industry" or PCI.
- Personal identifying information (PII)deemed confidential include: Social Security numbers, credit card numbers, drivers license numbers and bank account numbers.
- Dual-use technology used for scientific advancement as well as military applications is protected by ITAR (International Traffic in Arms Regulations) and EAR (Export Administration Regulations).
- Education records are protected by FERPA (Family Educational Rights and Privacy Act) include tax records of parents and students, class lists, grade rosters, records of advising sessions, grades, and financial aid applications.
- Financial Aid records are protected by GLBA (Gramm-Leach-Bliley/Financial Services Modernization Act).
- Sensitive Identifiable Human Subject Research is information that reveals or can be associated with the identities of people who serve as research subjects.

Data Breaches

- OPM – estimated number of stolen records is 21.5 million
- Other examples where hackers obtained personal information, including credit card numbers, debit card numbers, e-mail addresses, birth dates, social security numbers, and bank account numbers.
  - US Veterans Affairs – cost $25 – $30 million
  - Heartland Payment Systems – cost $140 million
  - TJX – cost $256 million or more
  - Epsilon – cost estimated between $225 million to $4 billion
  - Sony – cost estimated up to $2 billion
- More often than not, the hackers had help from insiders.
- In addition to consumer data, think about the impact of the theft of research data, classified data, data detailing the locations of critical infrastructures, data that could manipulate our financial markets or compromise our National security (like OPM).

DON'T LET THIS BE YOU

"I DON'T BELIEVE ANYONE (AT THE OFFICE
OF PERSONNEL MANAGEMENT) IS
PERSONALLY RESPONSIBLE."
- OPM DIRECTOR KATHERINE ARCHULETA,
WHEN ASKED ABOUT THE RECENT DATA BREACH.

Office of Personnel Management (2006)

- In summary, OPM has embraced technologies that not only support traditional mainframe information systems, but also support new Internet technologies. … Today, these technologies have improved communications among OPM headquarters, FIPC, PIC, and the investigators in the field. Policy changes are implemented much more quickly, and workload changes can be addressed as they happen, rather than after-the-fact. Timeliness can be monitored and dealt with as concerns develop, instead of acting on crises. Cumbersome, manual record-keeping and calculating systems have been eliminated.
- The research and development process is constantly ongoing. OPM continues to look for new technologies that will improve quality, content, and timeliness throughout the investigative process. These technologies include software applications, hardware, networking, system security, and data repository access.

Use of Information Technology, OPM 2006 Report

- The Office of Personnel Management ("OPM") data breach involves the greatest theft of sensitive personnel data in history. But, to date, neither the scope nor scale of the breach, nor its significance, nor the inadequate and even self-defeating response has been fully aired.
- It appears that OPM maintained an unsecured and unencrypted database for the security clearances. A 2006 OPM report states that the "Data Repository" is premised on a "shared-disk (shared-data) model," and that "all of the disks containing databases are accessible by all of the systems."
- Along with the aforementioned databases, the OPM systems are linked electronically to other agencies and databases, and it stored much of this data alongside the security clearance files.
- Whatever actor successfully breached the OPM system potentially has pass-through access to a complete set of other extraordinarily sensitive National Security data.

Michael Adams is currently Global Director for Information Security with a Swiss-based company.

