Marketfinder

Cloud Provisioned Dashboard

Processes, Policies, and Safeguards

Marketfinder, Elucidator KPI Dashboard

January 15, 2013

1. Why the Cloud? Why Elucidator?

Benefits of going to the cloud over an internally hosted solution. Why should we choose Elucidator over a different cloud based solution?

Elucidator KPI Dashboard for Web & Mobile is a web-based dashboard platform that allows users to connect to their business data, build KPIs and data visualizations that update in real-time, and share these securely with other users. It is currently being used by financial institutions such as Danske Bank, National Australian Bank; insurance firms such as Blue Cross Blue Shield and Aviva; retailers such as IKEA and Kelloggs; hospitals such as Stanford Hospitals and Clinics and William Osler Health Center; and technology companies such as IBM and Verizon.

Cloud provisioned solutions generally offer the following benefits over on-premise solutions:

- Significantly lower initial investment.
- Lower cost of maintenance.
- Data security that can be comparable or better than on-premise storage.
- Uptime and performance that is ensured by a load-balanced architecture.
- Greater feature and patch cadence.

Elucidator differs from other dashboard and BI solutions in that we are focused entirely on operational data -- frequently changing business critical metrics. Our scalable architecture, clean visualizations, and self-serve dashboard development tools are all focused around making operational metrics visible to audiences in the most efficient and simple manner.

2. Elucidator Security Protocols and Practices

What security protocols and practices Elucidator uses to protect the data in the cloud?

Our data center

Elucidator hosts our applications and your data with Rackspace, a top-tier hosting and cloud storage provider. Their security measures and features to ensure consistent service are detailed below:

All production servers for Elucidator Dashboard operate on Rackspace ‘Cloud Servers’ in the DFW1 datacenter (Dallas TX). http://www.rackspace.com/whyrackspace/expertise/

Physical security

Physical security includes keycard protocols, biometric scanning protocols, and round-the-clock interior and exterior surveillance monitor access to every one of the Rackspace data centers. Only authorized data-center personnel are granted access credentials to our data centers. No one else can enter the production area of the data center without prior clearance and an appropriate escort. Every data-center employee undergoes multiple and thorough background security checks before they're hired.

Precision environment

Every data center's heating, ventilation, and air conditioning (HVAC) system is N+1 redundant. This practice ensures that a duplicate system immediately comes online should there be an HVAC system failure. Every 90 seconds, all the air in the Rackspace data centers is circulated and filtered to remove dust and contaminants. The data centers' advanced fire-suppression systems are designed to stop a fire from spreading in the unlikely event one should occur.

Conditioned power

Should a total utility power outage ever occur, all of our data centers' power systems are designed to run uninterrupted, with every server receiving conditioned uninterruptible power supply (UPS) power. The Rackspace UPS power subsystem is N+1 redundant, with instantaneous failover if the primary UPS fails. If an extended utility power outage occurs, the routinely tested, on-site diesel generators can run indefinitely.

Core routing equipment

Only fully redundant, enterprise-class routing equipment is used in Rackspace data centers. Fiber carriers enter our data centers at disparate points to guard against service failure.

Network technicians

Rackspace requires that the networking and security teams working in their data centers be certified. They also require that they be thoroughly experienced in managing and monitoring enterprise-level networks. Certified Network Technicians are trained to the highest industry standards.

Our application

Logical components

Elucidator KPI Dashboard for Web & Mobile can be broken down into the following logical parts:

- Load balancer: software load balancer which distributes traffic to multiple WebUI nodes.
- WebUI: a traditional web-application that provides a user interface for users to interact with the product
- Data-Refresh-Nodes: are responsible for connecting to user data sources and refreshing them at specified intervals.

- Data-Provider-Nodes: are responsible for executing formulas against user data. Once users have authenticated to their dashboards their browsers establish connections to DPNs to get real-time updates.

Technologies used

- Nginx (load balancer)
- Jetty (webui application server)
- Java
- MySQL (domain DB)
- MongoDB (grid file system for user data sources)
- Redis (caching layer; job queue; pub-sub)
- Ubuntu

Elucidator allows users to connect to data using a connector architecture; users may establish connections to their data using an appropriate connector (REST, SQL, FTP/SFTP, etc).

Connectors pull user data into our database where it can then be referenced to create visualizations via formulas. Users may also specify a refresh interval at which we will automatically reconnect to the data and pull it into our system. User data is stored in a separate database from application (domain) data.

Traffic management

We use software load balancing – specifically Nginx – to achieve horizontal scalability on our front-end. Nginx is configured to distribute users to nodes based on their IP address. If the server that a user is assigned to goes down they will be seamlessly be routed to another server.

Client registration process

Users may sign their company up for a trial, which can then be upgraded to a full account. Once a company is signed up the primary user who initiated the registration process may add new user accounts to the company.

Sign-in functionality

All access to Elucidator dashboard is via HTTPS. Users enter credentials into the webui where they are authenticated against the database. User credentials are stored in the database in a salted-MD5 format.

After authenticating, the user will be given a session that will last approximately 30 minutes without activity. However, when their browser is displaying their dashboard their session will be kept alive.

Client end-user access controls

Unique identifiers that are exposed in the UI are not guessable and cannot be used to URL-spoof access to different resources.

