RSA CHARGE
2017

ADVANCED ANALYTICS ON RSA ARCHER SUITE

Rajesh Subramanian
Microsoft EGRC Program Manager
Microsoft

#RSACharge

AGENDA

How Azure can tell you more about Archer and your user behavior

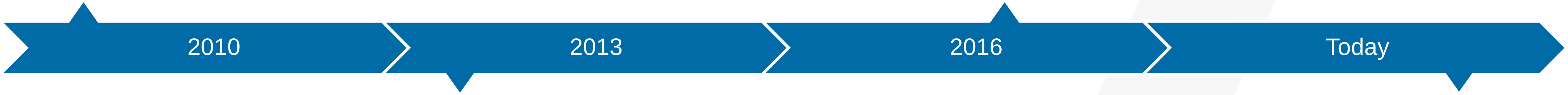
- ► Introduction to Microsoft’s EGRC Archer Platform
- ► Our Problem Statement
- ► Our Solution
- ► What We Learned

INTRODUCTION TO MICROSOFT’S EGRC ARCHER PLATFORM

MICROSOFT'S EGRC ARCHER PLATFORM

EGRC is Microsoft's Archer enterprise governance, risk, and compliance tool that provides a centralized information repository for the reporting of security, compliance, and enterprise risks.

EGRC Timeline



Developed the GRC tool strategy and rolled-out EGRC at Microsoft

Enhanced our change management and governance program

Enabled user tracking to gather actionable insights

We're focused on optimizing the EGRC platform to achieve even greater efficiencies

Platform Size

- **8** core solutions:
  - Policy Management
  - Compliance Management
  - Issue Management
  - Policy Exception Management
  - Business Continuity Management
  - Risk Management
  - Incident Management
  - Enterprise Management
- By the numbers:
  - **50+** Workspaces
  - **20+** ODAs
  - **40+** Questionnaires
  - **20+** Active data-feeds

Platform Usage

- **30+** business groups across the company run their services in the tool
- We average approximately **5000 unique users** every month from over 15 countries
- **1500+** unique notifications are sent each month

Azure Migration Overview

- Identified best-in Azure architecture that will meet the platform's growing needs
- Successfully transitioned environment to Azure in FY16
- Continuously optimizing cloud usage through weekly tracking activities

Microsoft

RSA CH>RGE 2017

OUR PROBLEM STATEMENT

EGRC'S USER FEEDBACK

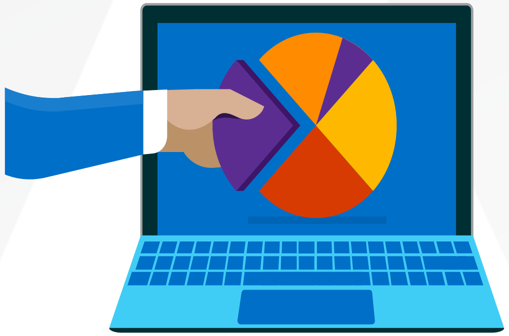
1. Navigational & Performance Concerns

Significant customization and configurations were negatively impacting the performance and users were getting confused with the platform's user interface

2. Lack of Alerting

Lack of standardized monitoring to correct failures on the server (SQL and custom jobs), thereby causing after-hour outages

3. Limited Reporting Capabilities



Due to Archer's limited reporting capabilities, EGRC users as well as the engineering team were unable to leverage the data to make insightful business decisions

Led to

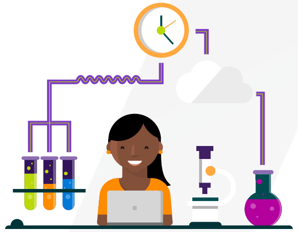
Inability to identify high-impact areas for improvement + Reactive approach to system outages + Limited data insights

CHALLENGES WITH ARCHER

ARCHER CHALLENGES

1. Inability to track unique user count, activity by geography, usage by workspaces and application
2. Lack of monitoring at the server-level to alert the team on system failures
3. Inability to present “live” data visualizations to senior leadership

OUR SOLUTIONS



1. Microsoft Azure’s Application Insights
2. Microsoft’s Operations Management Suite (OMS)
3. Microsoft’s Power BI

As our platform scaled, our ability to track and address performance and user experience issues were limited with the native Archer capabilities but moving to Azure provided us with the solutions we needed.

