Architecting your success

Simon Rice, VP Enterprise Services, Cintra

Jon Kobrick, COO, STI Group

Modern Data Security

Critical information to keep your data platform secure against cyber-security threats

Cintra …

Driving World Class Oracle Architecture Solutions, Services and Support

Oracle Architecture Expertise

Oracle on Oracle Architecture & Cloud Solutions

Applications
Middleware
Database
Operating System
Virtual Machine
Servers
Storage

Proactive Expert Oracle Managed Services

Oracle Commercial Expertise

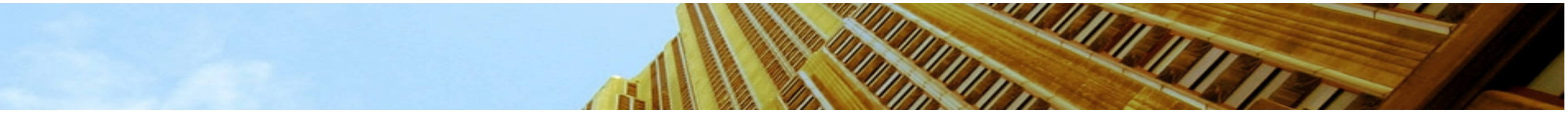
- Oracle architecture expertise driving modernization and transformation
- Oracle architecture blueprints driving the Oracle on Oracle and cloud solutions
- Oracle proactive 24x7 expert managed services for operational excellence
- Oracle commercial licensing expertise driving greater value and efficiencies

STIGroup…

Balancing Information Security Investment with Risk Mitigation

CyberSecurity Consulting (CSC)

Managed Security Operations (MSO)

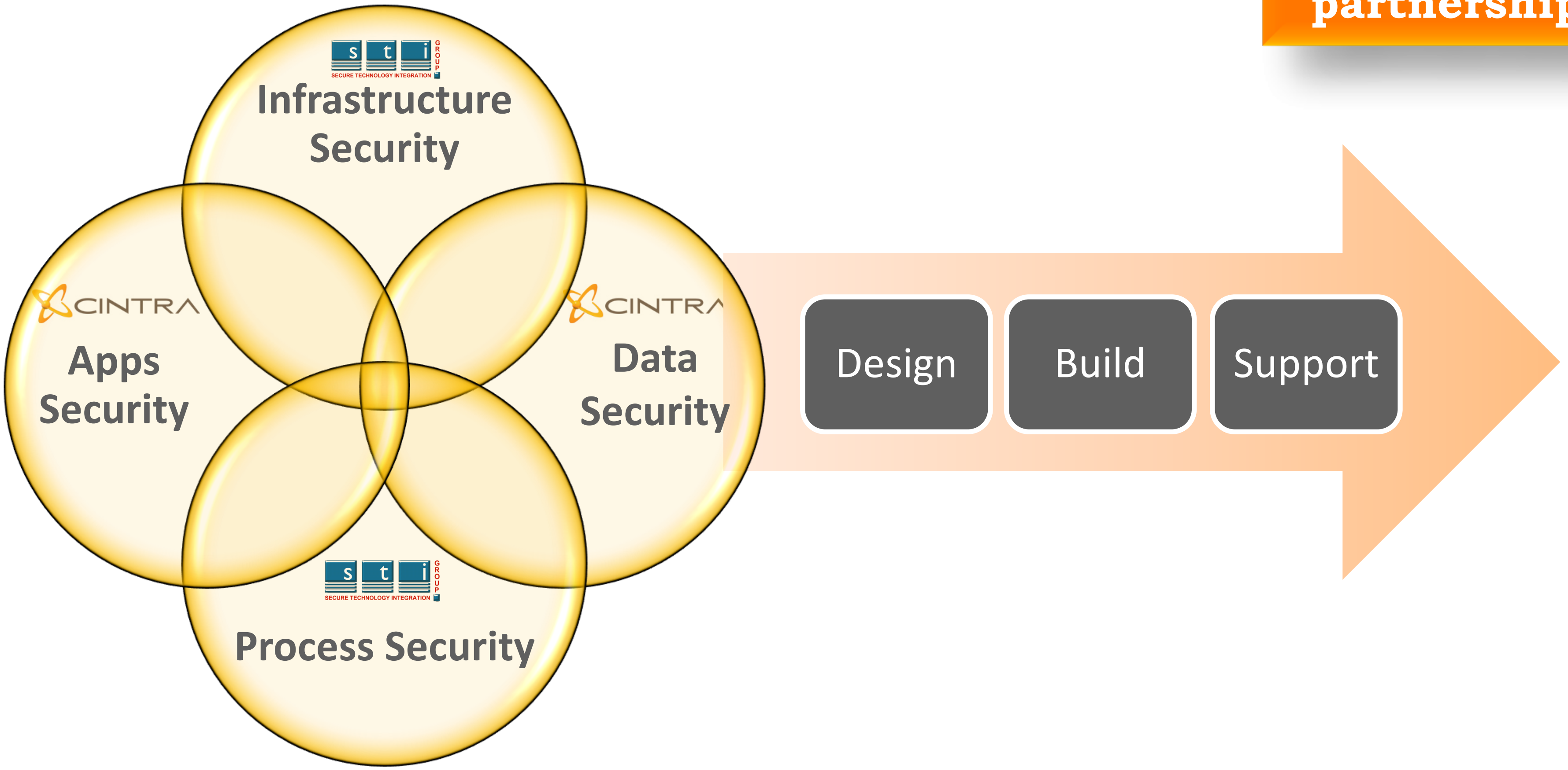


- Risk Assessment & Policy Development
- Audit & Security Posture Assessment
- Architecture, Remediation, & Certification
- Information Security Management

- Sec Ops Program Management
- Alert/Event Monitoring & Response
- Managed Breach Detection
- Security Infrastructure Management

Best of Breed Enterprise Security Alliance

12 year partnership



Infrastructure Security

Apps Security

Data Security

Process Security

Design

Build

Support

Cintra / STI Tiered Security Model

Level	Definition
DEFCON1	Secured in line with top security clearance standards.
	Extreme access control in line with stringent change management processes.
	Access to information locked down and governed by CISO.
DEFCON2	Secured in line with regulatory compliance requirements.
	Centralized, protected audit log including superuser and data-related activities.
	Data encrypted in motion and at rest.
DEFCON3	Default state for all Cintra / STI managed services customers.
	Infrastructure, OS, DB and Apps hardening.
	Auditing of superuser activities enabled.

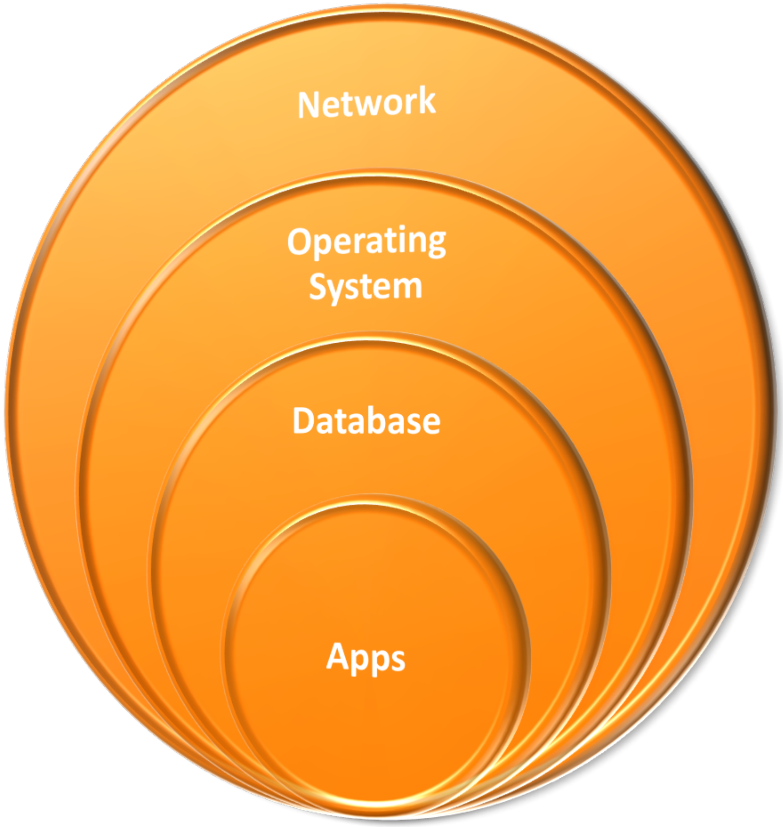
Cyber Security:

Introduction to the Modern Data Security Methodology

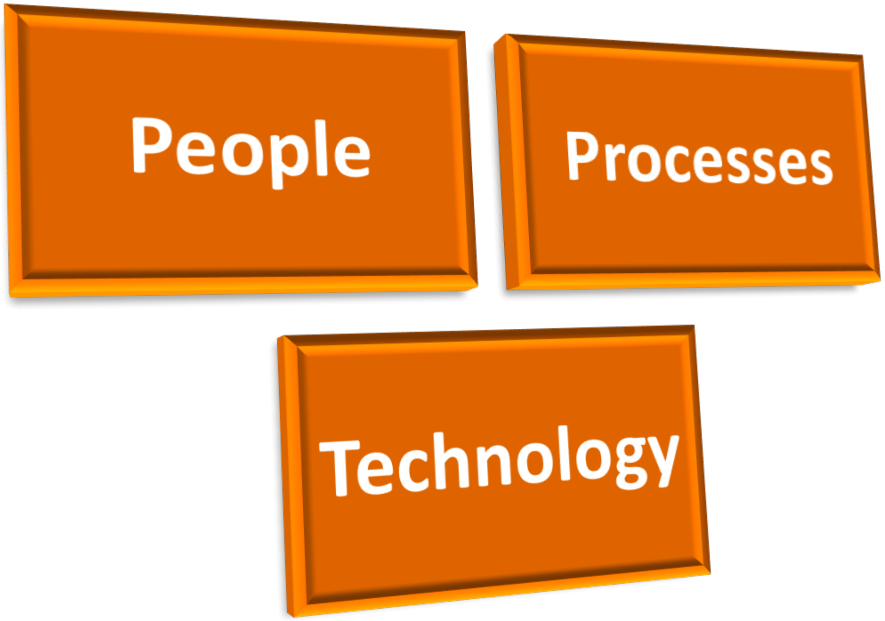
CINTRA

Security Controls Overview

Surface Area of Attack



Security Controls

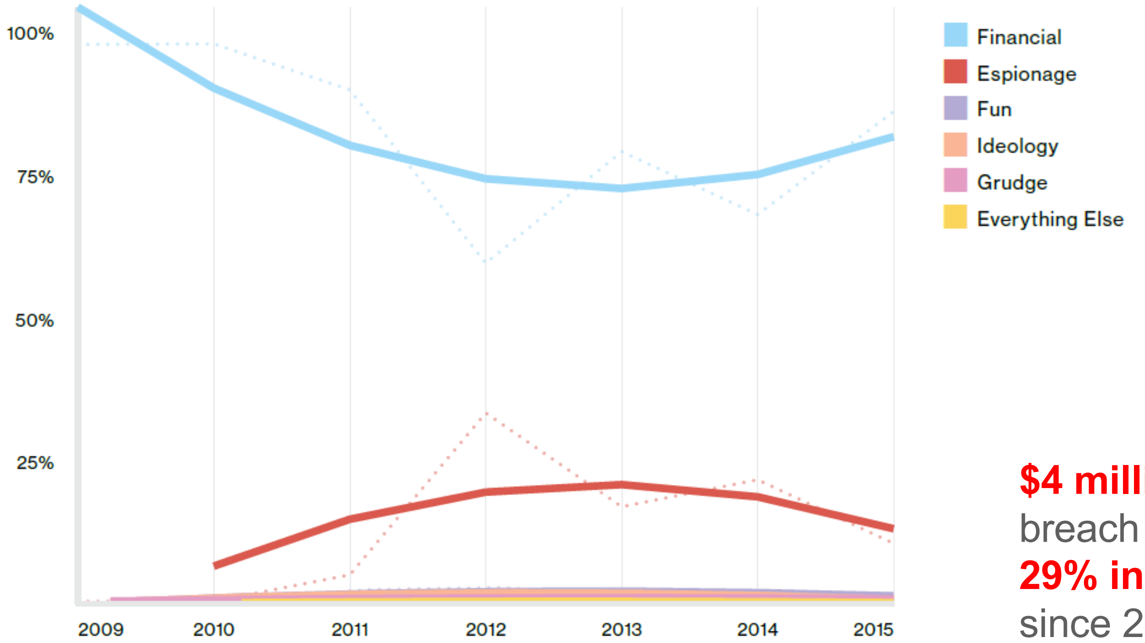


Cyber Security:

Understanding the Threat Landscape

CINTRA

Overall Breach Trends



89% of breaches had a financial or espionage motive.

$4 million is the average total cost of data breach
29% increase in total cost of data breach since 2013

$158 is the average cost per lost or stolen record
15% percent increase in per capita cost since 2013

*2016 Verizon Data Breach Investigations Report
*2016 Cost of Data Breach Study: Global Analysis, Sponsored by IBM and Conducted by Ponemon Institute LLC

Overall Breach Trends

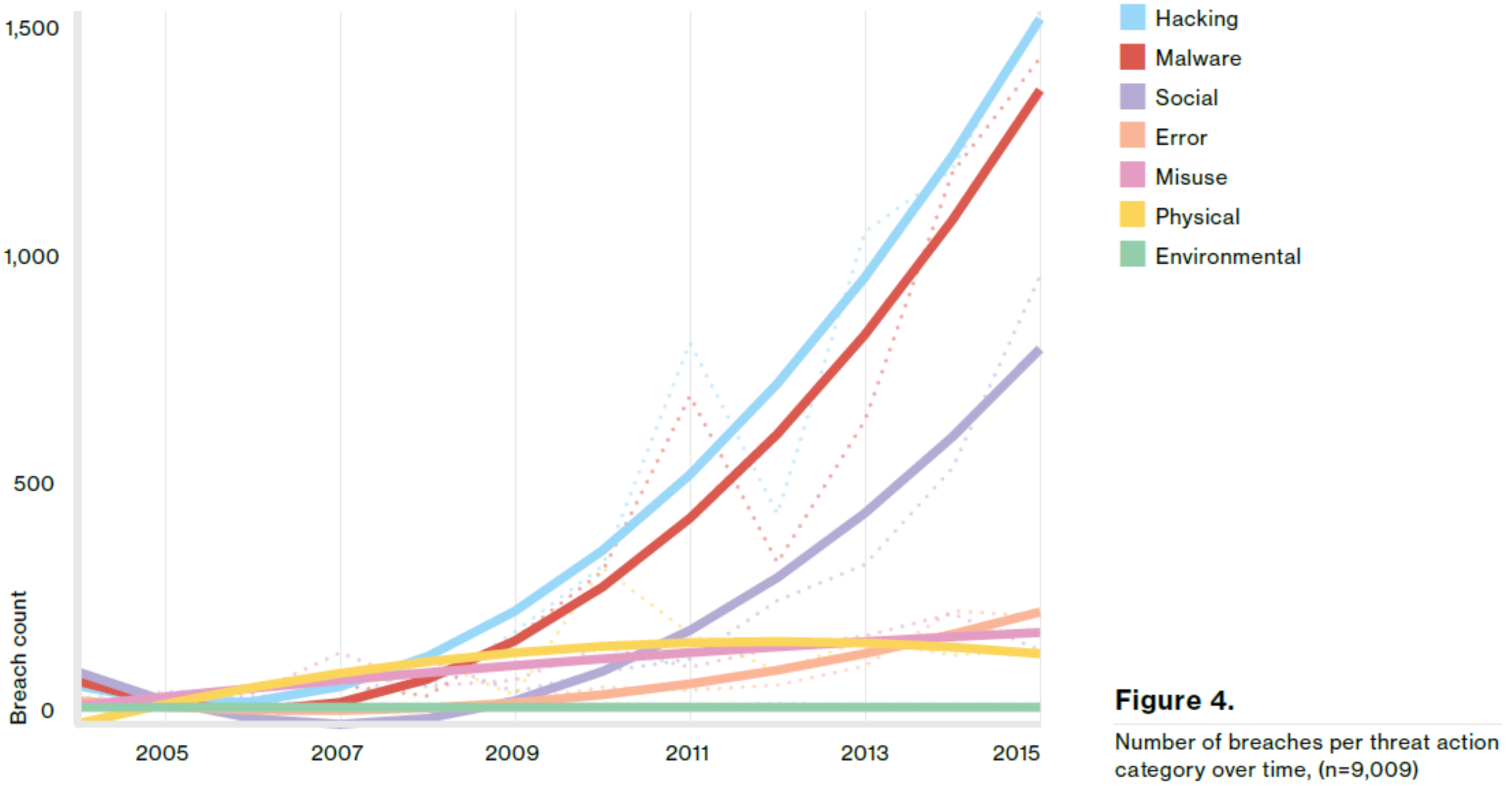
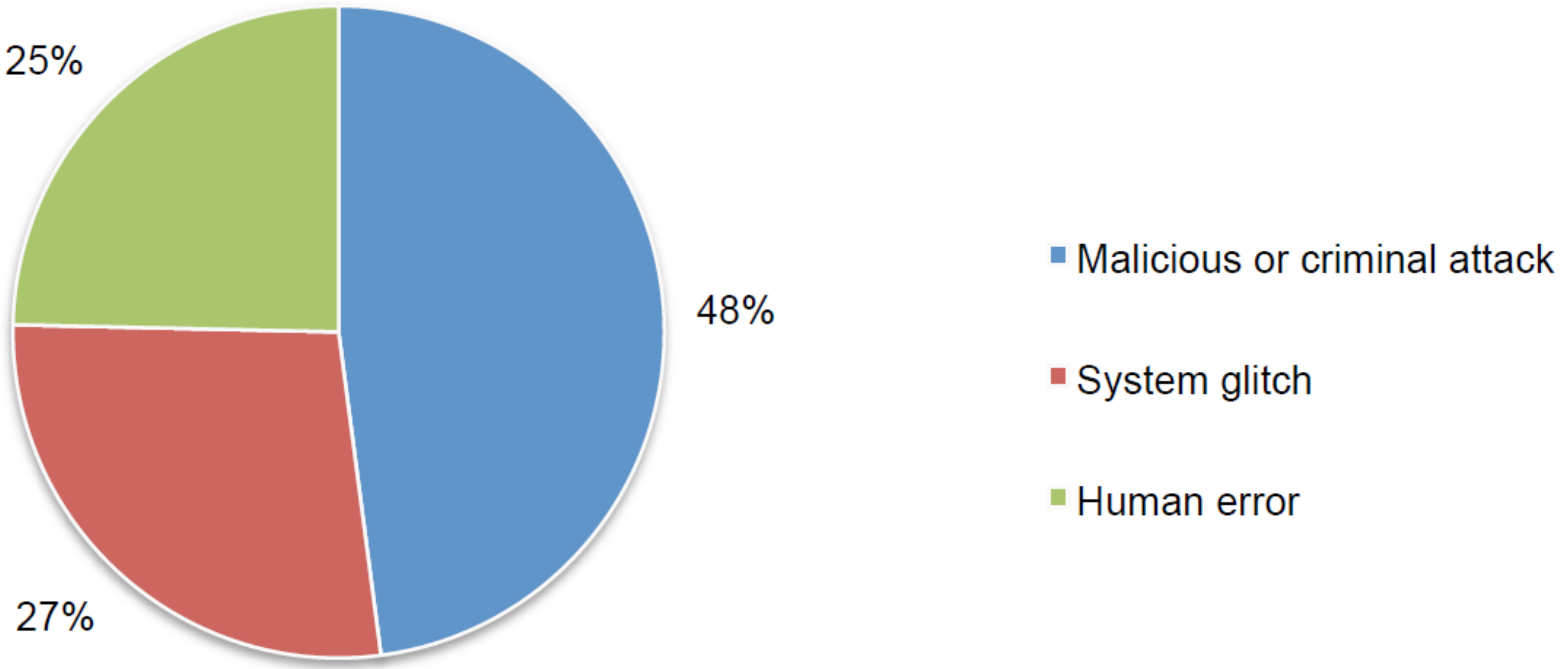