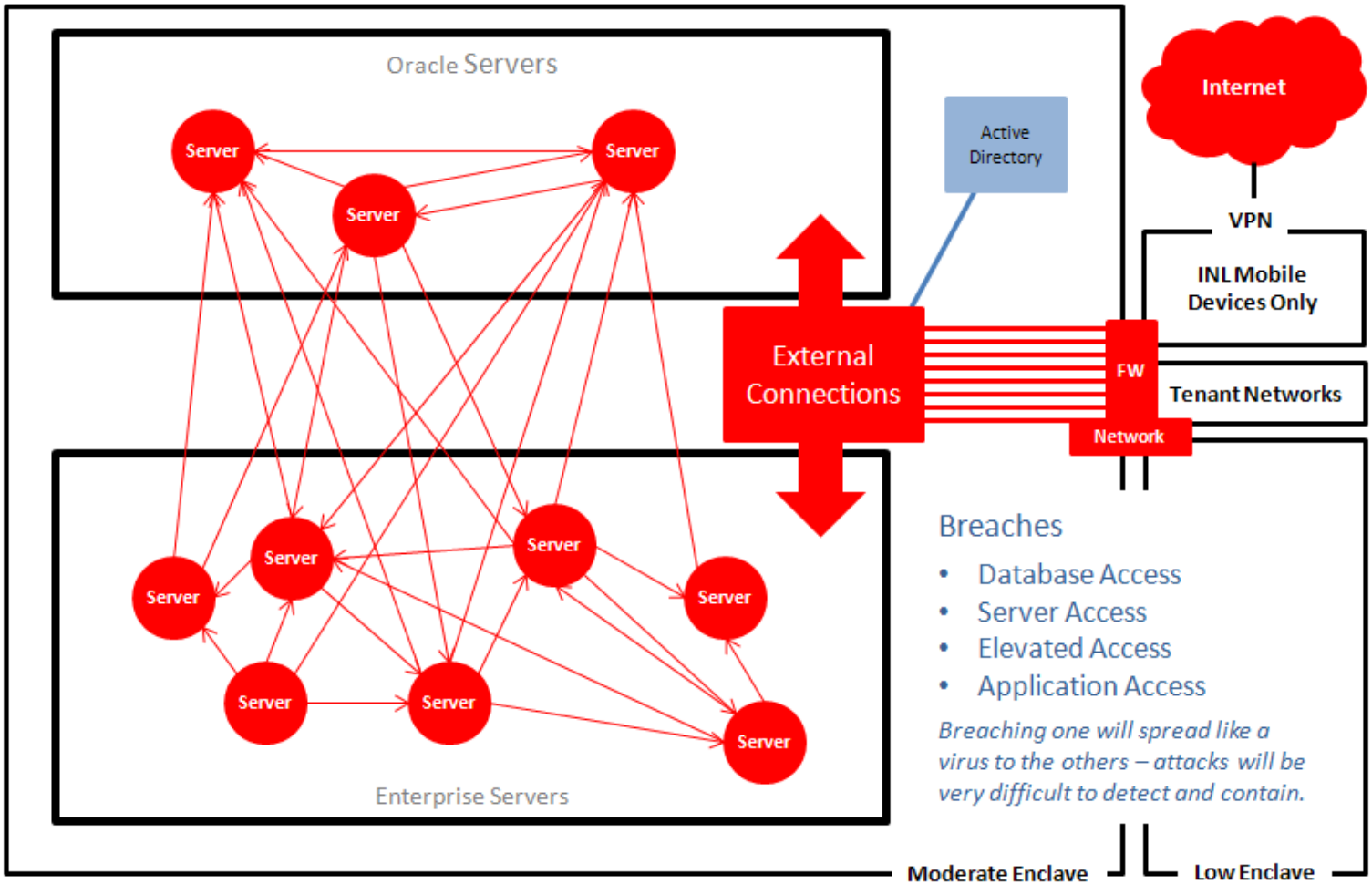
ars technica

- In the meantime, the Obama administration has ordered a “30-day Cyber-security Sprint." Agencies must perform vulnerability testing and patch existing holes in security.
- They must prune the number of privileged user accounts and expand adoption of multifactor authentication for all systems.
- The Department of Defense and intelligence community have led the way on that last requirement, but many civilian agencies (such as OPM) have been slow to put it in place.
- Just how much this "sprint" will improve government security remains to be seen, especially since agencies such as OPM have been repeatedly warned in the past about minimum "security hygiene.“
- Thirty days is not likely enough time to correct a decade-plus of neglect of antiquated systems, poor leadership, and spotty attempts at modernization.

by Sean Gallagher - Jun 21, 2015 8:30pm MDT

SO WHAT HAPPENED?

Too Many Open Doors



How and why is data breached?