OUR SOLUTIONS

MICROSOFT AZURE’S APPLICATION INSIGHTS

GOAL: OPTIMIZE WORKSPACES AND APPLICATIONS PER USAGE PATTERN

What?

- Sends telemetry from Archer to the Application Insights portal on Azure
- Helps detect and diagnose performance issues, and understand how users navigate within Archer

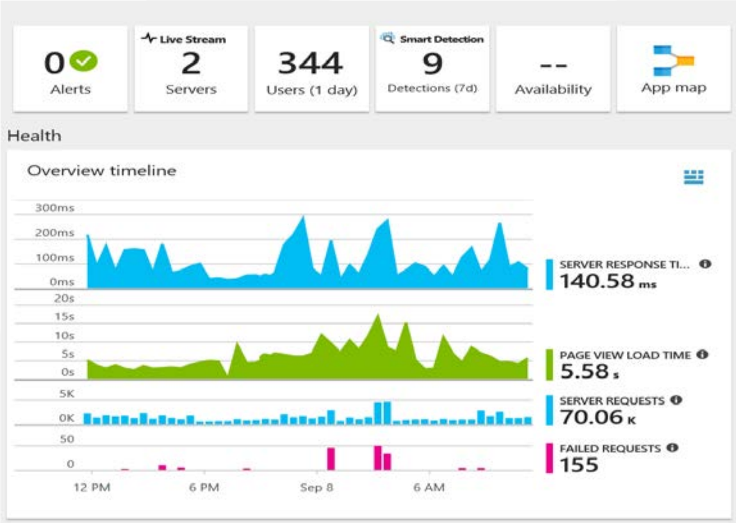
How?

- Added Azure SDK script into workspace.aspx page on the web-server to retrieve the workspace name
- Added Application Insights instrumentation code as a custom object to modules

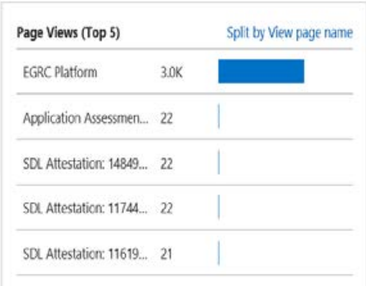
Value Added

- 360 degree view of EGRC and complete visibility into the heavily-used areas including applications and questionnaires
- Transitioned from *logging* telemetry to *analyzing* and *acting* on telemetry

Overall Platform Usage



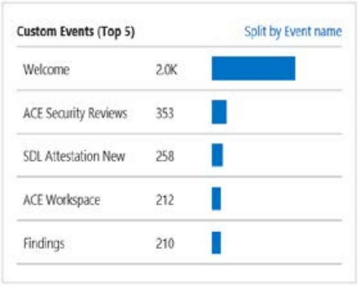
Top 5 Page Views



Page Views (Top 5) — Split by View page name

EGRC Platform	3.0K
Application Assessmen...	22
SDL Attestation: 14849...	22
SDL Attestation: 11744...	22
SDL Attestation: 11619...	21

Top 5 Applications



Custom Events (Top 5) — Split by Event name

Welcome	2.0K
ACE Security Reviews	353
SDL Attestation New	258
ACE Workspace	212
Findings	210

Microsoft

RSA CH>RGE 2017

MICROSOFT'S OPERATIONS MANAGEMENT SUITE (OMS)

GOAL: DETECT AND RESPOND TO SERVER ISSUES

What?