Figure 4.

Number of breaches per threat action category over time, (n=9,009)

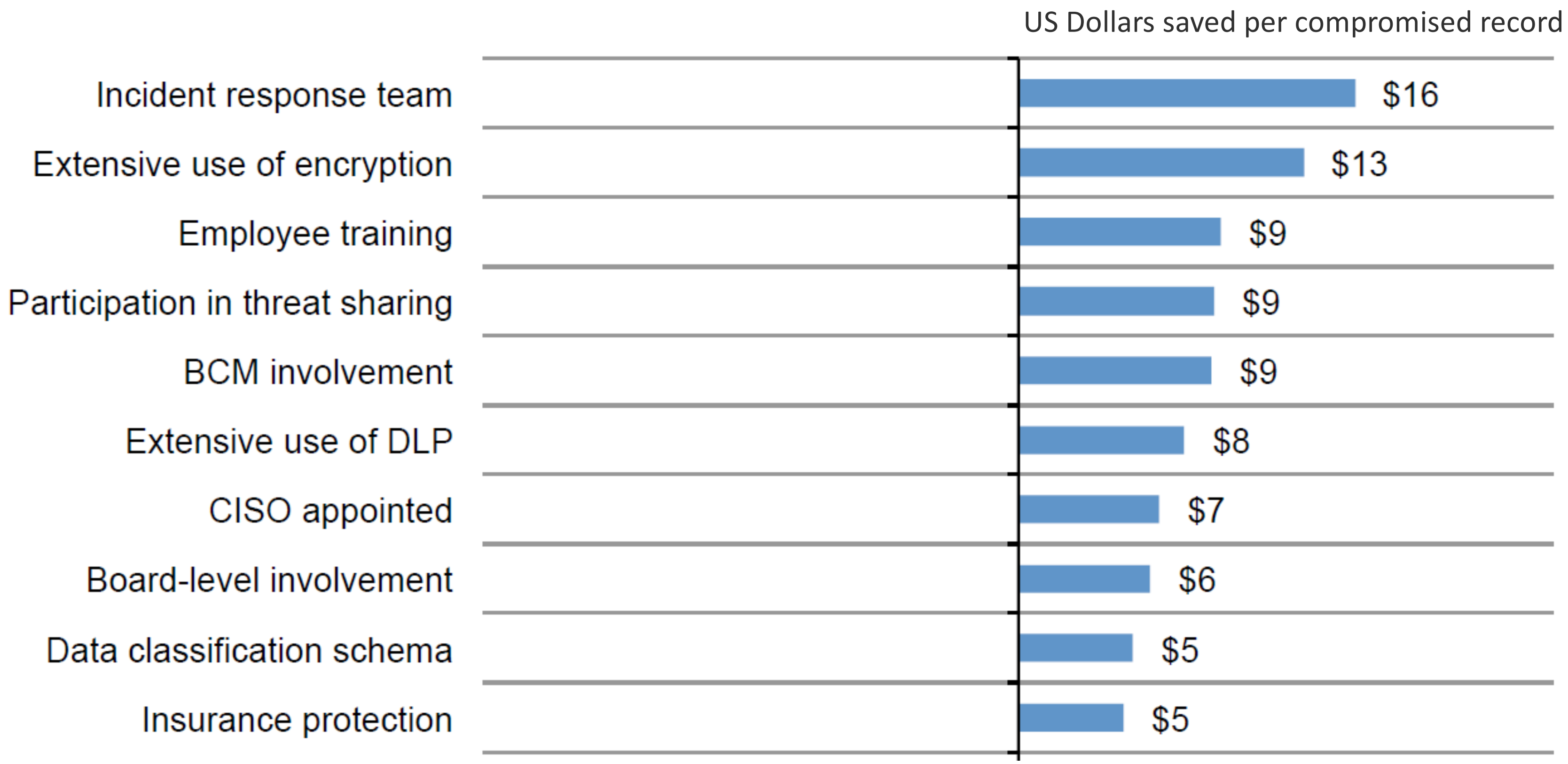
*2016 Verizon Data Breach Investigations Report

Root causes of data breach



*2016 Cost of Data Breach Study: Global Analysis, Sponsored by IBM and Conducted by Ponemon Institute LLC

Factors that reduce the cost of a data breach



*2016 Cost of Data Breach Study: Global Analysis, Sponsored by IBM and Conducted by Ponemon Institute LLC