- It usually caused by two factors
  - Neglect
  - Insecure Practices
- Some reasons why they occur
  - Ego
  - Curiosity
  - Whistle blowing
  - Disgruntled employee
  - Financial gain
  - Coercion
  - Cyber warfare

Logging and Auditing (Opinion)

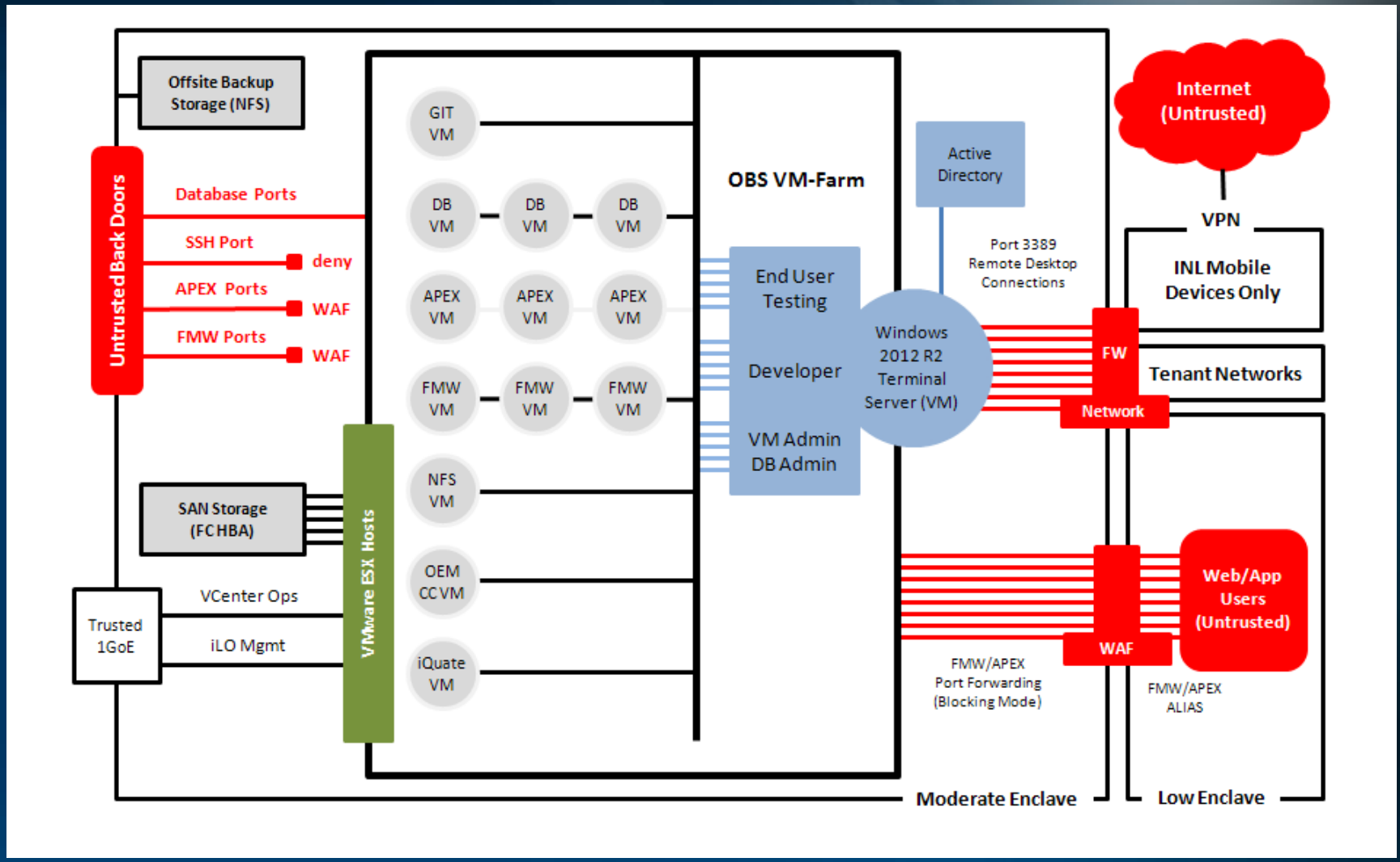
- May alert you to an attack – but only if someone is watching.
- Definitely can be used to confirm you have been breached.
- Absolutely will not prevent you from being breached.

This is a reactive-based strategy useful only after the fact for “lessons learned” analysis.

