Compliance & Data Protection in the Big Data Age - MongoDB Security Architecture

Mat Keep
MongoDB Product Management & Marketing
mat.keep@mongodb.com
@matkeep
Agenda

• Data Security Landscape and Challenges
• Best Practices and MongoDB Implementation
• Resources to Get Started
Security Breaches: More Users, More Cost

http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
...and it’s getting worse

- **$5.4m** average cost of a data breach

- **10%** annual growth in financial impact of cybercrime

- **96%** of thefts come from database records

Source: Symantec
Security: #2 Spending Increase

<table>
<thead>
<tr>
<th>Category</th>
<th>2014 Spending Will Increase</th>
<th>2014 Spending Will Stay Flat</th>
<th>2014 Spending Will Decrease</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud computing services (N=276)</td>
<td>72%</td>
<td>21%</td>
<td>6%</td>
</tr>
<tr>
<td>Security (N=261)</td>
<td>62%</td>
<td>31%</td>
<td>7%</td>
</tr>
<tr>
<td>Virtualization/private cloud infrastructure software (N=197)</td>
<td>52%</td>
<td>39%</td>
<td>9%</td>
</tr>
<tr>
<td>Storage infrastructure (N=306)</td>
<td>52%</td>
<td>31%</td>
<td>17%</td>
</tr>
<tr>
<td>Network infrastructure (N=301)</td>
<td>49%</td>
<td>38%</td>
<td>14%</td>
</tr>
<tr>
<td>Business intelligence/analytics (N=187)</td>
<td>48%</td>
<td>45%</td>
<td>7%</td>
</tr>
<tr>
<td>Server infrastructure (N=337)</td>
<td>47%</td>
<td>38%</td>
<td>15%</td>
</tr>
<tr>
<td>Databases (N=282)</td>
<td>46%</td>
<td>44%</td>
<td>10%</td>
</tr>
<tr>
<td>Business applications (N=261)</td>
<td>46%</td>
<td>41%</td>
<td>14%</td>
</tr>
<tr>
<td>Infrastructure management software (N=178)</td>
<td>43%</td>
<td>46%</td>
<td>12%</td>
</tr>
<tr>
<td>Endpoint computing devices (N=175)</td>
<td>41%</td>
<td>46%</td>
<td>13%</td>
</tr>
<tr>
<td>Information management software (N=168)</td>
<td>40%</td>
<td>48%</td>
<td>12%</td>
</tr>
</tbody>
</table>

Security: Largest Skills Deficit

- Information security: 25%
- IT architecture/planning: 24%
- Mobile application development: 21%
- Business intelligence/data analytics: 20%
- Server virtualization/private cloud infrastructure: 19%
- Mobile device management: 18%
- Application development: 18%
- Database administration: 17%
- Data protection (i.e., backup and recovery): 17%
- Social media/marketing technologies: 15%
- Help desk/service desk: 15%
- Network administration: 15%
- Server administration: 14%
- Compliance management, monitoring and reporting: 14%
- Social enterprise/collaboration technologies: 13%
- Storage administration: 11%
- We do not have any IT skills shortages: 12%

More Data, New Data

• **Data growth**: 1.8 trillion gigabytes in 2011 to 7.9 trillion gigabytes by 2015 (IDC)

• **Technologies Growth**: DB-Engines now tracks over 210 data stores

• **Market Growth**: Big data market forecast to reach $50bn by 2017 (Wikibon)
New Reality

• Analytics derived from “big data” becoming as valuable as traditional enterprise data

• Big data technologies must evolve to meet compliance standards of industry & government
Regulatory Compliance

• Multiple standards
  – PCI-DSS, HIPAA, NIST, STIG, EU Data Protection Directive, APEC data protection standardization

• Common requirements
  – Data access controls
  – Data protection controls
  – Data permission
  – Data audit
Requirements Define Security Architecture

Database

- Authorization
- Authentication
- Administrators
- Encryption
- Storage
- Auditing
- Clients
  (Users • Apps • Tools)
Best Practices & Enforcement in MongoDB
**Authentication**

- Confirming identity for everything accessing the database
- Create unique credentials for each entity
  - Clients, admins/devs, software systems, other cluster nodes
- Integrated with the corporate authentication standards

---

Application: application@enterprise.com

Reporting: reporting@enterprise.com

ETL: etl@enterprise.com

Joe.Blow@enterprise.com
Jane.Doe@enterprise.com
Sam.Stein@enterprise.com

shard1@enterprise.com
shard2@enterprise.com
shard3@enterprise.com
Authentication in MongoDB

• Integrate with choice of corporate authentication mechanisms
  • Kerberos protocol, with support for Active Directory
  • PKI integration with x.509 Certificates, for clients and inter-cluster nodes
  • IdM integration with LDAP support
  • Red Hat Identity Management
Authorization

- Defines what an entity can do in the database
  - Control which actions an entity can perform
  - Grant access only to the specific data needed
Authorization in MongoDB

- User-defined roles assign fine-grained privileges, applied per collection, delegate across teams

