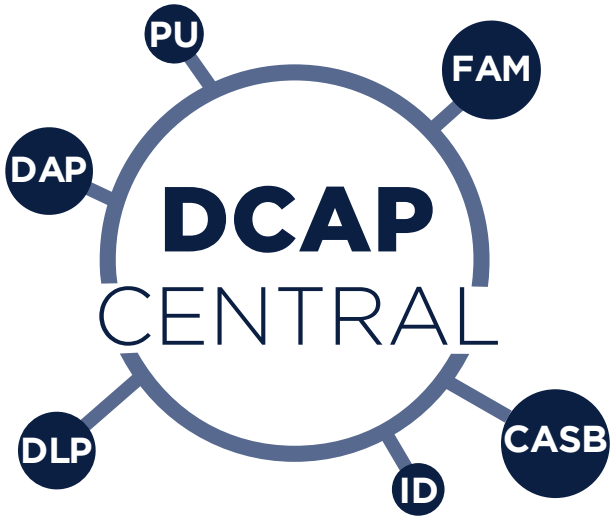
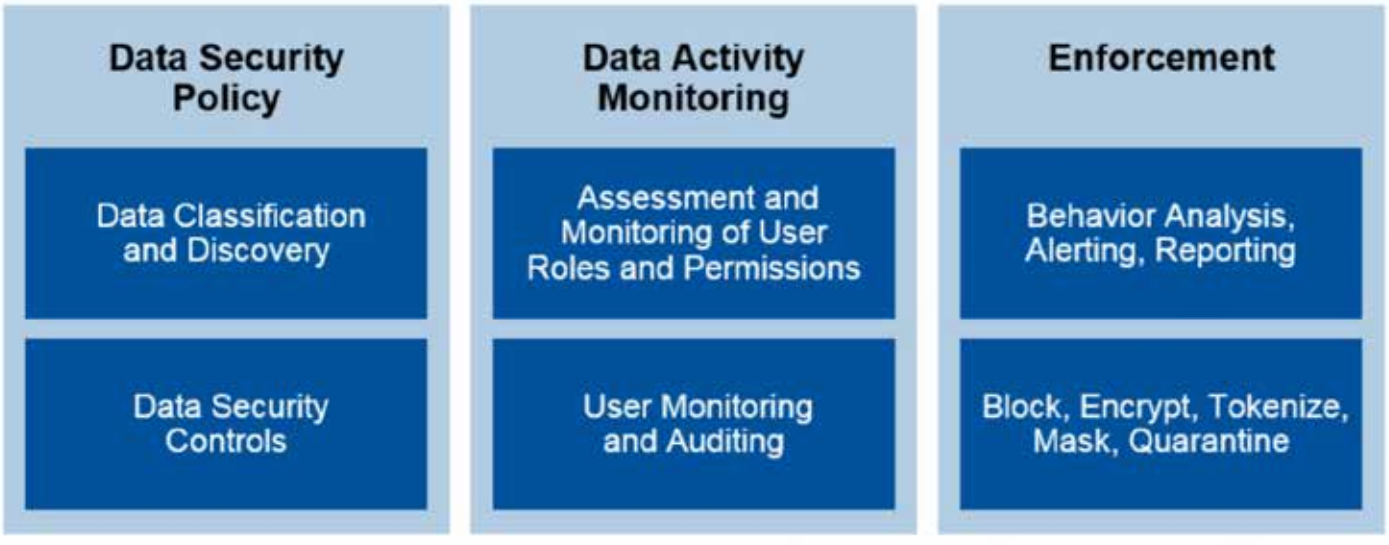


We are constantly reminded that traditional security models are no longer valid, as perimeters dissolve; new platforms are introduced and new technologies such as Big Data and Cloud become commonplace in the enterprise. Of course the most powerful reminder is the steady stream of breach announcements that seem to continue to grow in frequency and magnitude. Organizations are being forced to re-think their security strategies and embrace the concept of data security as a core focus. Rather than being a complement to traditional network-centric strategies, data security must emerge as the primary pillar of every enterprise organization in order to properly protect their most vital asset: data.

To that end, Gartner is leading a key strategic initiative around Data-Centric Audit and Protection, or DCAP. The idea is to develop a comprehensive and enterprise-wide perspective on all data access within the organization, regardless of the underlying data sources (DBMS, Big Data, Files, Cloud services, etc.), and across all platforms, including on-prem, Cloud and SaaS. The enhanced visibility will be coupled with a unified policy tier for rationalizing policy across all sources, as well as facilities for proactive/preventive controls in order to enforce policy.