Breach Trends – Asset Varieties

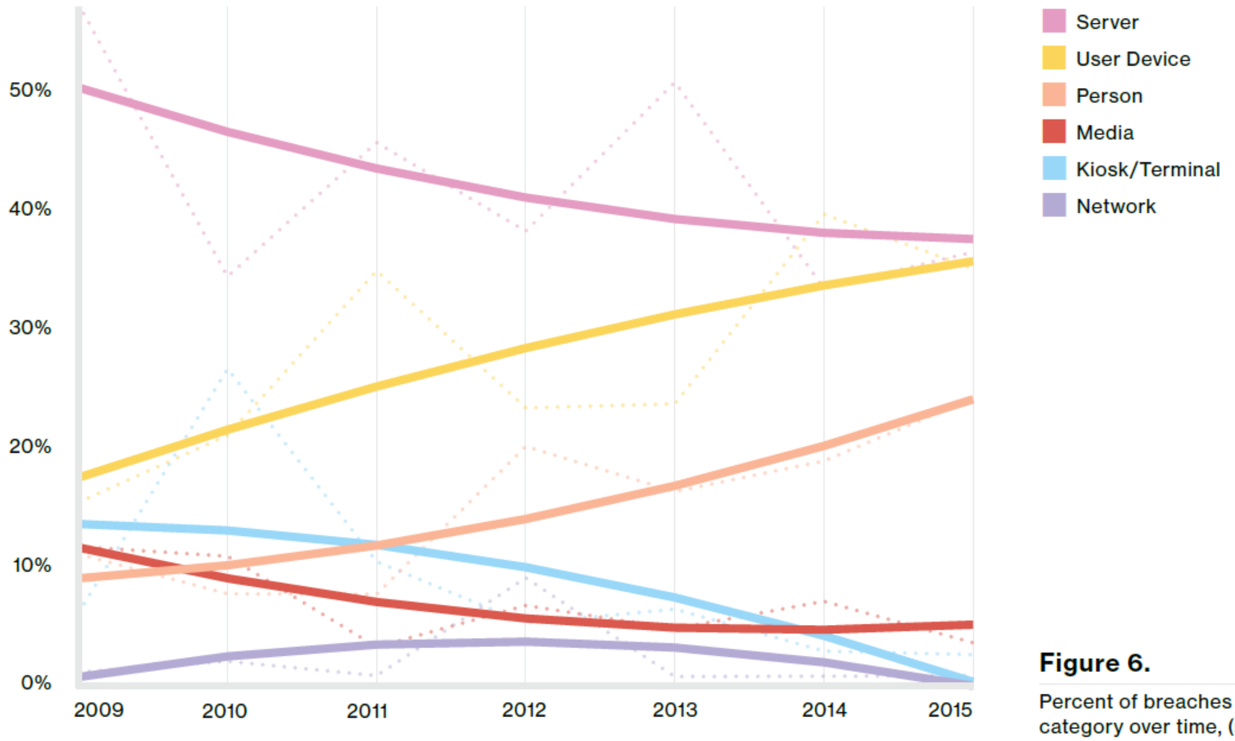
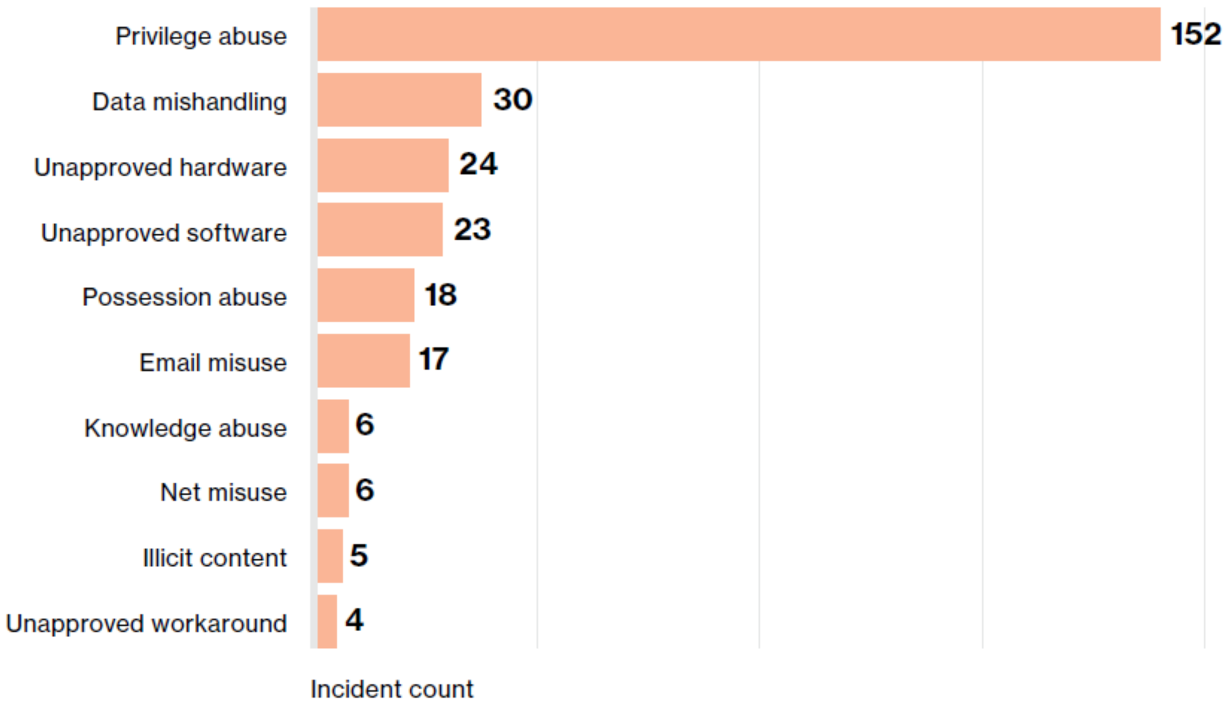


Figure 6.

Percent of breaches per asset category over time, (n=7,736)

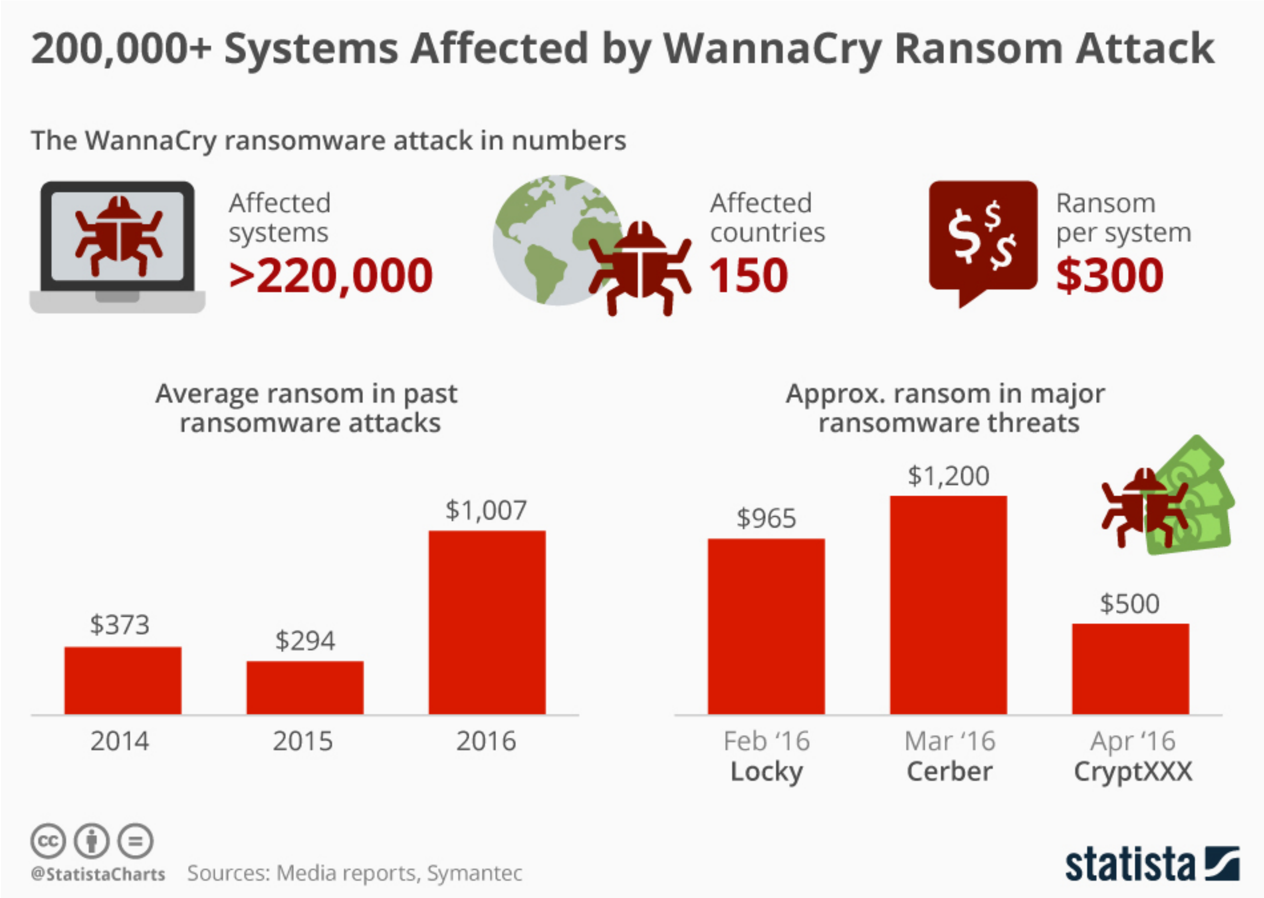
*2016 Verizon Data Breach Investigations Report