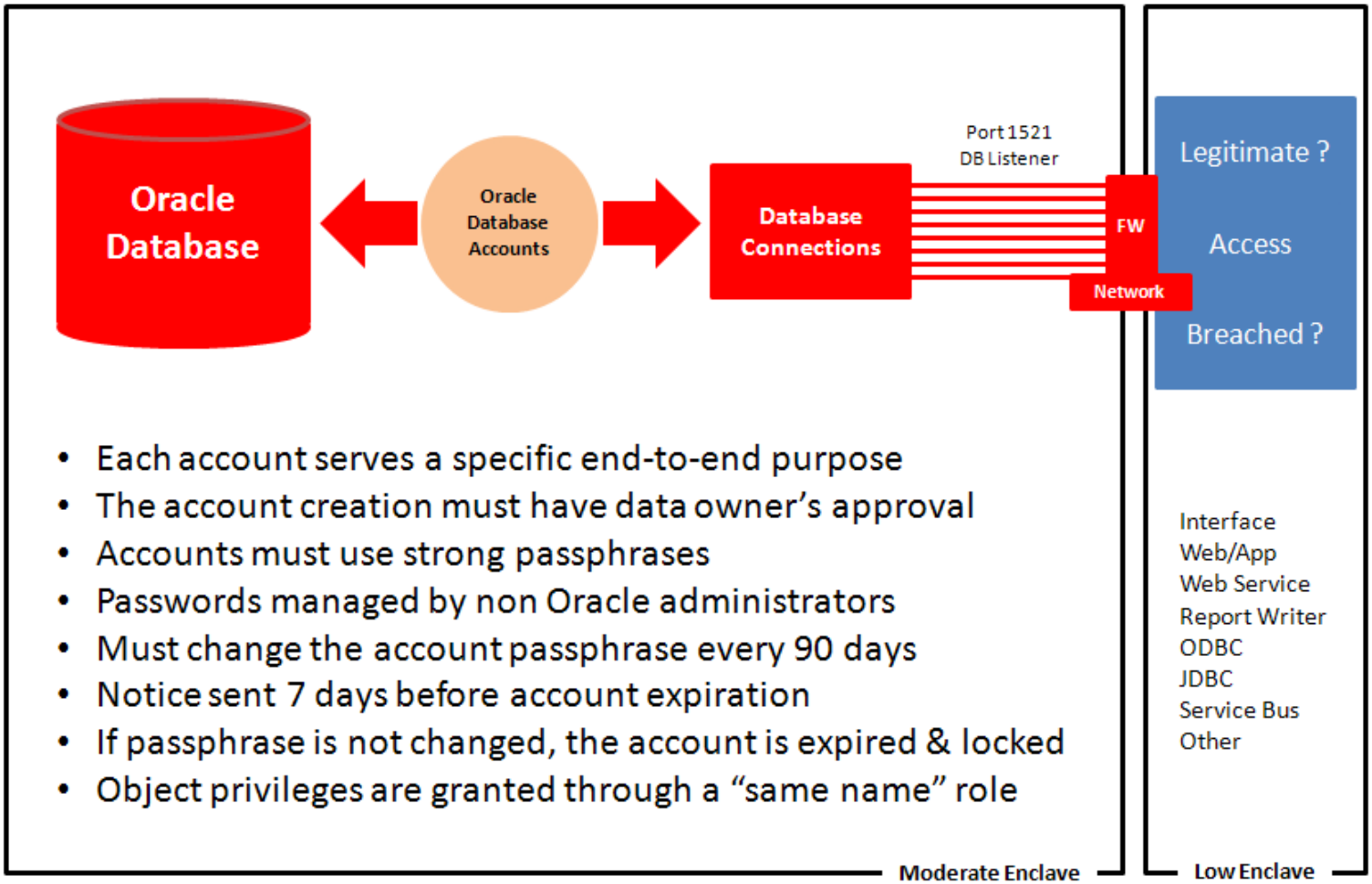
Don’t make this your front-line defense strategy.