Source: Gartner (March 2017)

FIGURE 1 - Gartner DCAP Vision

At a high level this is clearly the strategy that needs to be adopted; however, as you drop down and consider how to achieve the DCAP vision, the magnitude of the challenge quickly emerges. The implications and need for change spans a broad swath of teams, tools and well-established processes, requiring a level of coordination well beyond what is typically done within many organizations. And don't lose sight of the fact that this transformation must occur "in situ" while concurrently executing already difficult security and compliance challenges with your existing tool investments.

As evidence of the degree of difficulty, consider that in Gartner's 2014 Market Guide for Data-Centric Audit and Protection the estimation was that less than 5% of the enterprise had achieved some level of DCAP strategy, while projecting that by 2018 this number would hit 25%. Fast forward to the 2017 Market Guide for Data-Centric Audit and Protection and the rate of achievement is still less than 5%, but with a goal of 40% by 2020. What will accelerate the rate of adoption given that the past several years have seen little progress?

A comprehensive and effective DCAP architecture is a multi-year journey that demands both top-down strategic initiatives as well as a series of ongoing tactical shifts, many of which must start immediately. These near-term steps will drive existing data security strategies away from being a collection of tools and silos and towards a centralized data security framework that will serve as the foundation for an evolving DCAP program. At the same time, these changes can address immediate challenges that continue to diminish the value of data security tools, especially in the face of increasingly stringent compliance regulations such as NY DFS or GDPR.

The awareness of the need for a DCAP model continues to increase and now the challenge is to leverage and optimize existing security and compliance tool investments, while at the same time evolve your overall data security strategy to establish a centralized model for visibility, control and overall effectiveness. Within this paper we review various current challenges and outline an approach for initiating the transformation to Data Centric Audit & Protection.

Managing the Security and Compliance "Hairball"

Most enterprise organizations already have deployed key components of a DCAP strategy, but they did so before the concept of DCAP even existed. Until recently this was simply a collection of tools including DAM, FIM/FAM, CASB, Classification and numerous others that were used to solve critical aspects of the enterprise security and compliance strategy. So the good news is that you likely already have multiple DCAP building blocks in place; however, the bad news may be that the list of challenges associated with these tools is already long and thus it may be quite difficult to see how these tools can be consolidated into a cohesive framework that facilitates the adoption of a more comprehensive DCAP strategy and its centralized control model.

Most enterprise security and compliance initiatives can best be described as a "hairball." A complex web of tools, teams and processes that mostly struggle to 1) capture and manage the steadily increasing flow of underlying raw data, 2) efficiently execute the manual processes required to route this data for review and remediation and 3) optimize the value from the aggregate array of tools since each tool is simply providing isolated views into pieces of the data security and compliance puzzle.

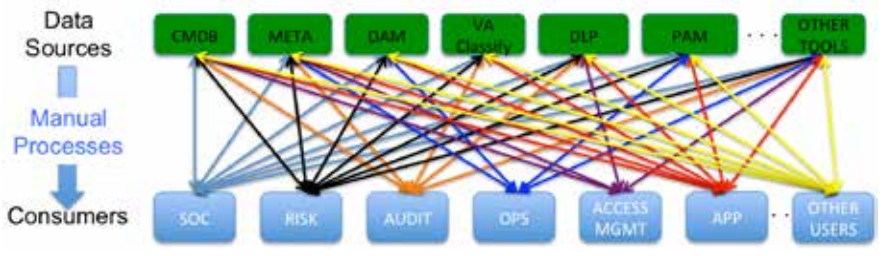


FIGURE 2 - The Security & Compliance Hairball

Moving forward without a change in strategy, the hairball will continue to grow as new tools and regulatory requirements are added to the mix, along with a steady increase in the dynamics of the enterprise environment under management. In the background is the steady pressure from the regulatory community to increase the depth of visibility and to preserve the raw data from these various feeds for years of active access and forensic exploration.

Let's take a closer look at current challenges that effect many organizations, keeping in mind that the full extent of the challenge is calculated as an aggregate of all of your tools:

Fragmented Data and Reporting

This remains a persistent challenge, as organizations manage these key steps concurrently across typically 5-10 tools, with each tool having its strengths and weaknesses in terms of reporting and data retention. Is much of your team's time spent on the mechanics of capturing and reporting on the raw data as a series of isolated reports? Is it challenging to dynamically link metadata to the raw data in order to improve the context? Do you have a solution for multi-year active data retention as defined by new regulatory requirements? While many organizations have gotten away with simply archiving data away into a data graveyard, the compliance community is rapidly rejecting that approach, as they better understand the challenges and limitations of restoring this data and demand persistent access.