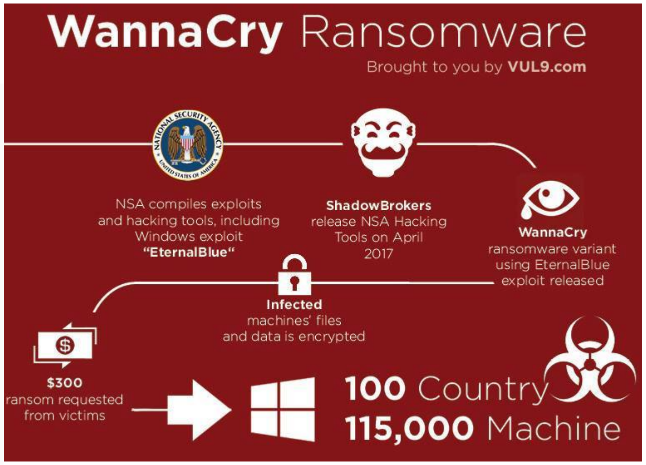
Insider and Privilege Misuse



*2016 Verizon Data Breach Investigations Report

WannaCry

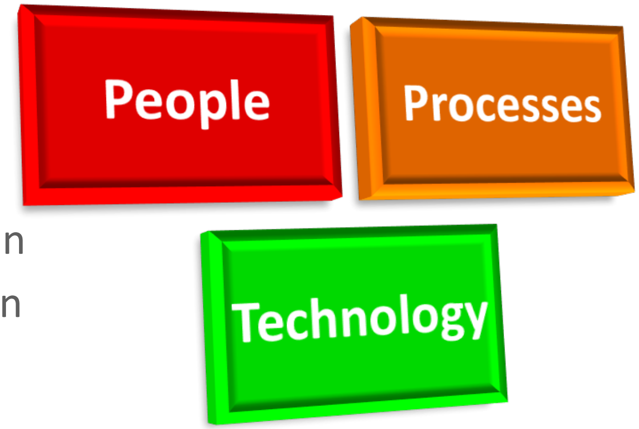

200,000+ Systems Affected by WannaCry Ransom Attack
The WannaCry ransomware attack in numbers
Affected systems
>220,000
Affected countries
150
Ransom per system
$300
Average ransom in past ransomware attacks
$373
$294
$1,007
2014
2015
2016
Approx. ransom in major ransomware threats
$965
$1,200
$500
Feb '16 Locky
Mar '16 Cerber
Apr '16 CryptXXX
@StatistaCharts
Sources: Media reports, Symantec
statista


WannaCry Ransomware
Brought to you by VUL9.com
NSA compiles exploits and hacking tools, including Windows exploit "EternalBlue"
ShadowBrokers release NSA Hacking Tools on April 2017
WannaCry ransomware variant using EternalBlue exploit released
Infected machines' files and data is encrypted
$300 ransom requested from victims
100 Country
115,000 Machine

Real Life Examples:

Cintra and STI Group Customers

Customer 1: Hospital Patient Data Loss



- **The Scenario**
  - Large hospital network
  - Patient data is encrypted, running on Oracle Enterprise Edition
  - For 18 months a nurse printed off records and sold them to an entity in Russia

- **Why did this happen?**
  - Lack of processes in place to validate unusual behavior
  - Lack of management oversight

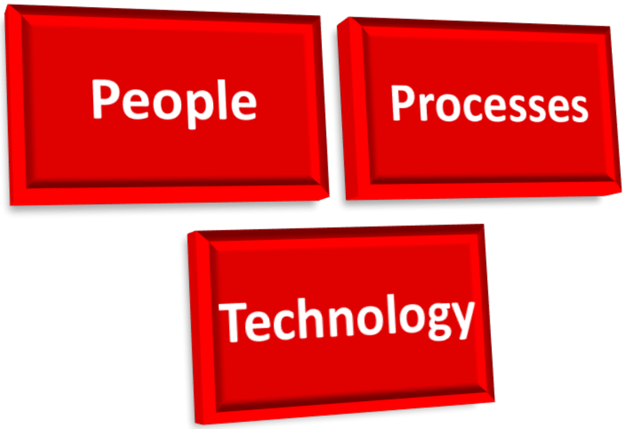
- **How did Cintra / STI help?**
  - Deployment of centralized auditing software
  - Automatic audit alerts in line with HIPAA regulations
  - Tighter staff security training and controls

Customer 2: Website Hacked

- **The Scenario**
  - Popular editorial content website
  - A web application vulnerability was exploited
  - They were after the target's customers

- **Why did this happen?**
  - Lack of application security development processes
  - Insufficient production change management and integrity monitoring

- **How did Cintra / STI help?**
  - Coordinated and executed incident response plan
  - Conducted log analysis and code review
  - Implemented enhanced integrity monitoring

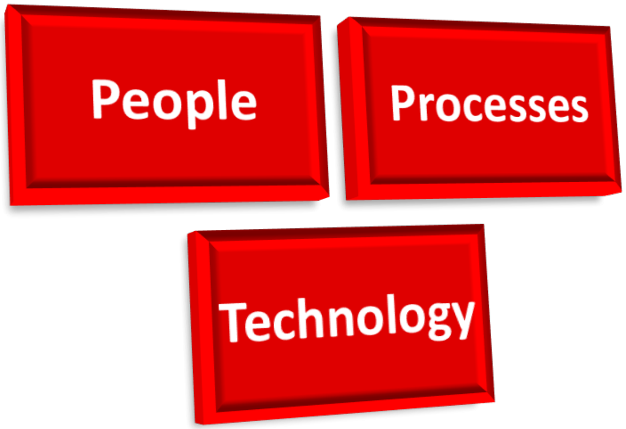


People

Processes

Technology

Customer 3: Retail POS Breach


People

Processes

Technology

- **The Scenario**
  - Retail sites with hundreds of POS machines
  - Compromise through insecure remote access configuration
  - Attacker lateral movement

- **Why did this happen?**
  - Poor security configuration hardening
  - Excessive privilege assignment

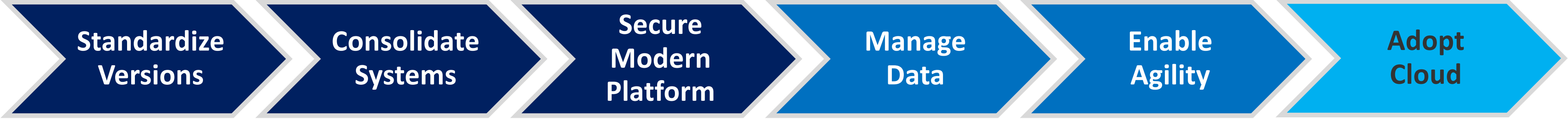
- **How did Cintra / STI help?**
  - Developed secure configuration standard
  - Implemented more robust access management solution

Cyber Security:

Architecting for Security

CINTRA

The Modern Architecture Journey Requires Modern Security



Standardize Versions → Consolidate Systems → Secure Modern Platform → Manage Data → Enable Agility → Adopt Cloud

Lower Costs

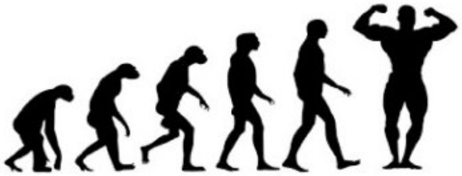
Faster Time To Market

Business Focus

Innovation Focus

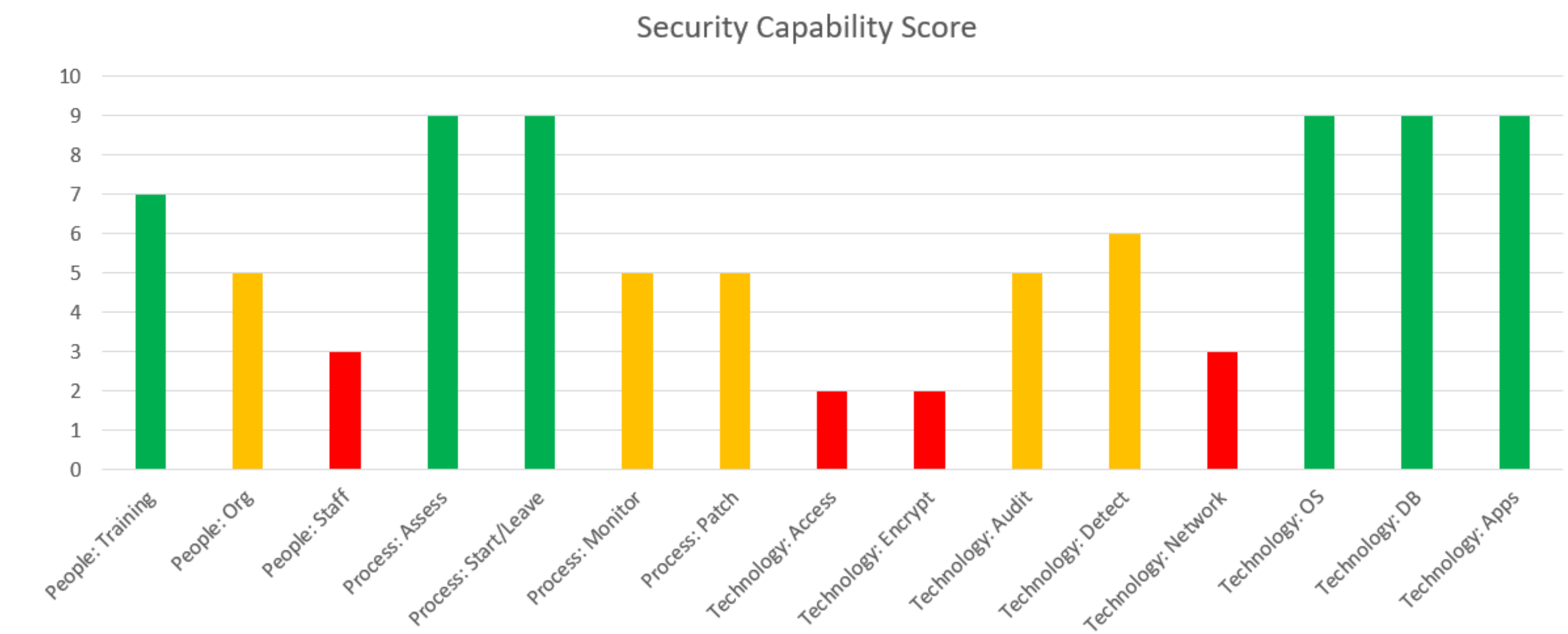
Traditional Security models are no longer sufficient in today's modern landscape