WHAT WE ARE DOING …

Locking Down Access



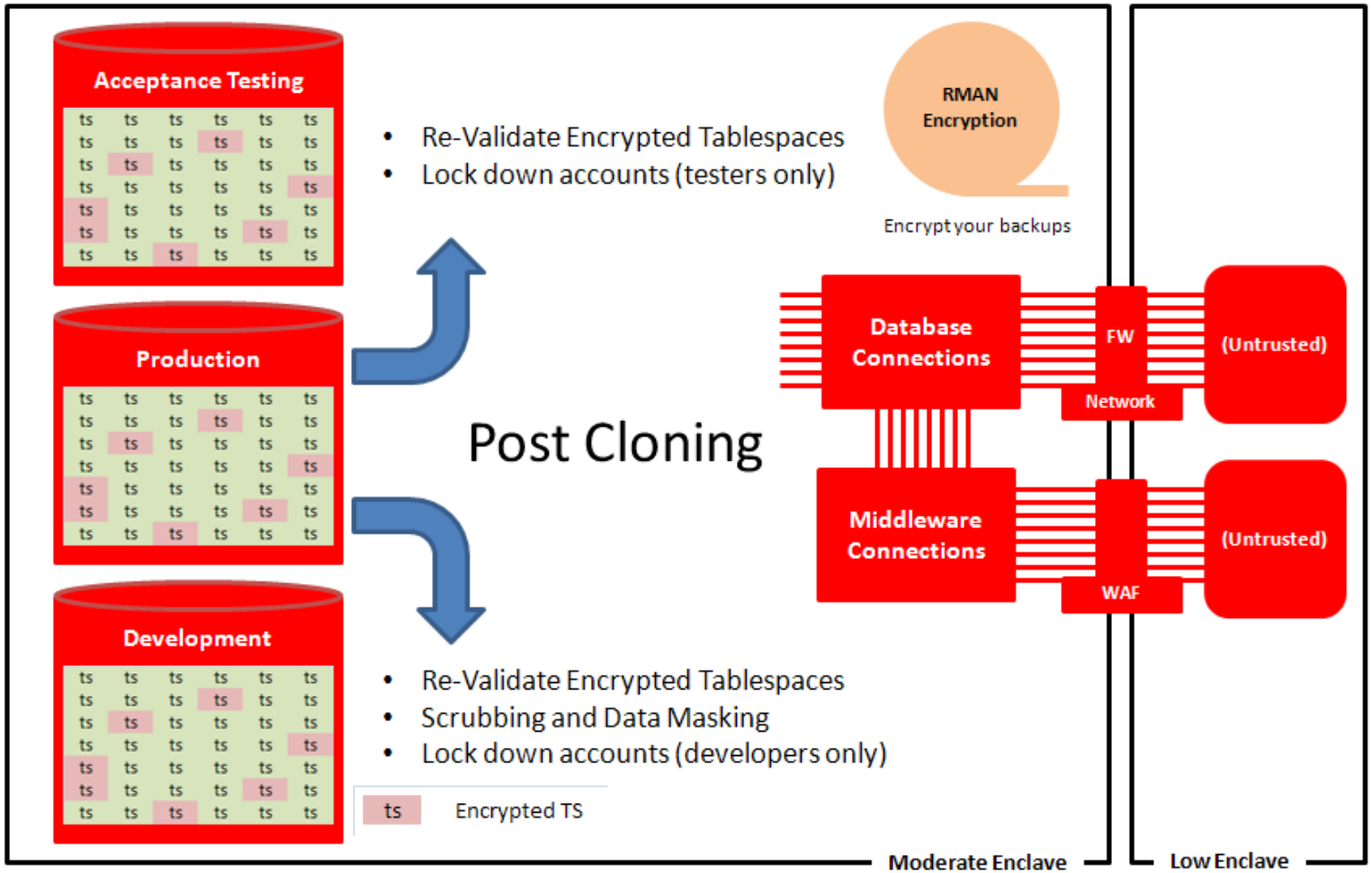
Preventing Account and Role Misuse



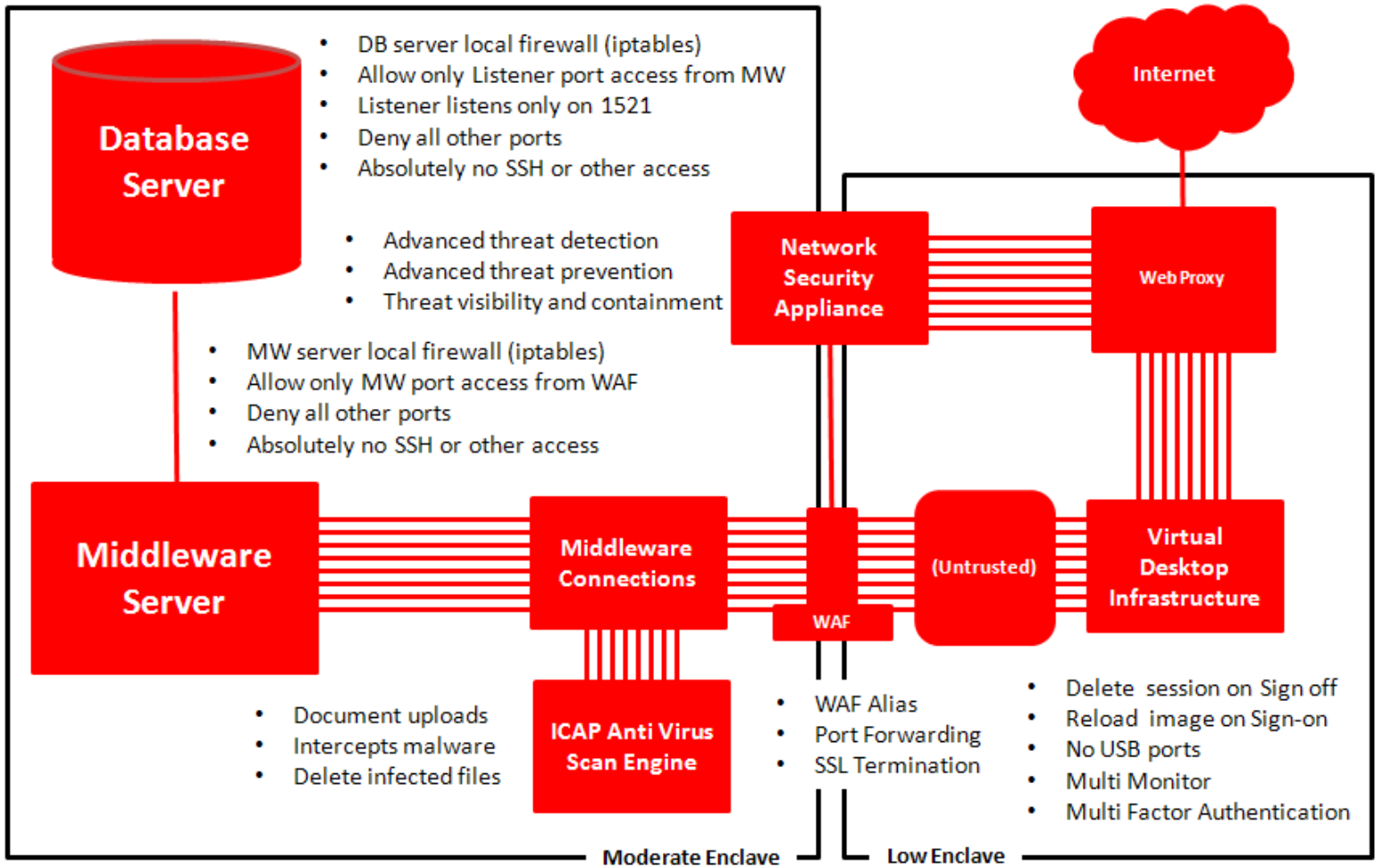
- Each account serves a specific end-to-end purpose
- The account creation must have data owner's approval
- Accounts must use strong passphrases
- Passwords managed by non Oracle administrators
- Must change the account passphrase every 90 days
- Notice sent 7 days before account expiration
- If passphrase is not changed, the account is expired & locked
- Object privileges are granted through a "same name" role

Interface
Web/App
Web Service
Report Writer
ODBC
JDBC
Service Bus
Other

Refresh and Lockdown



Hardening the Middleware



Questions?