Cumbersome Administration of Disparate Tasks

Looking at a "day in the life" of the security and compliance teams exposes an extensive collection of manual tasks spanning the entire lifecycle for each actionable item identified by the tools. The tool's team generates a series of reports on a recurring basis and determines the appropriate routing of these reports to their respective recipients. In many cases these are manual lookups, followed by filtering and then distribution, typically via email or Sharepoint, to an application owner for review and approval. From there it may go to a management tier and then on to security for final disposition and compliance for ongoing oversight. Seems pretty straightforward at first, but the execution and costs quickly spiral out of control when you consider this common set of challenges across the majority of the tools and the increasingly large number of people affected by these processes. And it is important to note that these complex processes directly impact the frequency at which you are able to execute scans and reviews, which of course ties directly into the effectiveness of the tool utility.

Inefficient Silos of Tools and Processes

The combination of shortcomings and nuances for each of the various tools, along with their cumbersome and extensive manual processes, leaves many leaders frustrated over the unrealized value of their tool investments, especially when viewed alongside the steadily increasing costs of their security and compliance programs. It is obvious that the threat landscape will continue to grow, as will the dynamics introduced by Cloud, SaaS, Big Data and many other emerging technologies and services.

Missing UEBA Insights

Given the explosion of raw data, User Entity Behavior Analytics (UEBA) has become a critical facility for transforming data into actionable insights; however, many of today's security and compliance tools provide little to no capability in this area and as a result often simply deliver the data downstream in the hopes that "other" tools may be able to discern behavioral patterns. While there is clear benefit to enterprise-wide UEBA solutions, it is also clear that there is significant additional value to be gained by applying UEBA engines at the individual tool level in order to more effectively isolate anomalies earlier in the inspection process.

What If...

You could decouple the data collection and management process entirely from the reporting and analysis steps and enable secure access via hundreds of commercial tools using a self-service model?

You could cost-effectively aggregate and retain years of raw security and compliance data from all of your tools and have this readily available for behavioral profiling, reporting and forensics?

The majority of your manual processes could be converted into fully automated work streams that leverage metadata enrichment, analytics and integrated workflow engines?

You could rapidly derive insights from data across all data-centric domains and also perform data-centric user behavior analysis?

It's time to dig deeper into the DCAP Central solution and discover how you can 1) rapidly solve a wide swath of current tactical challenges, 2) optimize your existing tool investments by significantly improving their effectiveness and efficiency, and, and at the same time 3) launch a strategic initiative to adopt the DCAP framework in order to more effectively achieve comprehensive Data-Centric Audit & Protection.

A Pre-Built Platform for Integrating Security and Compliance

The jSonar DCAP Central solution was designed from the ground up to address a wide range of today's data-centric security and compliance challenges, while at the same time enable organizations to rapidly increase the benefits and value available from their current tool investments. In addition, the underlying technology and architecture are specifically targeted at helping organizations adopt the more strategic security and compliance model known as Data Centric Audit and Protection, or DCAP. Rather than attempting a highly disruptive revolutionary approach to achieving the DCAP model, requiring significant investments in new tools, multi-year projects, organizational changes and process flows, DCAP Central offers an evolutionary approach that enables organizations to leverage their existing solutions while incorporating a more strategic DCAP framework that will evolve over time to achieve the full benefits of the DCAP vision.

At the core of the DCAP Central solution lies an "out of the box" security data lake specifically optimized for rapid enterprise integration, massive data sets, flexible data ingestion and consumption, advanced analytical engines, orchestration and many other capabilities. This solution goes well beyond the current definition of a data lake to provide all of the facilities needed to rapidly and substantially optimize your security and compliance initiatives. And it does so without any of the pain, cost and delays of assembling a team of developers to construct a "DIY" lake. While there is widespread consensus of the benefits of the data lake concept, there is also a growing realization that taking advantage of "free" open source technologies to construct a data lake is fraught with complexity, high costs and delays, and that a very small percentage of these programs are actually successful.