Assessing Against Modern Cyber Security Standards



We perform honest assessments of database architectures

Architecture Eleme	Current Capability
People: Training	
People: Org	
People: Staff	
Process: Assess	
Process: Start/Lea	
Process: Monitor	
Process: Patch	
Technology: Acces	
Technology: Encry	
Technology: Audit	
Technology: Detec	
Technology: Netw	
Technology: OS	
Technology: DB	
Technology: Apps	

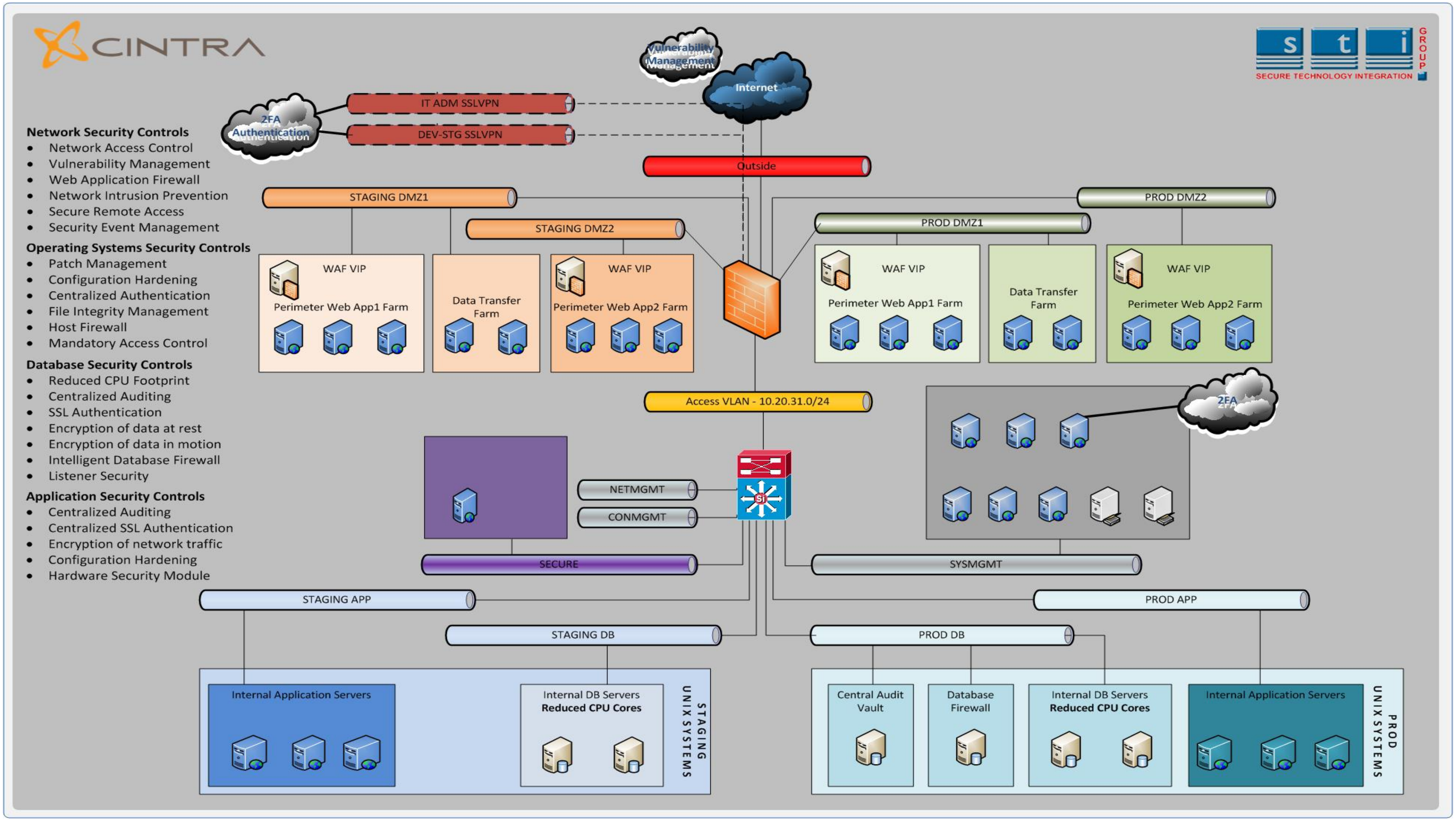


CINTRA

sti GROUP SECURE TECHNOLOGY INTEGRATION

CINTRA

sti GROUP
SECURE TECHNOLOGY INTEGRATION



Network Security Controls

- Network Access Control
- Vulnerability Management
- Web Application Firewall
- Network Intrusion Prevention
- Secure Remote Access
- Security Event Management

Operating Systems Security Controls

- Patch Management
- Configuration Hardening
- Centralized Authentication
- File Integrity Management
- Host Firewall
- Mandatory Access Control

Database Security Controls

- Reduced CPU Footprint
- Centralized Auditing
- SSL Authentication
- Encryption of data at rest
- Encryption of data in motion
- Intelligent Database Firewall
- Listener Security

Application Security Controls

- Centralized Auditing
- Centralized SSL Authentication
- Encryption of network traffic
- Configuration Hardening
- Hardware Security Module

The Cloud Journey Starts with A Secure Foundation

HYBRID ENTERPRISE CLOUD

YOUR CLOUD

12c
Consolidate. Compress. Control.
11g
ORACLE 11g DATABASE

Private Cloud

- Cloud Maturity
- No Security Compromises
- Matched or Greater Controls
- Matched or Greater Capabilities
- <u>Not all clouds are created equal!</u>

PUBLIC CLOUD

12c
Consolidate. Compress. Control.
11g
ORACLE 11g DATABASE

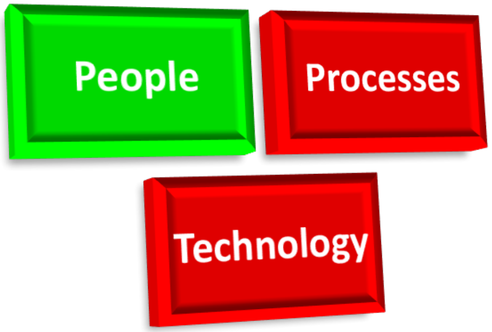
Public Cloud

Cyber Security:

General Recommendations

CINTRA

Security Considerations: People



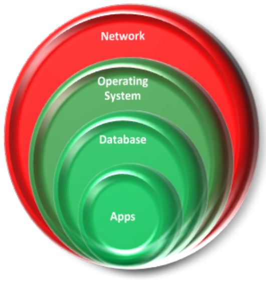
People
Training – Commercial, in house, on the job, etc.
Security Accountability – formally assigned responsibilities
Sufficient Resources – sufficient time for security tasks
Performance Metrics – measure, measure, measure

Cyber Security:

Network Security

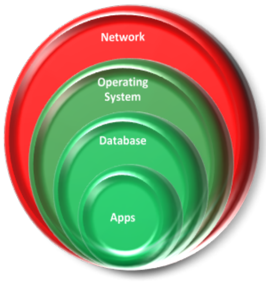
CINTRA

Network Security Considerations: Process Best Practices



Processes
Change Control
Configuration Management
Vulnerability Management
Configuration Hardening
Security Monitoring

