IBM Security

Guardium GBDI:
Guardium Big Data Intelligence for Data Security Insights and Integration

Chris Brown
jSonar

Dale Brocklehurst
IBM

IBM

Agenda

- Q & A
- Overview of GBDI
  - Infrastructure & Architectural Benefits
- Powerful Data Integrations
  - Splunk, Cyberark, ServiceNow, anything via NoSQL
- Q & A
- GBDI Demo
- Hands On Lab
- More Q & A

IBM Security Guardium + IBM Security Guardium Big Data Intelligence

IBM Security Guardium

- Discover and classify sensitive data
- Discover data source vulnerabilities and track remediate progress over time
- Data and file activity monitoring
- Dynamic data protection with advanced analytics, supporting real-time alerting, blocking, quarantining
- Data encryption and key management

IBM Security Guardium Big Data Intelligence

- Gather, manage and store huge data volumes while keeping operational costs low
- Store data over longer timeframes to support compliance requirements
- Deliver data security, compliance, and operational reporting in near-real time
- Perform big data analytics on historical, context-aware, and enriched data
- Provide easy assess to insights for authorized users, from across the business

Enrich IBM Security Guardium with the power of a big data platform that's purpose-built to optimize Guardium for cost and functionality

How GBDI Increases of Value of any DB Security Program

USE THE DATA

Process Optimization

- Data Enrichment for Context
- Self-Service Reporting
- FTE efficiency via Automation

Leverage Analytics

- Pre-built solutions for DAM
- SIEM volumes ↓ >95% via Noise Reduction, De-dup
- UBA for Anomaly Detection

Improve Data Accessibility

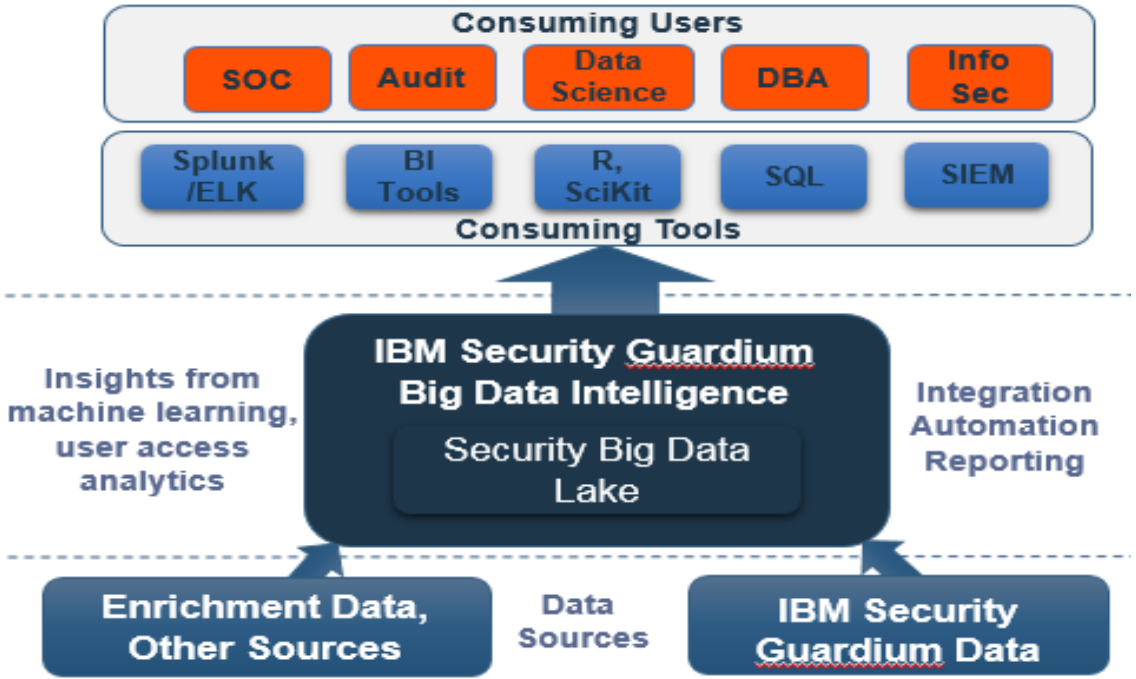
- Retention 30 days → 3 years+
- Reporting Performance ↑ >100X
- Self-Service Access

Streamline Data Collection

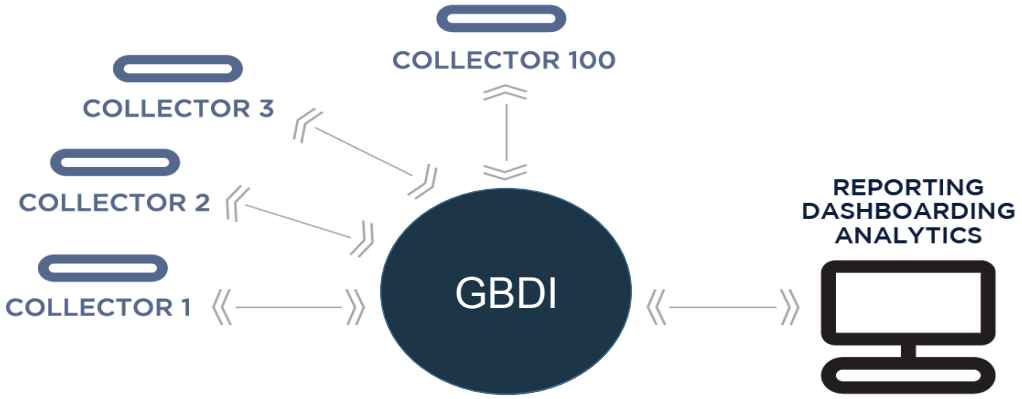
- Migrate Aggregator Tier to Big Data
- HW costs ↓ >25%
- Storage efficiency ↑ >30X

COLLECT THE DATA

What is Guardium Big Data Intelligence (GBDI)?