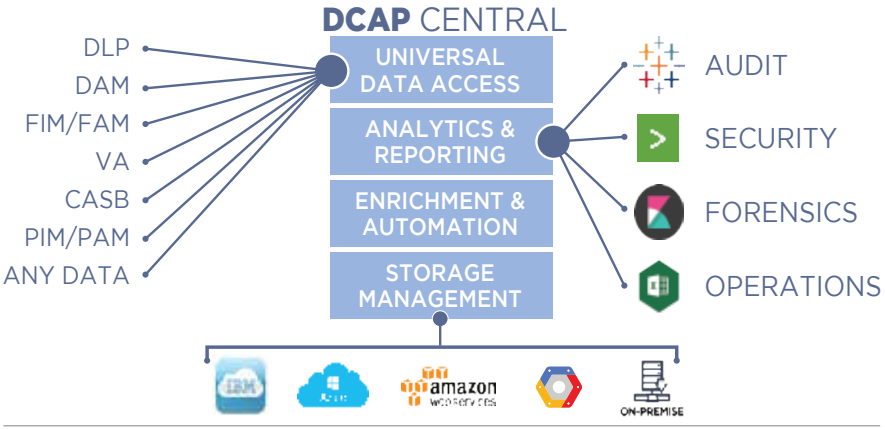


FIGURE 3 - DCAP Central Architecture

DCAP Central provides a powerful facility for centrally capturing and managing the massive volumes of data generated by a wide range of tools, thereby rapidly solving a core challenge that negatively impacts many enterprise tool teams. The current reality is that a disproportionate amount of their time and energy is spent on data/tool management, which of course detracts from the resources available to more effectively leverage the output of the various tools. DCAP Central delivers the key operational benefit of being able to take for granted that any security and compliance data is readily accessible and easily joined with applicable metadata. In doing so, teams can finally focus their resources on evolving their usage of the tools for more sophisticated policy, automation and interpretation, as opposed to constantly wrestling with the tools.

With DCAP Central, today's hairball is rapidly transformed into a comprehensive and highly flexible solution that solves a wide range of tactical and strategic challenges, increases the value of your existing tool investments and at the same time lowers the cost of security and compliance.

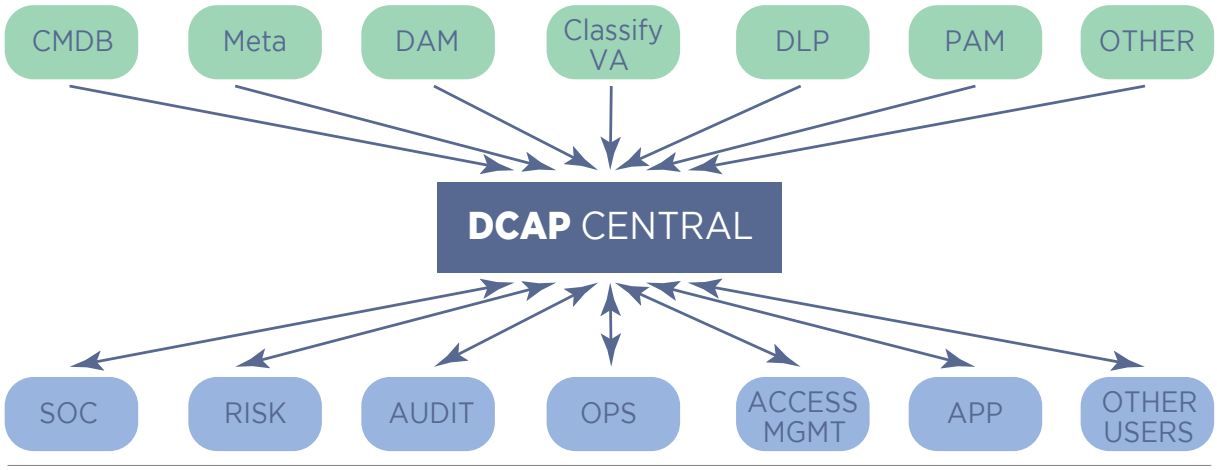


FIGURE 4 - DCAP Central Streamlined Solution

There are a number of key building blocks that enable DCAP Central to deliver these capabilities, as outlined below:

Flexible Data Consumption via Self-Service

Organizations are universally challenged by the difficulties of consuming the data generated by their various security and compliance tools, especially with the unique reporting capabilities and limitations associated with each of the tools. Specific skills and expertise are needed to overcome these limitations and often these skills are not easily applicable to adjacent tools. In several cases, customers have shared that the investment in specialized training limits their ability to migrate to different tool options, in effect a vendor "lock-in." These challenges are even associated with simple access to the appropriate data, not to mention more intelligent filtering, routing and interpretation of the data.

In addition to reporting tool limitations, many tools are closed systems from a reporting perspective and thus the consumers of their data are wholly dependent on the tool owners to create this output. This creates a bottleneck that prevents the optimal use of the tool output by a range of potential consumers. And since the tool teams are typically over-subscribed from a resource perspective, it is especially challenging to secure output for additional use cases.