Network Security Considerations: Technology Best Practices

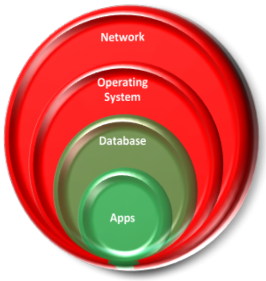


Technology
Firewalls, ACLs, Network Segmentation, Private VLANs
Signature IPS/AV, Threat Emulation, Network Behavior Monitoring
Data Loss Prevention
Encryption, TLS, IPSec, GRE, SSH
Network Access Control, Port Security
Secure Remote Access/Multi-Factor Authentication

Cyber Security:

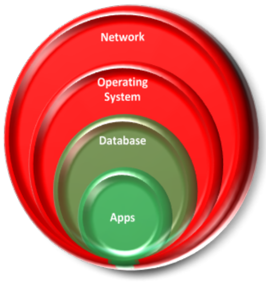
Operating System Security

Operating System Security Considerations: Processes



Processes
Security Operations Assessment
Security Monitoring
Vulnerability Management
Security Administration
Device and Software Inventory
Privilege / RBAC Review

Operating System Security Considerations: Technology

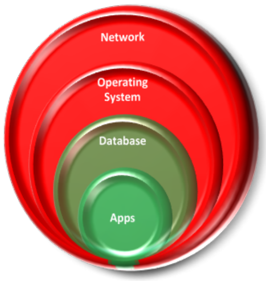


Technology
Endpoint Security (Anti-malware/AV, EDR, DLP, etc.)
Disk and File System Encryption
Mandatory Access Control System, Application Whitelisting
System and Process Accounting, Logging, EDR
File Integrity Management
Privilege Escalation Management

Operating System Security Considerations

CIS Oracle Linux 7 Benchmark

v2.0.0 - 06-02-2016



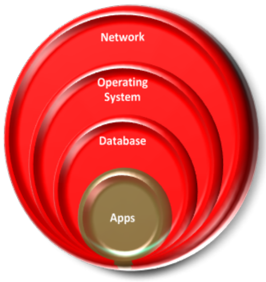
1. Initial setup
    1. File system configuration
    2. Configure software updates
    3. Filesystem integrity checking
    4. Secure boot settings
    5. Additional boot settings
    6. Mandatory access control
    7. Warning banners
2. Services
    1. Inetd services
    2. Special purpose services
    3. Service clients
3. Network configuration
    1. Network parameters (host only)
    2. Network parameters (host and router)
    3. IPv6
    4. TCP wrappers
    5. Uncommon network protocols
    6. Firewall configuration
4. Logging and Auditing
    1. Configure system accounting (auditd)
    2. Configure logging
5. Access, Authentication and Authorization
    1. Configure cron
    2. SSH server configuration
    3. Configure PAM
    4. User accounts and environment
6. System Maintenance
    1. System file permissions
    2. User and Group Settings

Cyber Security:

Database Security

CINTRA

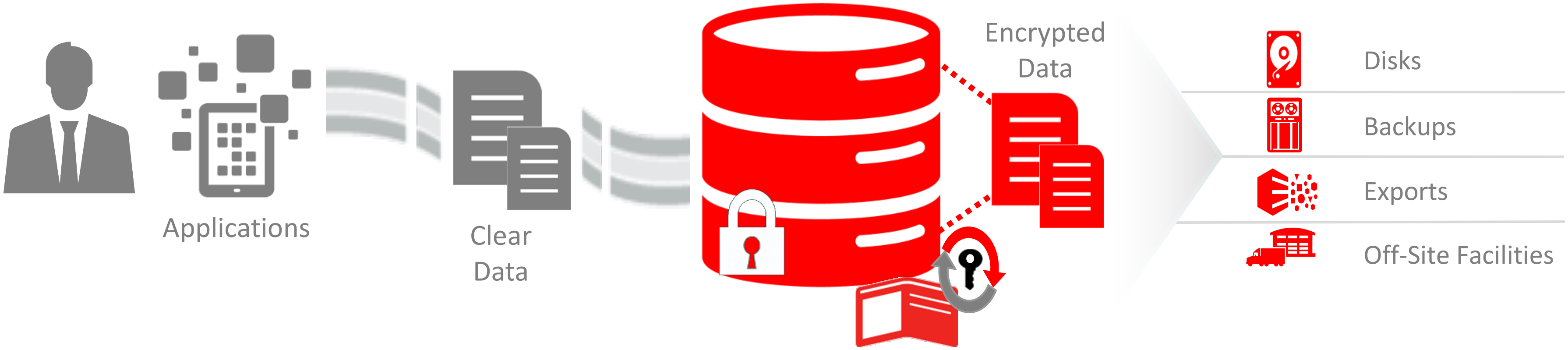
Database Security Considerations: Technology



Technology
Encryption – personally identifiable information is encrypted at rest and in transit and that database logons are encrypted.
Auditing – superuser access or access to sensitive data is audited, with triggered alerts.
Patch Procedures – database clusters and instances are patched with the latest security fixes at least quarterly.
Access Controls – least-privileged access, with deactivation on termination.
Intelligent Firewalls – SQL injection attack protection from software firewalls.
Complete Vaulting – Total lockdown of administrative and database access using vault technology.
Oracle Listeners – Non-standard ports, white-lists of allowed hosts, password protection

Transparent Data Encryption

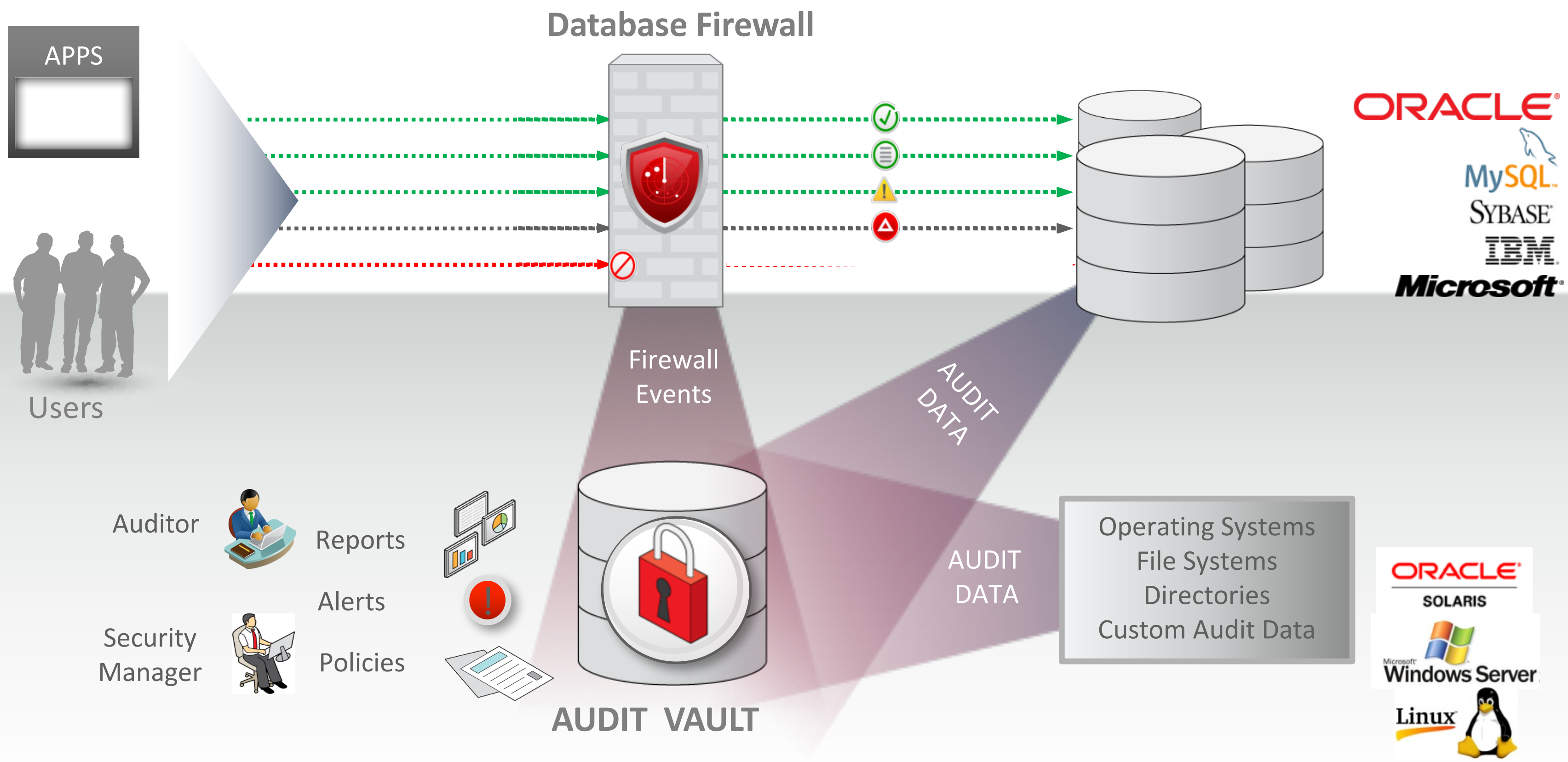
Feature Summary



- Encrypts columns or entire application tablespaces
- Protects the database files on disk and on backups
- Transparent to applications, no changes required
- High-speed performance, low overhead
- Optimized for Exadata

ORACLE JDEDWARDS
SIEBEL SAP
PeopleSoft.