Simplified Enterprise Architecture



- Replace Aggregation with the SonarG central repository
  - Most of the benefits come from what you can do with the data
- Key efficiency and cost gains for Guardium infrastructure
  - Eliminate entire aggregation tier including HW, processes and latency
  - Large reduction in Collector storage needs (600GB → 100GB)
  - 10-20 % increase in Collector throughput tied to workload shift, MySQL boost, visibility
- Single low-cost warehouse node can support >200 collectors
  - >1 year active data using less storage than existing footprint
  - Fast, ad hoc access to 10's of TB's of data, eliminate restores

A Transparent Overlay to Existing Guardium Footprint

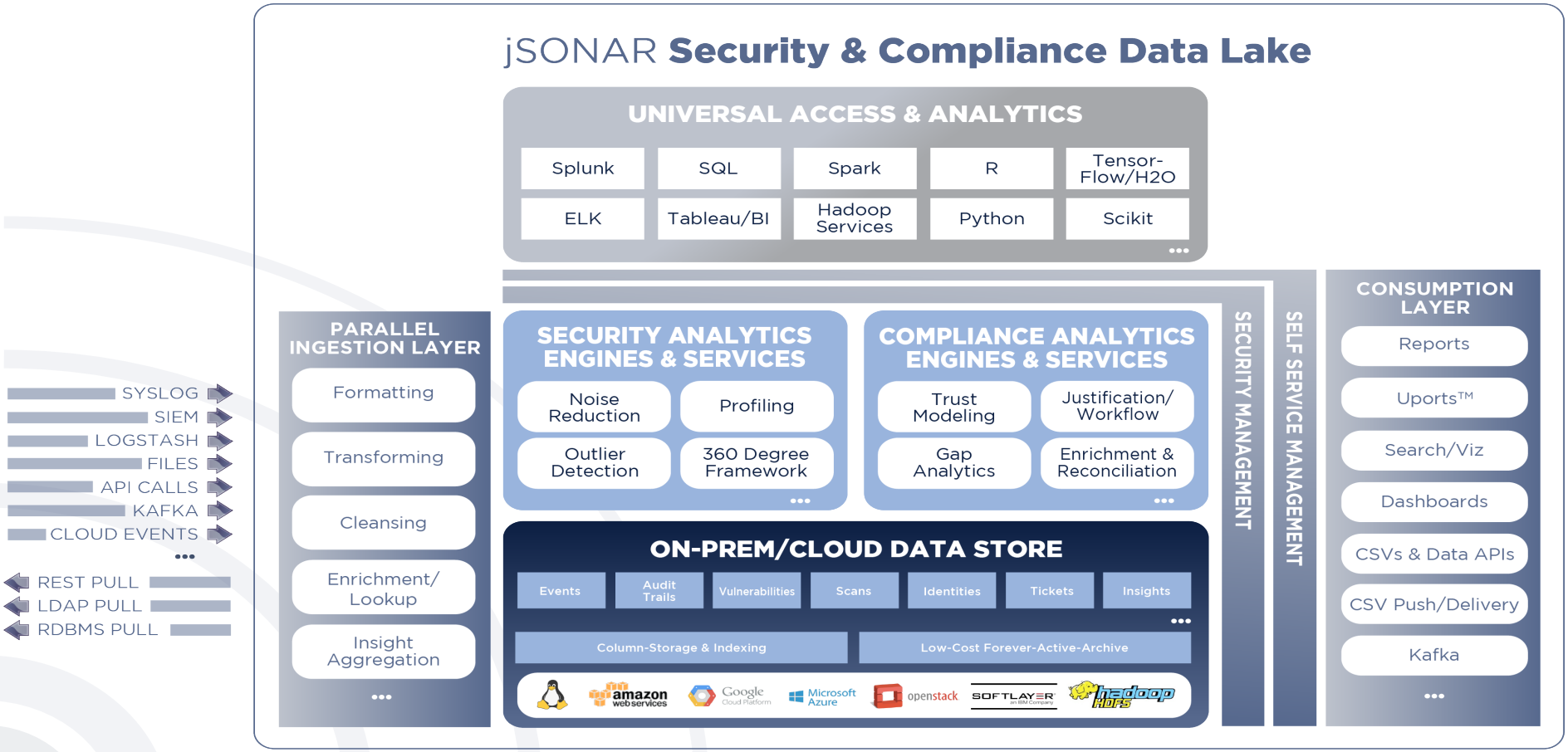
- No Disruptive Transitions – highly controlled and easily managed
- 3 Primary integration points to enable GBDI – all low risk & proven:

1) Collector Datamart extractions to move raw data to GBDI
   - Automated grdAPI scripts to enable appliances to publish extract files
     - Simple SCP file pushes from Guardium appliances to GBDI
     - Easily validated in a tech session, without having GBDI installed