DCAP Central empowers multiple data consumers within an organization to directly access relevant data via a Self-Service data access model. Rather than rely on a closed model for reporting tools, DCAP Central is architected to enable consumers to use whatever tool they are most comfortable with for interacting with the data. Business analysts may prefer Tableau, whereas a security analyst may prefer Splunk; these tools, along with hundreds of others, are fully compatible with the DCAP Central solution and provide a wide range of methods for interacting with the years of data under management. Of course a self-service model can only be effective if there are fine-grained access controls in place to restrict access to appropriate data and thus DCAP Central also includes a rich set of access control options. See Figure 5 for an example of using Tableau to analyze PCAP networking access log data stored within DCAP Central.

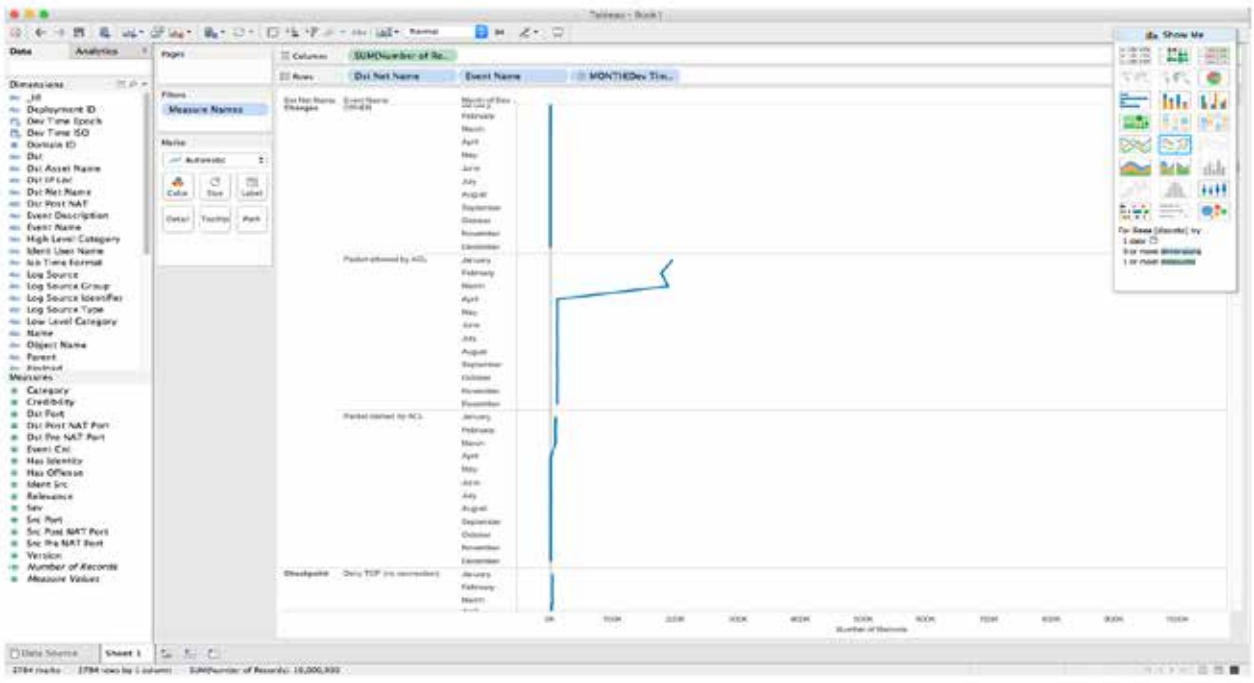


FIGURE 5 - Leveraging Tableau for Insight

There is also an enhanced Kibana subsystem (SonarK) for interactive data exploration that provides instantaneous response and powerful filtering mechanisms. The example below highlights results from Qualys vulnerability scans for the past 1 year. Note that the underlying DCAP Central data store is not the ELK stack; however, Kibana is a powerful facility for interactive access and visualization and thus an excellent complement to the platform.