Within the application, users & resources (data sources, KPIs, and tabs) can be assigned to groups with different levels of access (read, write, etc), allowing company administrators to have full control over what their users can see and use.

Access to all resources goes through user-group access checks making cross-account data access impossible.

User ids & passwords are stored in the domain database. Passwords are salted (using their user-id and random characters) and hashed using MD5. Users can initiate a password reset from within the application, which will email the user a token (that expires after 4 hours) they can use to reset their password. Users can also ask a CSR to reset their password.

The user ID and password are both set by the user. The password is never shared outside of the application. The minimum password length is 4 characters and with no character requirements. This however can be configured on an account-wide basis to require passwords of any length, and require a mix of alpha, numeric, and special characters. Passwords do not currently expire. One-time passwords are not used.

Multiple login attempts can be locked out. The options are after 3, 5, or 10 attempts, and the lockout period can be configured from 15 mins, 30 mins, 1 hour, 24 hours, or until reset by the admin. Login attempts are logged, and admins are alerted to which users are locked out if any.

Session management controls

Sessions are terminated after 30 minutes of inactivity (not currently customizable). During this time a user may implicitly end their session by logging out. Session IDs are stored in a database table to allow seamless failover. No passwords are stored in sessions.

All user access to the service is via SSL. Administrators access the infrastructure via SSH.

Access logs

An in-application event log can be viewed by admins. Event log information may also be used by Elucidator to infer anonymous usage statistics. Logs are archived for 3 months. The application maintains an event log which can be viewed by admins at any time. Event log information includes information related to: authentication, failed login attempts, asset creation, deletion, and modification. Event log information is stored in a database and is purged after three months. No sensitive information is stored in the log.

Elucidator policies and procedures

Elucidator access to client data

Elucidator CSRs have no ability to mimic user login on production environments and can only login with user credentials if they supplied by the user or a special account has been created for our CRSs by a customer. Once logged in their actions are tracked in the even log in the same way as normal users.

Vulnerability testing

New features undergo a security assessment to determine if they will introduce new vectors of attack. Features are then hardened to prevent possible exploits. Code reviews are used to identify potential issues. User input is validated to conform to the expected input ranges. Access is via keys that can be revoked.

Websecurify is used to test for cross-site scripting, generic attack patterns and vulnerabilities, path/email/error disclosure. Reviews are done about once every month on our test and production servers.

Internal Security procedures and policies
Elucidator communicates with our employees and contractors about our obligation to safeguard confidential information, including customer data and personal information, in monthly meetings.

The following policies and procedure are enforced: Access to any information systems must be attributable to a uniquely identifiable individuals; default passwords must be used in any systems; passwords must comply with the Elucidator password usage policy; customer data must only be printed or stored if there is a clear need to do so; users with a defined need to access customer data shall be granted access and will be revoked as soon as access is no longer required.

Physical security policies include general access controls for all employees, as well as limited IT room access. Cameras and proximity cards are used to monitor activity.

Human resources security protocol includes the requirement for all employees and contractors to sign NDAs, submit to regular security briefings and also governs the procedures for employee termination. New employees are subject to reference checks and a three-month probation where access to customers or sensitive data is limited. Upon termination, employee is escorted until they have left the building, and if they return to pick up personal belongings. Keys, access cards, and any storage media are collected. Email, VPN, and external access to any other systems are immediately moved. All employees and contractors sign a confidentiality agreement. Our policies and procedures document, made available to all employees has a section on confidentiality and security best practices

All workstations and computers have up to date antivirus software installed and activated. Ad-hoc security scans and penetration tests are performed on test and production systems. Workstations are password protected. Screen savers are enabled after several minutes of inactivity. Antivirus software is installed and active. Employees that work from home may have access to the corporate VPN with the same level of restrictions that apply in-office.

3. Backups and Disaster Recovery

Backups and Disaster Recovery scenarios, to prevent data loss in the case of server failure.

Production application data is backed up on daily basis, as well as in a slave database for rapid recovery. Master/slave replication additionally ensures that database backups are hot-swappable. Backups and replications are not transported off site.

Internal Elucidator data backup is being handled locally by RAID arrays, encrypted for sensitive data, and then incrementally hosted off-site with AWS – encrypted. Data stored using this process is separate from data used within the dashboard application hosted with Rackspace.

4. Uptime and Service Level

Is there a guarantee for uptime for our dashboard to be running? If so, what is the guarantee for uptime?

The Elucidator application architecture has been designed to be scalable and redundant, allowing for fluctuation in demand and expansion of users while greatly reducing the threat of extended down-time. Features of our design include load-balanced networks, pools of application servers, and clustered databases.

Elucidator can commit to service availability of 99.9% (including scheduled maintenance interruptions); call-in answer time of less than 1 minute, 90% of the time (between business hours 9am to 5pm ET); and an average ticket response time of 1 business day.

For the past 30 days, as of the time of the writing of this proposal, uptime is at 99.96%, including scheduled maintenance.

Depending on the scope of the issue, most vulnerabilities can be hot-fixed into the production environment within hours of announcement.

Production servers are monitored with several different technologies: uptime and availability is monitored with Pingdom. Service health and recovery is monitored with Monit. Websecurify for security scanning and penetration testing.

--- End ---