- **APPLICATION SERVER ROLE**
  - Read & Write on Application Database

- **BI ROLE**
  - Read only on Application Database

- **DBA ROLE**
  - Read & Write on Application Database
  - Administration on Application Database
  - Administration on MongoDB cluster
MongoDB Field Level Redaction

- Enables a single document to store data with multiple security levels

User 1
- Confidential
- Secret

User 2
- Top Secret
- Secret
- Confidential

User 3
- Unclassified

```json
{  _id: 'xyz',
   field1: {
     level: ['Confidential'],
     data: 123
   },
   field2: {
     level: ['Top Secret'],
     data: 456
   },
   field3: {
     level: ['Unclassified'],
     data: 789
   }
}
```
Field Level Redaction

User 1
- Confidential
- Secret

User 2
- Top Secret
- Secret
- Confidential

User 3
- Unclassified

Field Level Access Control

{  
  _id: ‘xyz’,
  field1: {
    level: [ “Confidential” ],
    data: 123
  },

  field2: {
    level: [ “Top Secret” ],
    data: 456
  },

  field3: {
    level: [ “Unclassified” ],
    data: 789
  }
}
Field Level Redaction

User 1
- Confidential
- Secret

User 2
- Top Secret
- Secret
- Confidential

User 3
- Unclassified

Field Level Access Control

```javascript
{_id: 'xyz',
  field1: {
    level: ['Confidential'],
    data: 123
  },
  field2: {
    level: ['Top Secret'],
    data: 456
  },
  field3: {
    level: ['Unclassified'],
    data: 789
  }
}
```

mongoDB
Field Level Redaction

User 1
- Confidential
- Secret

User 2
- Top Secret
- Secret
- Confidential

User 3
- Unclassified

Field Level Access Control

```json
{_id: 'xyz',
  field3: {
    level: ['Unclassified'],
    data: 789
  }
}
```
Field Level Redaction: Implementation

APPLICATION AUTHENTICATES END USERS AND LOADS PRIVILEGES

APPLICATION

TRUSTED MIDDLEWARE

COMMAND WITH REDACTION PHASE

REDACTION RULES SENT BY TRUSTED MIDDLEWARE AND ENFORCED BY MONGODB

ENTERPRISE USER DIRECTORY

MONGODB AUTHENTICATES TRUSTED MIDDLEWARE
Auditing

- Capture actions in the database
  - Access
  - Data
  - Database configuration
- Used for compliance and forensics
Auditing in MongoDB

- Capture
  - Schema operations & database configuration changes
  - Authentication & authorization activities
  - Configurable filters
  - Write log to multiple destinations in JSON or BSON
- Partner solutions for capture of read / write activity
  - IBM Guardium
Encryption

• Encoding of data in transit & at rest
  – Connections to database, and between nodes
  – Data stored on disk…protected against attacks targeting OS or physical storage
  – Mechanisms to sign & rotate keys
  – FIPS-compliant cryptography
Encryption in MongoDB

- SSL on all connections & utilities
  - FIPS 140-2 mode
  - Mix with non-SSL on the same port
- On-disk encryption via partner solutions
  - Gazzang
  - LUKS
  - IBM Guardium
  - Bitlocker & TrueCrypt
MongoDB Management Service

- **Monitor**
  - Visualize 100+ system metrics
  - Custom alerts

- **Backup**
  - Continuous incremental backups
  - Point-in-time recovery

- **Automate (tech preview)**
  - Provision in minutes
  - Hot upgrades
Environmental Control

- **Network filters**: Router ACLs and Firewall
- **Bind IP Addresses**: limits network interfaces
- **Run in VPN**
- **Dedicated OS user account**: don’t run as root
- **File system permissions**: protect data, configuration & keyfiles
Putting it all Together
## MongoDB Enterprise-Grade Security

<table>
<thead>
<tr>
<th>Business Needs</th>
<th>Security Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication</td>
<td>In Database</td>
</tr>
<tr>
<td></td>
<td>LDAP*</td>
</tr>
<tr>
<td></td>
<td>Kerberos*</td>
</tr>
<tr>
<td></td>
<td>x.509 Certificates</td>
</tr>
<tr>
<td>Authorization</td>
<td>Built-in Roles</td>
</tr>
<tr>
<td></td>
<td>User-Defined Roles</td>
</tr>
<tr>
<td></td>
<td>Field Level Redaction</td>
</tr>
<tr>
<td>Auditing</td>
<td>Admin Operations*</td>
</tr>
<tr>
<td></td>
<td>Queries (via Partner Solutions)</td>
</tr>
<tr>
<td>Encryption</td>
<td>Network: SSL (with FIPS 140-2)</td>
</tr>
<tr>
<td></td>
<td>Disk: Partner Solutions</td>
</tr>
</tbody>
</table>