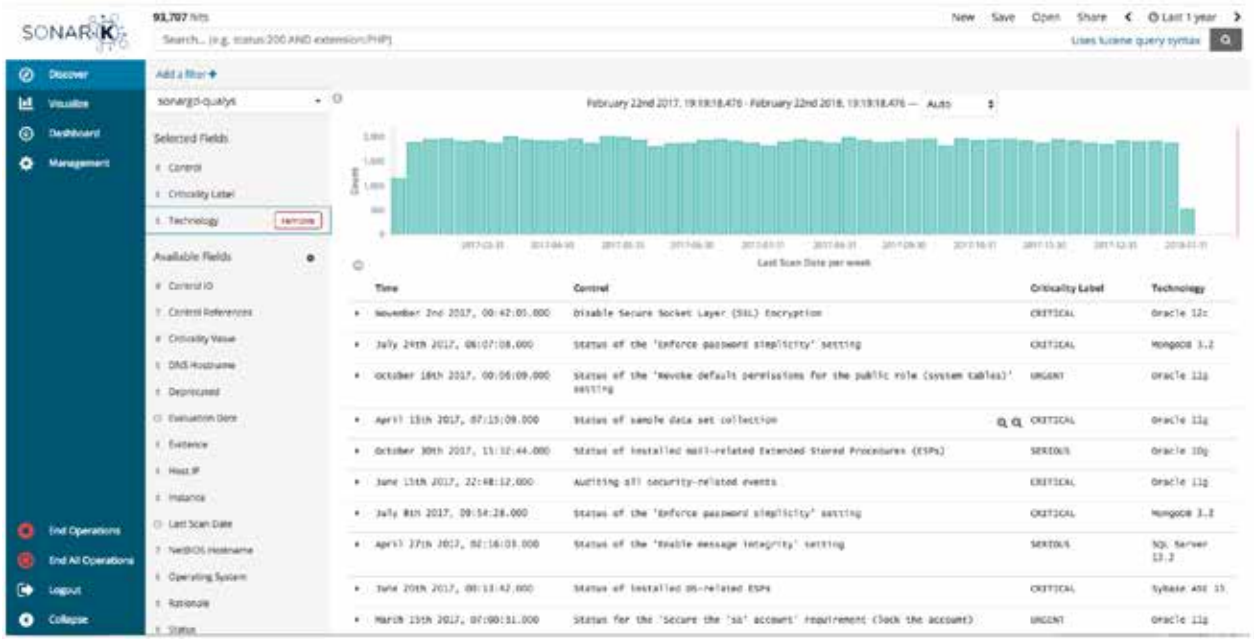


FIGURE 6 - Qualys Data Exploration

In addition to free-form interactive exploration, SonarK provides facilities for consumers to quickly and easily create their own custom dashboards to more effectively represent valuable information. The example dashboard below provides details on the top 10 DLP offenders, the top DLP targets in tag cloud form and the supporting raw data, broken down by weekly scans for the past year. Note that the construction of such a dashboard takes less than 30 minutes to create and recalculates in seconds as filters are interactively applied.

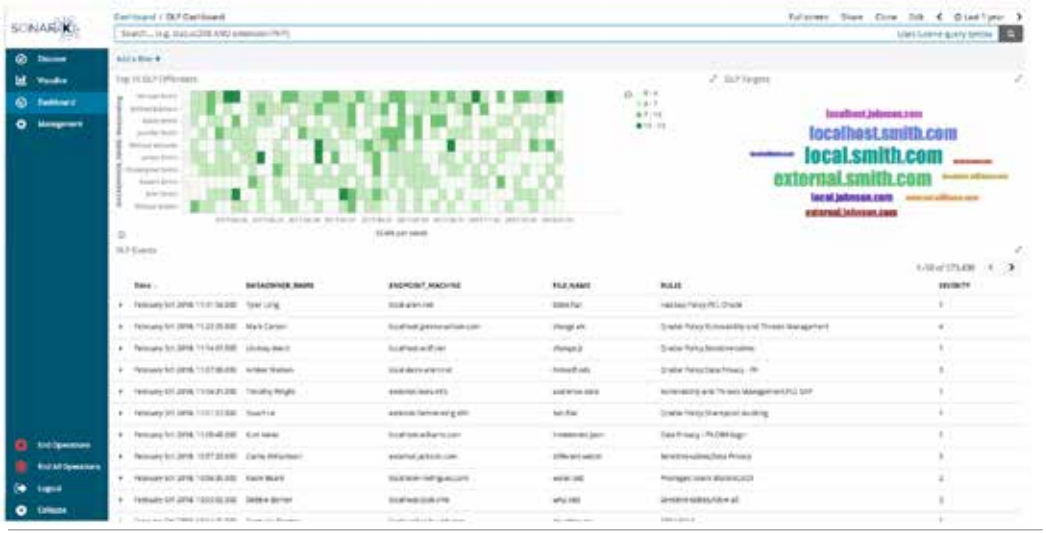


FIGURE 7 - DLP Dashboard

Increasing Value via Metadata and Context

Enterprise organizations leverage numerous tools in order to address their security and compliance needs and the aggregate of this information results in both numerous benefits and challenges. The aggregate view masks the fact that at a low level these are all independent tools and processes that operate for the most part decoupled from each other. For example, Privileged Identity Management tools such as CyberArk are key to overseeing privileged access, but why aren't they tightly coupled to the output from the tools that they are generating privileges for? Why do these disparate data sets need to be manually reconciled as opposed to leveraging automation to dynamically link their output together?