- Core services to address different operational scenarios:
  - Powerful Log analytics
  - Automation
  - Backup & Site Recovery

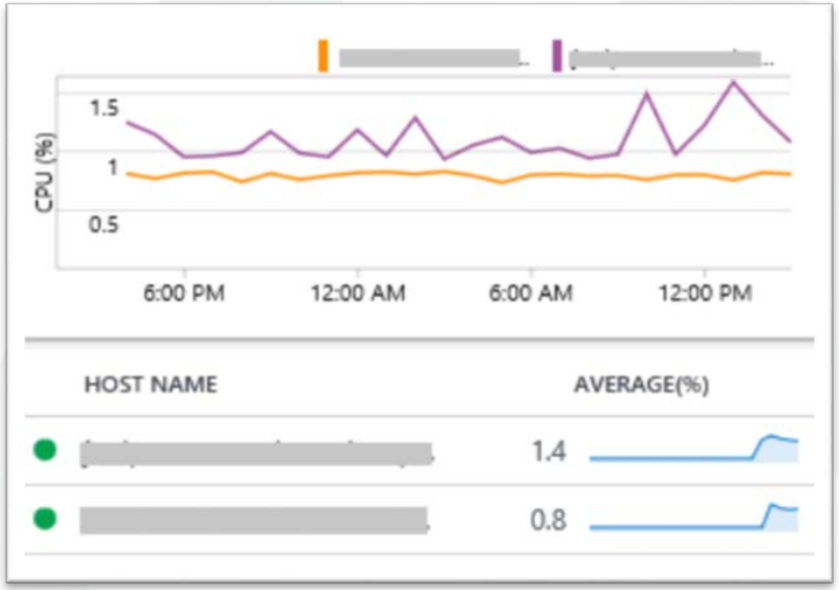
How?

- Installed Microsoft Monitoring Agent (MMA) on our Azure Virtual Machine (VM) and connected them to the OMS solution
- Added different data sources including IIS logs, Windows Event logs for tracking

Value Added

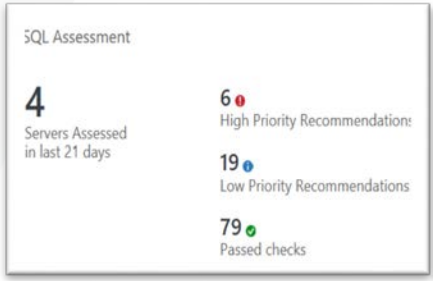
- Insights into our systems health, performance and availability, thereby alerting us on issues that we can actively prevent
- Improved security posture through the continuous monitoring and assessment of our servers