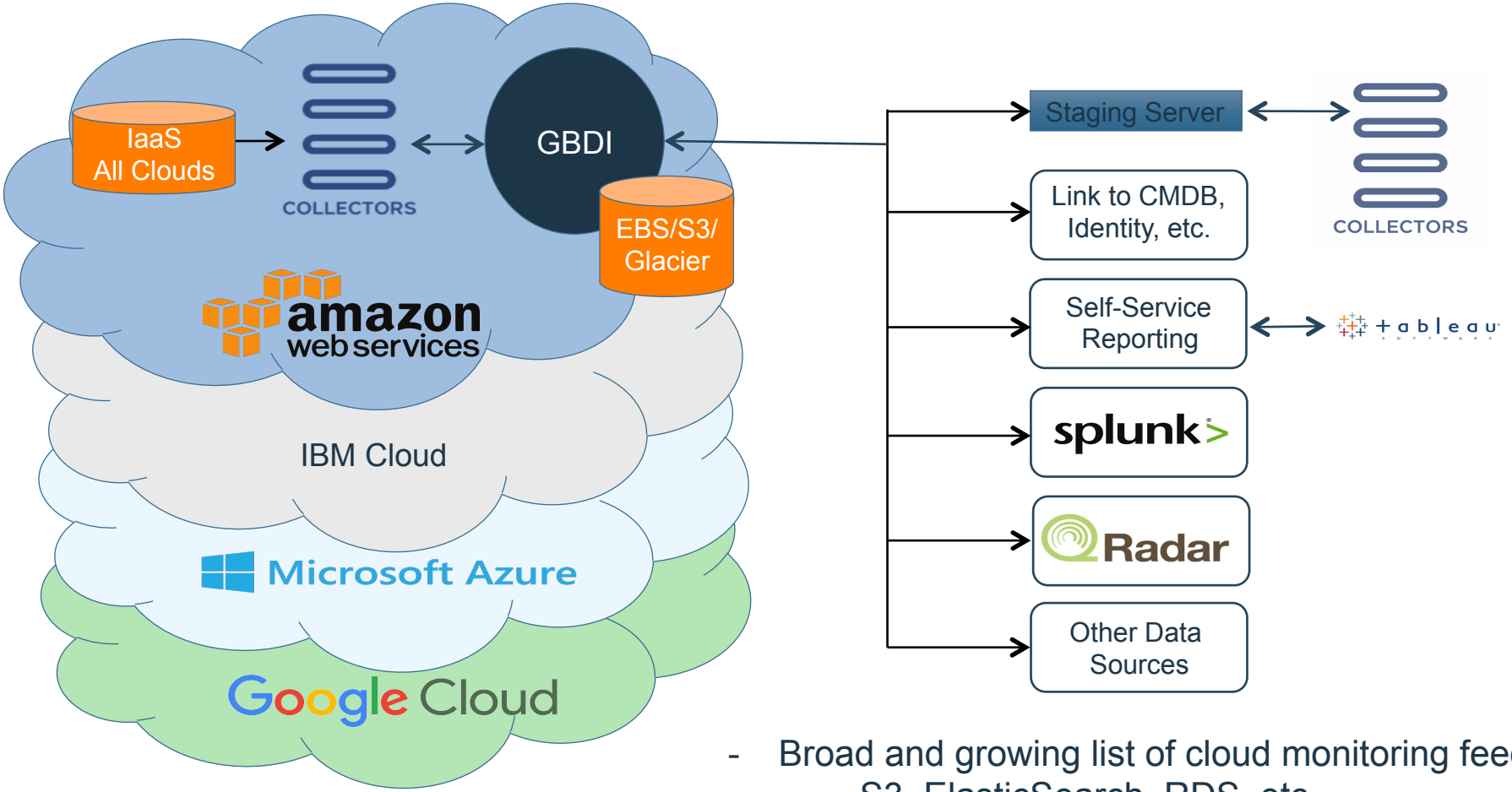
2) Mapping of Existing Guardium Reports
   - Easily replicate current Guardium reports within GBDI
     - Converted several during POC to demonstrate ease of migration

3) Publishing results to existing flows
   - Multiple publishing options

Out of the Box Security Data Lake



GBDI in the Cloud – A perfect fit



- Broad and growing list of cloud monitoring feeds
  - S3, ElasticSearch, RDS, etc.

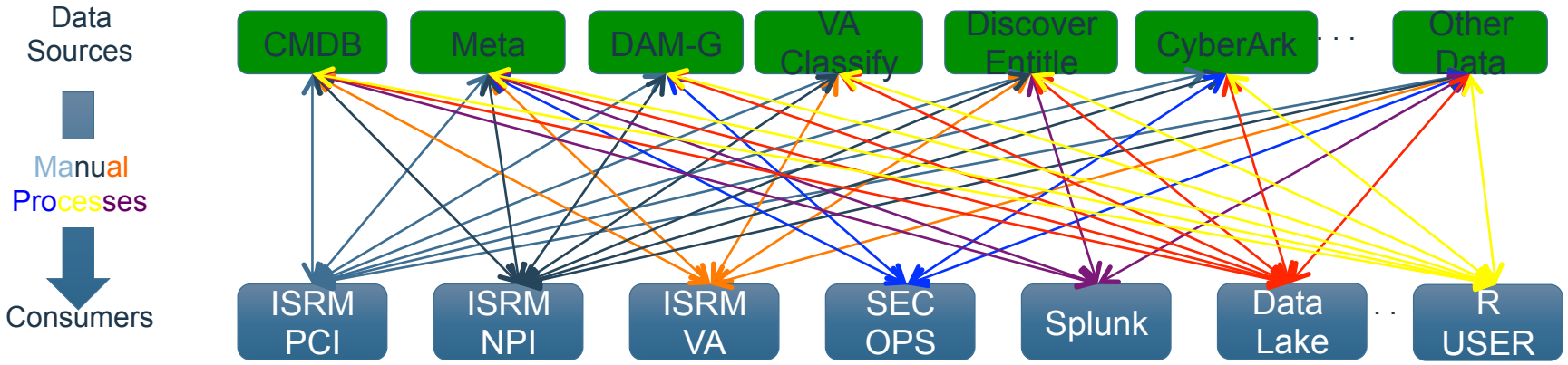
Core GBDI Benefits at the Infrastructure layer