*Requires a MongoDB Subscription
## Subscriptions

<table>
<thead>
<tr>
<th></th>
<th>Basic</th>
<th>Standard</th>
<th>Enterprise</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mgt. Tools</strong></td>
<td>Cloud</td>
<td>On-Prem &amp; Cloud</td>
<td>On-Prem &amp; Cloud</td>
</tr>
<tr>
<td><strong>Advanced Security</strong></td>
<td></td>
<td>SSL</td>
<td>•</td>
</tr>
<tr>
<td><strong>On-Demand Training</strong></td>
<td></td>
<td></td>
<td>•</td>
</tr>
<tr>
<td><strong>SLA</strong></td>
<td>4 hours</td>
<td>1 Hour</td>
<td>30 Minutes</td>
</tr>
<tr>
<td><strong>Support</strong></td>
<td>9am – 9pm M – F</td>
<td>24x7x365</td>
<td>24x7x365</td>
</tr>
<tr>
<td><strong>License</strong></td>
<td>AGPL</td>
<td>Commercial</td>
<td>Commercial</td>
</tr>
</tbody>
</table>
Try it Out

- MongoDB Security Architecture Whitepaper & Security Checklist
- Extensive tutorials in the documentation
- Download MongoDB Enterprise
## For More Information

<table>
<thead>
<tr>
<th>Resource</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>MongoDB Downloads</td>
<td>mongodb.com/download</td>
</tr>
<tr>
<td>Free Online Training</td>
<td>education.mongodb.com</td>
</tr>
<tr>
<td>Webinars and Events</td>
<td>mongodb.com/events</td>
</tr>
<tr>
<td>White Papers</td>
<td>mongodb.com/white-papers</td>
</tr>
<tr>
<td>Case Studies</td>
<td>mongodb.com/customers</td>
</tr>
<tr>
<td>Presentations</td>
<td>mongodb.com/presentations</td>
</tr>
<tr>
<td>Documentation</td>
<td>docs.mongodb.org</td>
</tr>
<tr>
<td>Additional Info</td>
<td><a href="mailto:info@mongodb.com">info@mongodb.com</a></td>
</tr>
</tbody>
</table>
Global Community

- 7,000,000+ MongoDB Downloads
- 150,000+ Online Education Registrants
- 30,000+ MongoDB Management Service (MMS) Users
- 25,000+ MongoDB User Group Members
- 20,000+ MongoDB Days Attendees
## MongoDB Use Cases

<table>
<thead>
<tr>
<th>Big Data</th>
<th>Product &amp; Asset Catalogs</th>
<th>Security &amp; Fraud</th>
<th>Internet of Things</th>
<th>Database-as-a-Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>BROAD INSTITUTE</td>
<td>CARFAX</td>
<td>stripe, McAfee</td>
<td>Top Global Shipping Company</td>
<td></td>
</tr>
<tr>
<td>github</td>
<td>salesforce</td>
<td>Top Investment and Retail Banks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ENERGIC</td>
<td>orange</td>
<td>Intelligence Agencies</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Top US Retailer, Telefonica</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Top Industrial Equipment Manufacturer</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Top Media Company</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Top Investment and Retail Banks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mobile Apps</td>
<td>Customer Data Management</td>
<td>Data Hub</td>
<td>Social &amp; Collaboration</td>
<td>Content Management</td>
</tr>
<tr>
<td>twitter</td>
<td>theguardian</td>
<td>MetLife, CERN</td>
<td>Cisco, Eventbrite</td>
<td>The New York Times</td>
</tr>
<tr>
<td>O₂, ADP</td>
<td>GILT, intuit</td>
<td>stripe, foursquare</td>
<td>foursquare, eHarmony</td>
<td>shutterfly, eBay</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Telefonica</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
MongoDB Products and Services

**Subscriptions**
Development & Production – On-Prem Monitoring, Advanced Security, Professional Support and Commercial License

**Consulting**
Expert Resources for All Phases of MongoDB Implementations

**MongoDB University**
Certification and Training for Developers and Administrators – Online & In-Person

**MongoDB Management Service (MMS)**
Cloud-Based Service for Monitoring, Alerts, Backup and Restore
MongoDB Company Overview

350+ employees

1,000+ customers

13 offices around the world

Over $231 million in funding
Fortune 500 & Global 500

• 27 of the Top 100 Organizations
• 10 of the Top Financial Services Institutions
• 10 of the Top Electronics Companies
• 10 of the Top Media and Entertainment Companies
• 10 of the Top Retailers
• 10 of the Top Telcos
• 8 of the Top Technology Companies
• 6 of the Top Healthcare Companies
Costs – Measured in Billions

BIGGEST DATA BREACHES OF ALL TIME:

Consumer fraud is a big problem, but the biggest security threats typically target companies.

1984 TRW  $5,400 million  90 Million
2005 CardSystems, Visa, MasterCard, and American Express  $2,400 million  40 Million
2007 TJX Companies Inc  $5,640 Million  94 Million
2009 Heartland Payment Systems  $7,800 million  130 Million
2011 Sony Corporation  $4,620 million  77 Million
2011 Sony Corporation  $1,476 million  24.6 Million