DCAP Central offers flexibility not only in ingesting data from virtually any source, but also in its ability to easily enrich/join otherwise disparate data sets to create much richer context, which in turn can drive more sophisticated automation. The secret to this flexibility is the underlying NoSQL data store that provides both schema-less ingestion and schema-on-read that can leverage any data that is housed within the DCAP Central data lake.

For example, ServiceNow has emerged as the central system of record for many enterprises and harbors a wide and steadily increasing range of data, including configuration items, change management, application ownership etc. Given the breadth of this metadata, substantial advantages can be gained by linking this directly to the various tools that are affected by this data. Shown below is a basic example of DB inventory details managed inside ServiceNow:

FIGURE 8 - ServiceNow DB Inventory Details

Any information resident in ServiceNow is available to be transferred to DCAP Central via the powerful APIs that ServiceNow makes available coupled with DCAP Central orchestration. These details can be used for reporting purposes as well as to automatically route output to appropriate users/roles in the Justify event level workflow system. Shown below are the ServiceNow DB inventory details resident within DCAP Central and accessed via the SonarK exploration tool.

FIGURE 9 - ServiceNow details in DCAP Central

The ServiceNow data, and actually any data that has been ingested into DCAP Central, can be used to create richer context around the raw data output created by the various security and compliance tools. In doing so, it becomes much easier for analysts to understand the significance of specific behaviors and also to drive sophisticated workflow automation, as will be outlined in the next section. Shown below are the results of a report that joins the ServiceNow data with results from a Qualys vulnerability scan.

Re-Query | Reduce | Timeline

#	Source System	Host IP	DNS Hostname	Operating System	Criticality Label	Rationale	Status	ServiceNow Comments
1	Qualys	1.195.111.251	dnoo.org	Ubuntu	URGENT	The 'Secure the 'sa' account' requirement (unlock the account) renders the default 'sa' user more inaccessible. As locking down the default 'sa' can help allow ordinary exploits aimed at this well-known target, this value should be set according to the needs of the business.	Failed	2015-11-16 15:17:50 - System Administrator (Additional comments) Added an attachment
2	Qualys	134.93.8.158	merriam-webster.com	Ubuntu	URGENT	The 'Secure the 'sa' account' requirement (unlock the account) renders the default 'sa' user more inaccessible. As locking down the default 'sa' can help allow ordinary exploits aimed at this well-known target, this value should be set according to the needs of the business.	Failed	2017-08-13 16:41:33 - System Administrator (Additional comments) turns out it was the sprinkler, not the rain. 2017-08-13 16:41:14 - System Administrator (Additional comments) please fix the roof
3	Qualys	180.141.31.122	ucsd.edu	Ubuntu	URGENT	The 'Secure the 'sa' account' requirement (lock the account) renders the default 'sa' user more inaccessible. As locking down the default 'sa' can help block ordinary exploits aimed at this well-known target, this value should be set according to the needs of the business.	Failed	2017-08-13 16:41:33 - System Administrator (Additional comments) turns out it was the sprinkler, not the rain. 2017-08-13 16:41:14 - System Administrator (Additional comments) please fix the roof
4	Qualys	112.8.93.39	hugedomains.com	Ubuntu	URGENT	The 'Secure the 'sa' account' requirement (lock the account) renders the default 'sa' user more inaccessible. As locking down the default 'sa' can help block ordinary exploits aimed at this well-known target, this value should be set according to the needs of the business.	Failed	2016-08-10 09:14:29 - System Administrator (Additional comments) test
5	Qualys	a104-118-179-179.deploy.static.akamaitechnologies.com	ucla.edu	Ubuntu	URGENT	The 'Secure the 'sa' account' requirement (lock the account) renders the default 'sa' user more inaccessible. As locking down the default 'sa' can help block ordinary exploits aimed at this well-known target, this value should be set according to the needs of the business.	Failed	2015-11-16 15:11:27 - System Administrator (Additional comments) Added an attachment 2015-11-02 14:05:42 - System Administrator (Additional comments) Everything is running really SLOW!
6	Qualys	101.184.75.141	fema.gov	Ubuntu	URGENT	The 'Secure the 'sa' account' requirement (unlock the account) renders the default 'sa' user more inaccessible. As locking down the default 'sa' can help allow ordinary exploits aimed at this well-known target, this value should be set according to the needs of the business.	Failed	2017-08-13 16:45:51 - System Administrator (Additional comments) I got some pat;he last night and now can't log in to the Unix box I need to for development.