- Dramatically simplify data collection process
  - Less pressure and focus on policy optimization – “collect all !”
  - Substantially reduce operational overhead – enable growth
  - Complete V9→V10 Upgrades in days
- Cost effectively retain years of data
  - NY DFS is strong driver for 3 year retention
- Self-Service and flexible access are key for new use cases
- Take it for granted that any data needed can be collected and accessed at any time
- Empower Guardium customers to move to Guardium2.0

Powerful and Valuable Data Integrations

- All Guardium programs need link to critical external data assets for enrichment
  - Drives consumption and context
- Splunk, Cyberark and ServiceNow are especially in demand
  - Privileged Account Activity Reconciliation is a new compliance “target”
- Ripe Opportunity for high value process optimization
- Excellent opportunity to elevate the discussion with clients
  - “Let’s explore your processes after data is collected..”

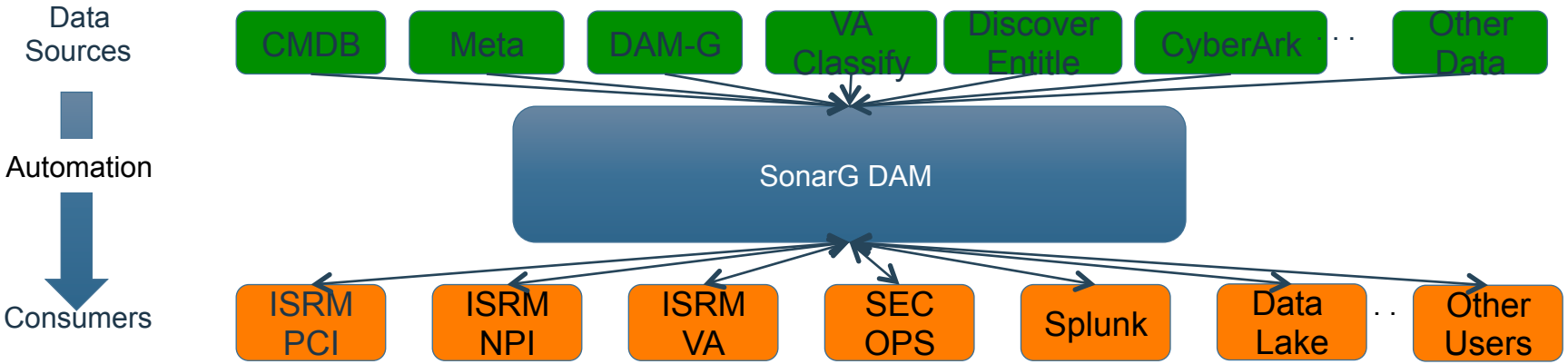
Typical Customer DB Security Landscape



Many current and looming challenges

- Large collection of manually intensive processes inhibit value
- Struggling to support all “customer” requests, more coming
- Critical need for secure, controlled Self-Service
- No consolidated, enterprise views of all DAM data from multiple tools
- Inflexible data ingestion & access limits context of DAM data
- High information latency limits inspection frequency & effectiveness
- Tool inflexibility limits integration and automation options – “closed” system