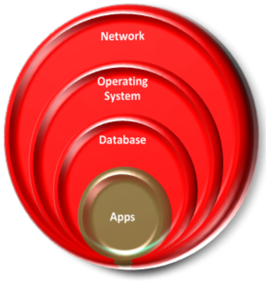
Oracle Audit Vault and Database Firewall



ORACLE

CINTRA

Database Security Considerations



3.0 Oracle Database Hardening – Oracle 11gR2

- 3.1 User Accounts Security: General Best Practices
- 3.2 Data Access from Non-Prod Databases
- 3.3 Non-default Database Naming is in place
- 3.4 Database Configuration Parameters
- 3.5 Implement profiles to enforce user security and compliance
- 3.5.1 Assign Profiles Appropriately
- 3.6 Empty caches during database shutdown
- 3.7 Storage is sufficient to prevent DoS attacks
- 3.8 Users have appropriate privileges and tablespace quota
- 3.9 Public access to sensitive packages has been removed
- 3.10 Regularly review changes to database objects
- 3.11 Production exports and backups are secure
- 3.12 Large objects (LOBs) are stored securely
- 3.13 Audit Java access to the O/S
- 3.14 Oracle Text Option

4.0 Oracle Auditing

- 4.1 Implement Auditing to Dedicated Tablespace
- 4.1.1 Audit Tablespace Defined with ASSM
- 4.2 Database auditing is configured appropriately
- 4.3 Ensure Audit Information is Regularly Reviewed
- 4.4 Ensure Audit Trail Records are Regularly Purged

5.0 Oracle Wallet Management for 11gR2

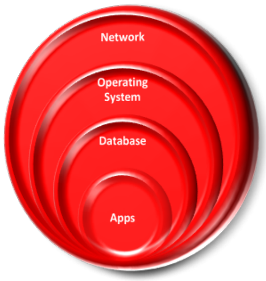
- 5.1 Using Oracle Transparent Data Encryption
- 5.1.1 Using Different Encryption Algorithms
- 5.1.2 Encrypting External Tables
- 5.1.3 Removing Encryption
- 5.1.4 Tablespace Encryption
- 5.2 Restricted Access to Oracle Wallets
- 5.3 Wallet passwords and keys are cycled at regular intervals
- 5.4 Oracle Wallets are configured optimally for RAC

Cyber Security:

Application Security

CINTRA

Application Tier Security Considerations: Technology



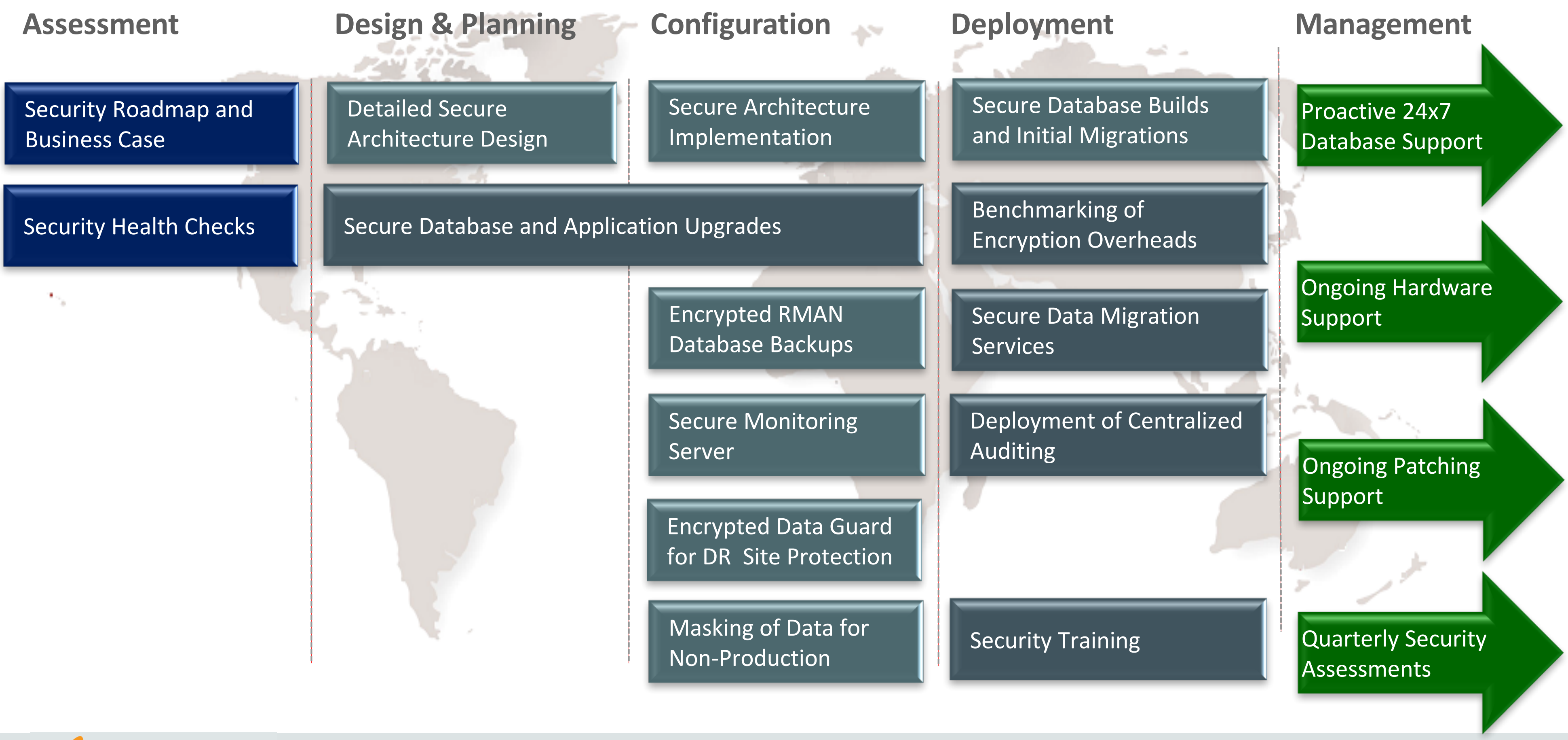
Technology
Encryption – of traffic between the database and app server and of traffic between the web tier and app tier.
Auditing – monitoring of performance baselines and suspicious activity.
Patch Procedures – full technology stack patching every quarter. More aggressive patching of public-facing assets.
Access Controls – integration with controlled LDAP directories where possible. Adoption of least-required privileges.
Hardware Security Modules – adoption of HSM to lock down web and app tier traffic.
Dedicated, secure domains – Java container design to ensure no commonality between clients / apps / environments.
Mobile Security – ensure that mobile access points are locked down and accessed appropriately.

Cyber Security:

Wrapping Up

CINTRA

Cyber Security: How can Cintra and STI Group help?



Assessment

- Security Roadmap and Business Case
- Security Health Checks

Design & Planning

- Detailed Secure Architecture Design
- Secure Database and Application Upgrades

Configuration

- Secure Architecture Implementation
- Encrypted RMAN Database Backups
- Secure Monitoring Server
- Encrypted Data Guard for DR Site Protection
- Masking of Data for Non-Production

Deployment

- Secure Database Builds and Initial Migrations
- Benchmarking of Encryption Overheads
- Secure Data Migration Services
- Deployment of Centralized Auditing
- Security Training

Management

- Proactive 24x7 Database Support
- Ongoing Hardware Support
- Ongoing Patching Support
- Quarterly Security Assessments

CINTRA

What’s Next: Database Security Assessment / Design

- **Contact us today :** info@cintra.com

- **Assess the security of your current Database platform and identify any gaps**
- **Build a business case for a modern, secure Database architecture**
- **Maximize your investment in Oracle Software and adopt security options**
- **Establish a Cintra and STI Group partnership for expert Oracle architecture guidance**
- **Benefit from Security-Focused Proactive Expert 24x7 Managed Services Support**