CPU Utilization



HOST NAME	AVERAGE(%)
● [redacted]	1.4
● [redacted]	0.8

SQL Recommendations


SQL Assessment

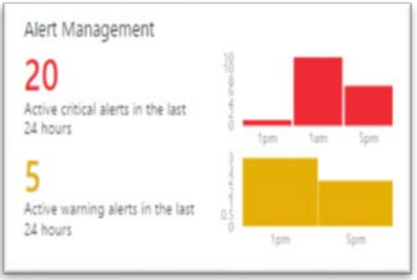
4 Servers Assessed in last 21 days

6 ● High Priority Recommendations

19 ● Low Priority Recommendations

79 ● Passed checks

Alert Management


Alert Management

20 Active critical alerts in the last 24 hours

5 Active warning alerts in the last 24 hours

Microsoft

RSA CH>RGE 2017

MICROSOFT'S POWER BI

GOAL: ENHANCE THE WAY WE VIEW COLLECT AND VIEW DATA

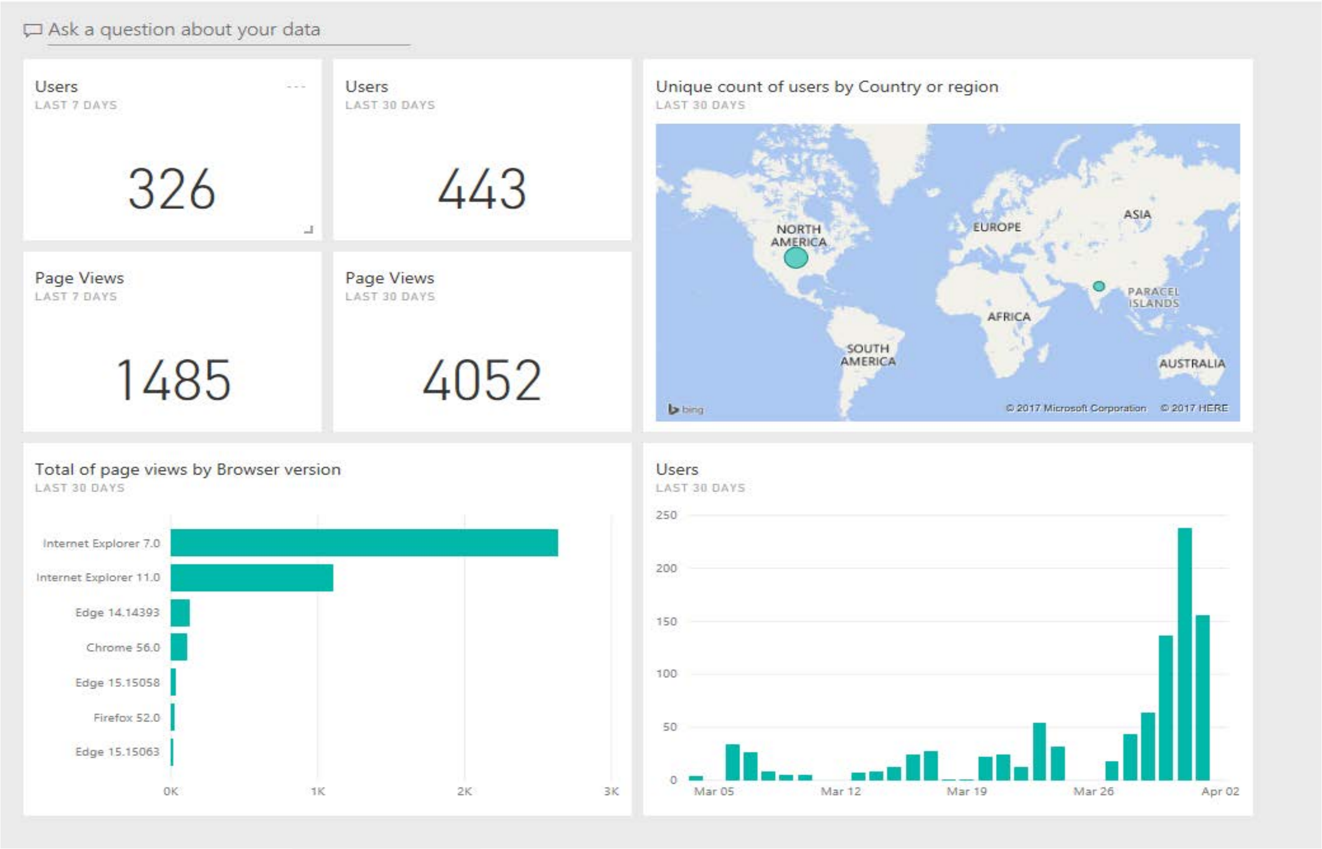
What?

- Business analytics tool that can connect to varied data sources to gather and deliver insights to your organization
- Enables different users based on their role and usage style

Value Added

- Better understanding of critical risk and failure through a single, consolidated view
- Data available *on-the-go* through Power BI's mobile view, alerts on sudden spikes in the data

Consolidated View of AppInsights, OMS & Archer



Ask a question about your data

Users
LAST 7 DAYS
326

Users
LAST 30 DAYS
443

Page Views
LAST 7 DAYS
1485

Page Views
LAST 30 DAYS
4052

Unique count of users by Country or region
LAST 30 DAYS

Total of page views by Browser version
LAST 30 DAYS

Users
LAST 30 DAYS

WHAT WE LEARNED

WHAT WE LEARNED

IT'S POSSIBLE

It is possible to learn about your platform's usage per application and solution

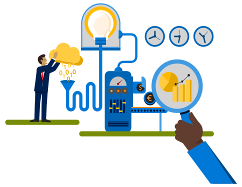
EASY TO DO

Plug-ins like Azure's Application Insight and OMS's make the implementation fast and easy

EFFECTIVE

The data we captured is highly influential in making key business descisions

BUILD KPIS



Benchmark your improvements with KPIs to ensure that your actions enables customers

THANK YOU