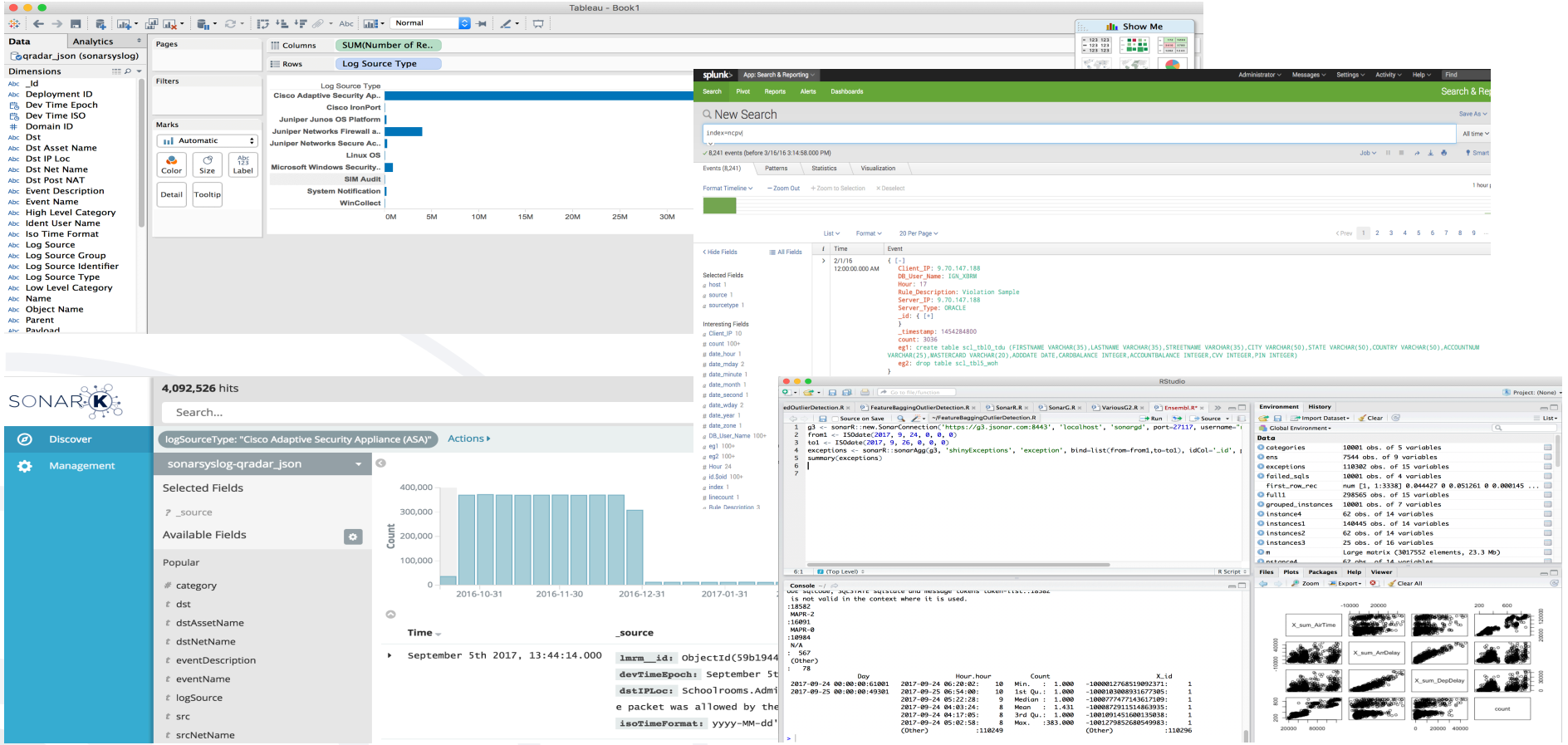
SonarG-Enabled Approach



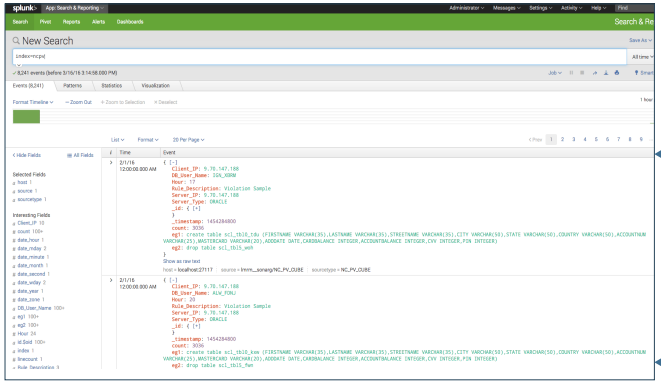
Embracing Flexibility, Orchestration and Automation

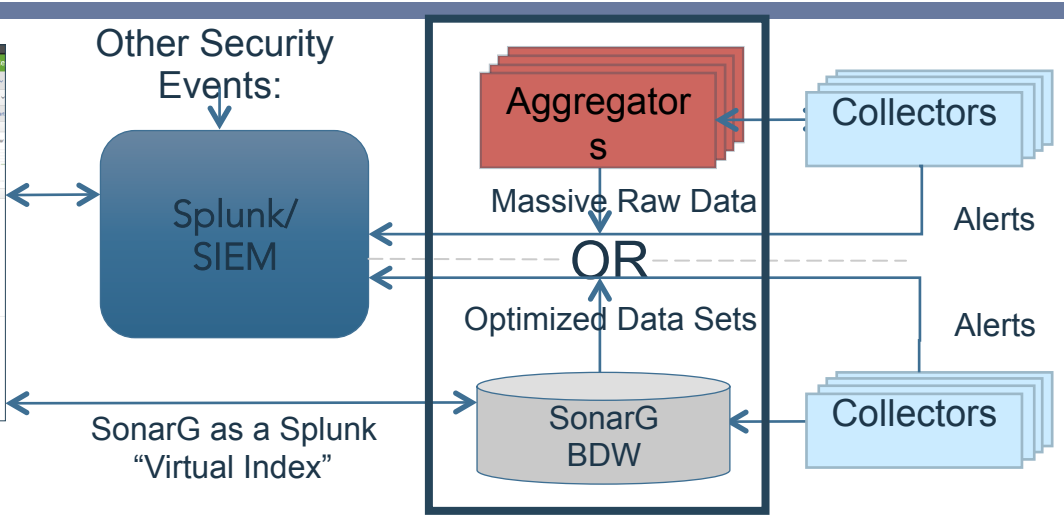
- Highly flexible data ingestion, reconciliation and access
- Heavy automation for both input & output
- Excellent complement to enterprise Splunk strategy
- Architected for Self-Service reporting and dashboards
- Data-Level Security for fine-grained access control
- Rich context via powerful NoSQL and Join options
- Wide variety of output options – csv, pdf, BI tools, Excel, etc.
- Automation drives improved quality, services and agility

Rich 3rd Party Tool Support for Self-Service



SonarG Optimizes Splunk for DAM





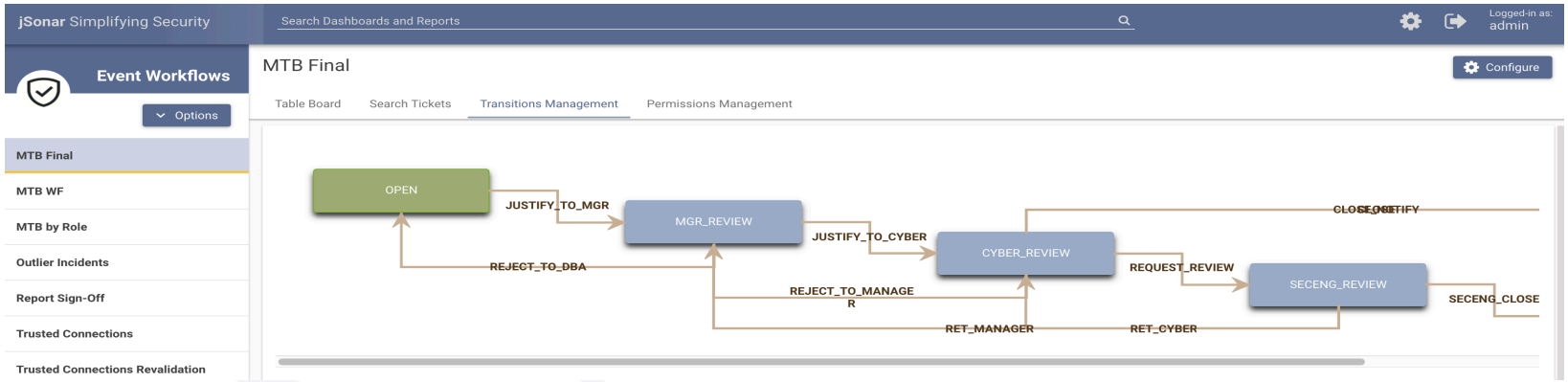
- SonarG does not compete with Splunk – We are a Powerful Compliment
  - SonarG + Splunk delivers best of breed architectural solution relative to data quality, flexibility, cost reduction, stability, ease of use and value of Guardium DAM output
- Reduce Splunk license costs by reducing volume of Indexed Data
- Splunk remains primary logging facility with SonarG in place
  - Provides both an efficient data flow to Splunk as well as direct access via Splunk UI

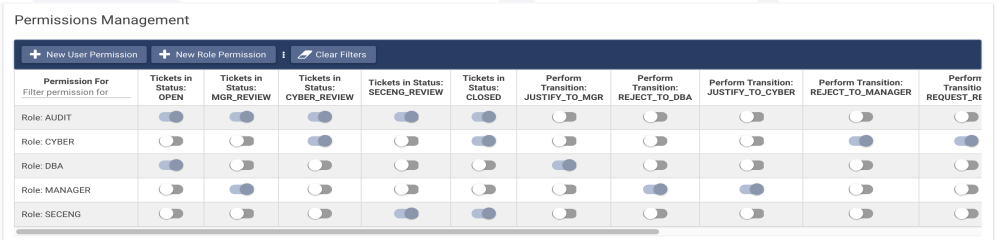
SonarG vs. Splunk

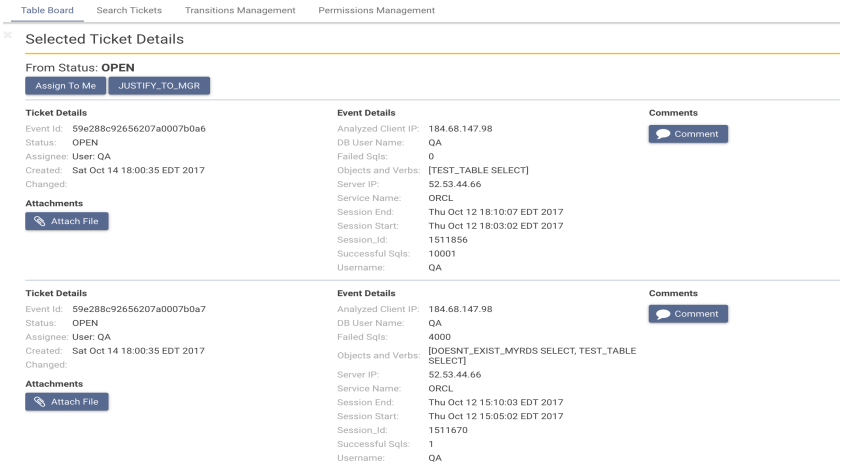
Consideration	Splunk	SonarG
Improve Guardium STAP, System Stability, Performance,	N	Y
Reduce Guardium HW Footprint	0%	>25%
Loss of Data Quality, Context and Security	Y	N
Splunk License Cost Impact	↑↑	↓
Fully compatible with existing Compliance reporting without large investment	N	Y
Integrated DB Security Analytics – Trusted Connections, User Behavior, Profiling, Outliers, etc.	N	Y
Easily automate current Guardium processes	N	Y
Enable Self-Service Access for customers	N	Y
Easily implemented fine-grained access control	N	Y
Cost Effective repository for months/years	N	Y
Purpose-built integration with IBM Guardium	N	Y
Fully Compatible with Splunk UI	**Y**	**Y**

SonarG Optimizes both Guardium and Splunk usage on DAM Data

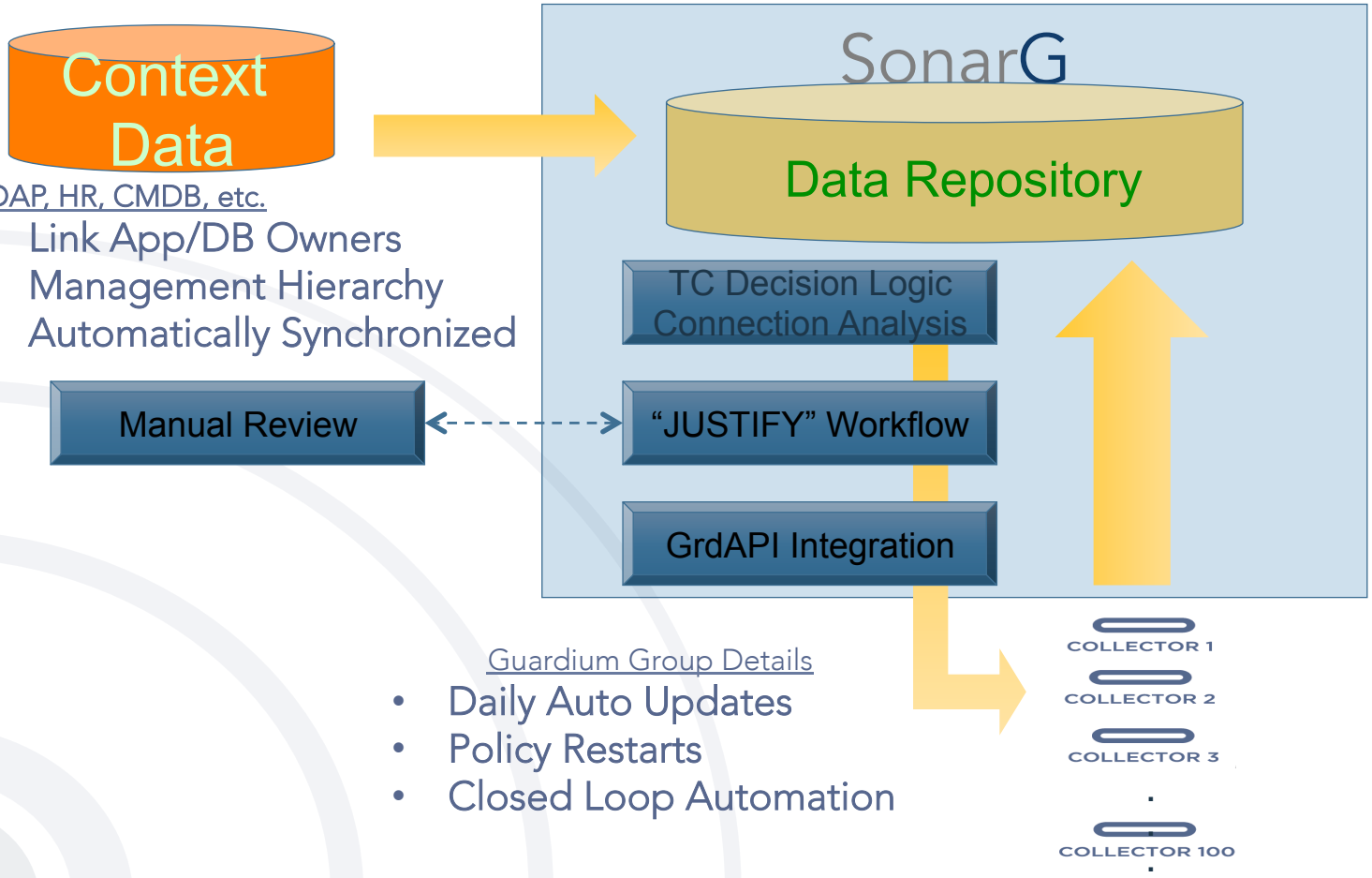
Justification / Workflow Engine



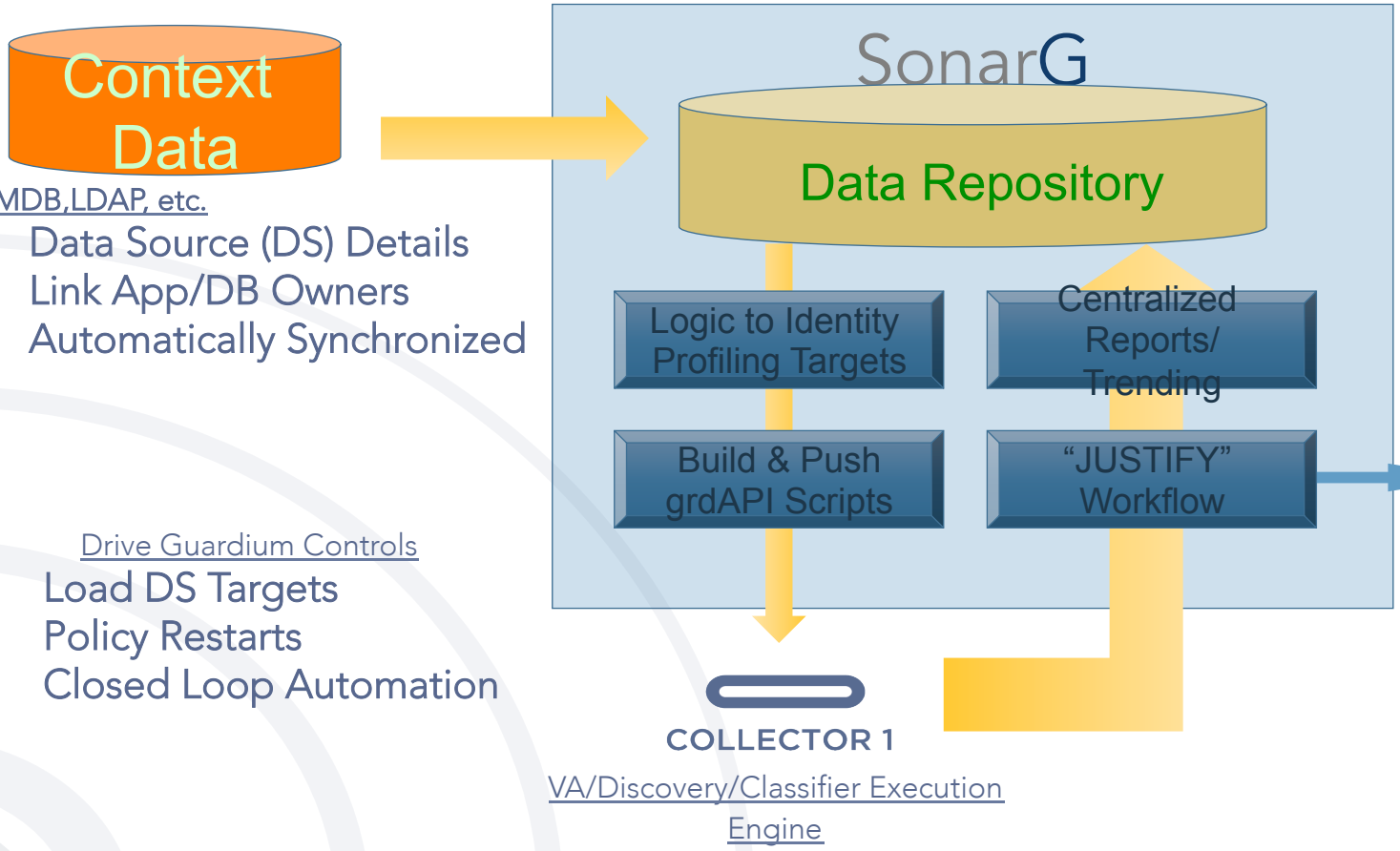




Automating Trusted Connection Profiling



Enterprise VA/Discovery/Classifier Management



CMDB,LDAP, etc.

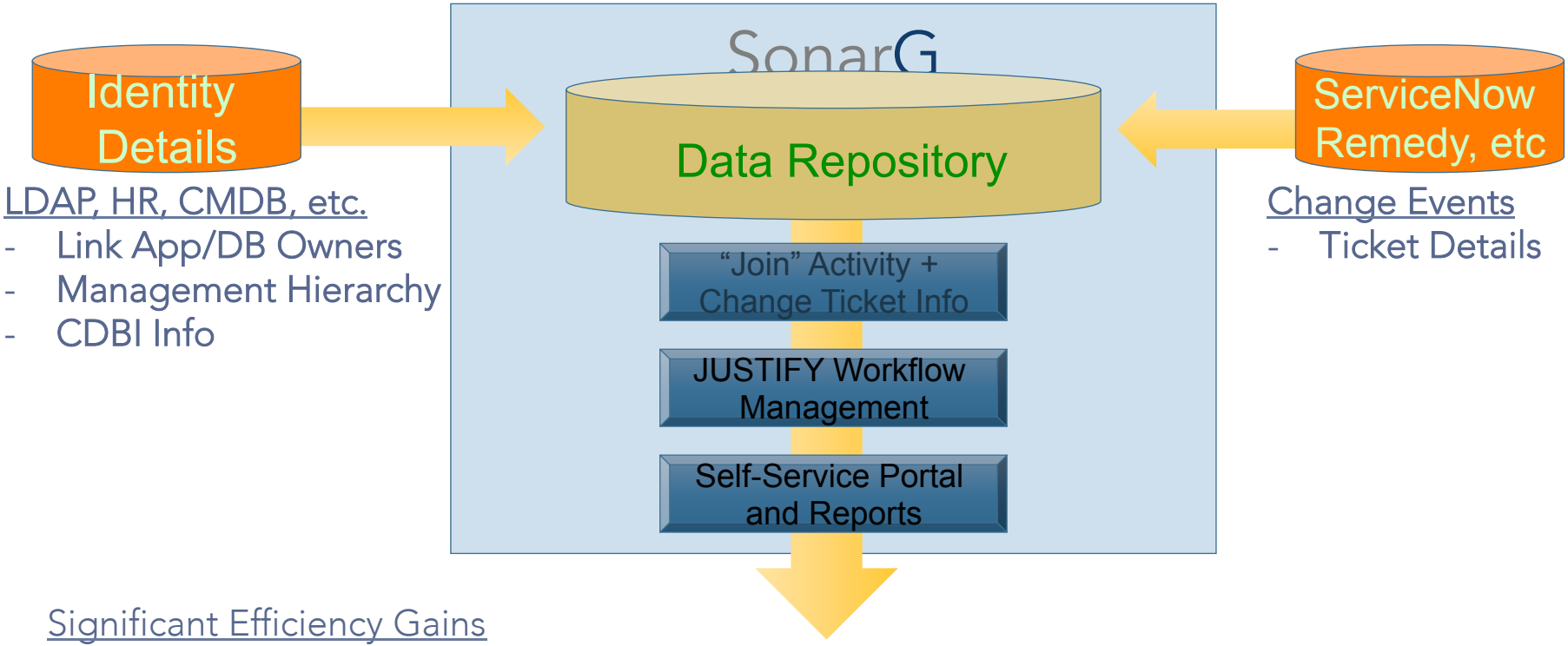
- Data Source (DS) Details
- Link App/DB Owners
- Automatically Synchronized

Drive Guardium Controls

- Load DS Targets
- Policy Restarts
- Closed Loop Automation

VA/Discovery/Classifier Execution Engine

Automating Change Reconciliation



Significant Efficiency Gains

- Automating cumbersome manual processes
- Impacts many organizational teams
- High value for audit/compliance

Demo time

IBM Security

THANK YOU

FOLLOW US ON:

- ibm.com/security
- securityintelligence.com
- xforce.ibmcloud.com
- @ibmsecurity
- youtube/user/ibmsecuritysolutions

IBM