FIGURE 10 - Enriching Qualys Data with Metadata

Transform Manual Tasks with Workflow Automation

A key pain point for every organization is managing both the operational processes associated with the tools themselves, and then the routing, review and remediation of the corresponding output. These processes have a significant and negative impact on operational costs, process discipline, responsiveness and ultimately the overall effectiveness of the tools themselves. How much time is spent sending emails to notify recipients that their report is ready, awaiting a response, sending a reminder to respond, remediating and then retiring the event? Could the team's time be better spent on higher value tasks such as executing scans more frequently?

"Justify" is a fully customizable event level workflow engine that provides tremendous power for applying automation to a broad range of today's manual tasks. As opposed to report level workflow systems, which operate at an aggregated data level, each event being funneled into Justify is automatically enriched to append metadata and routing logic as to determine which queue the event should be placed into for review and remediation. With this approach, the results of a vulnerability scan automatically appear in the review queue for the application owner and their entire review process is managed via a structured flow complete with a full audit trail. Something as basic as this process enhancement might save 30 minutes of FTE time per finding. Now consider that the current manual penalty applies to thousands of scans per year and that this type of process optimization could be applied to 10-20 tools and a clearer understanding of the substantial savings potential quickly comes into focus.

Shown below is an example workflow created to assist with the review of privileged user accounts. The individual event details are routed directly to the applicable admin, with routing information derived from the metadata that was imported from ServiceNow, and the admin can then justify the relevant privileged user role to their manager and if approved it can then move to Cyber and SecEng before finally being closed. Note that this approach is not only dramatically more efficient, but it also removes the tool administrators from being a key bottleneck in the review processes. If the admins or application owners were responsible for remediation and attestation on these events, why would the tool administrator need to be involved at all? And yet, for most organizations the tool administrators are currently responsible for stewarding tool results through a complex maze of manual processes.

These flows are easily customized to align with specific processes and as shown on the left side panel you can have as many workflows as needed to optimize automation across a wide range of tools and their associated process steps. No coding or professional services is needed to create and customize these workflows, enabling organizations to freely apply this automation concept to a wide range of manual process steps.

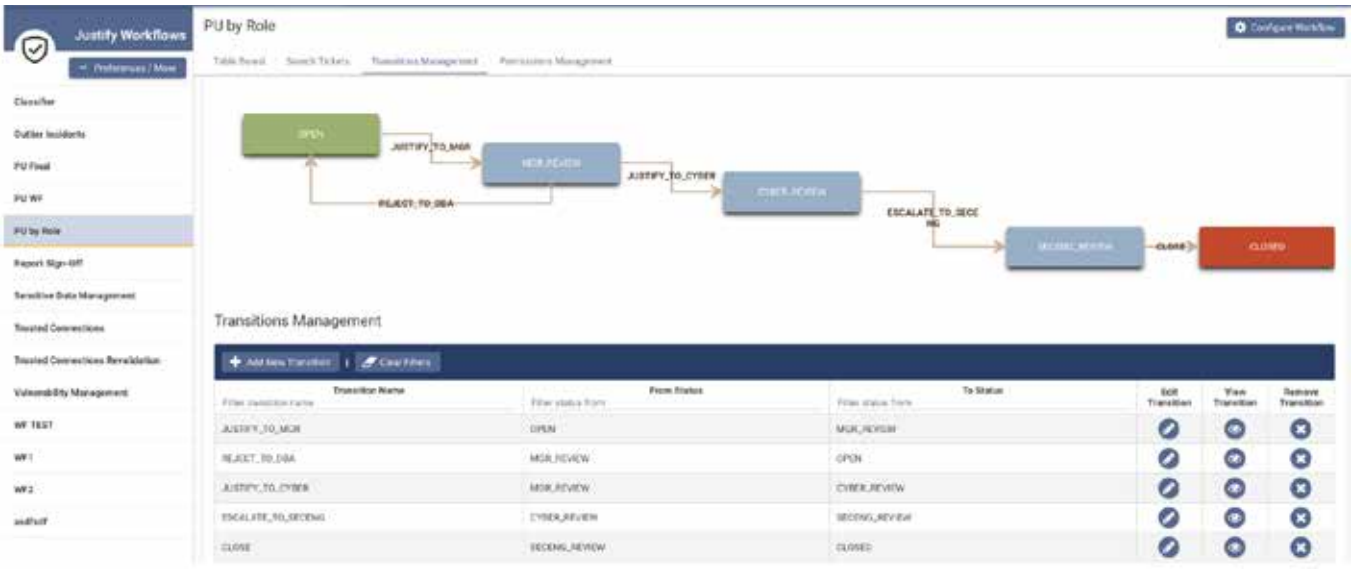


FIGURE 11 - Fully Customizable Justify Workflow Automation

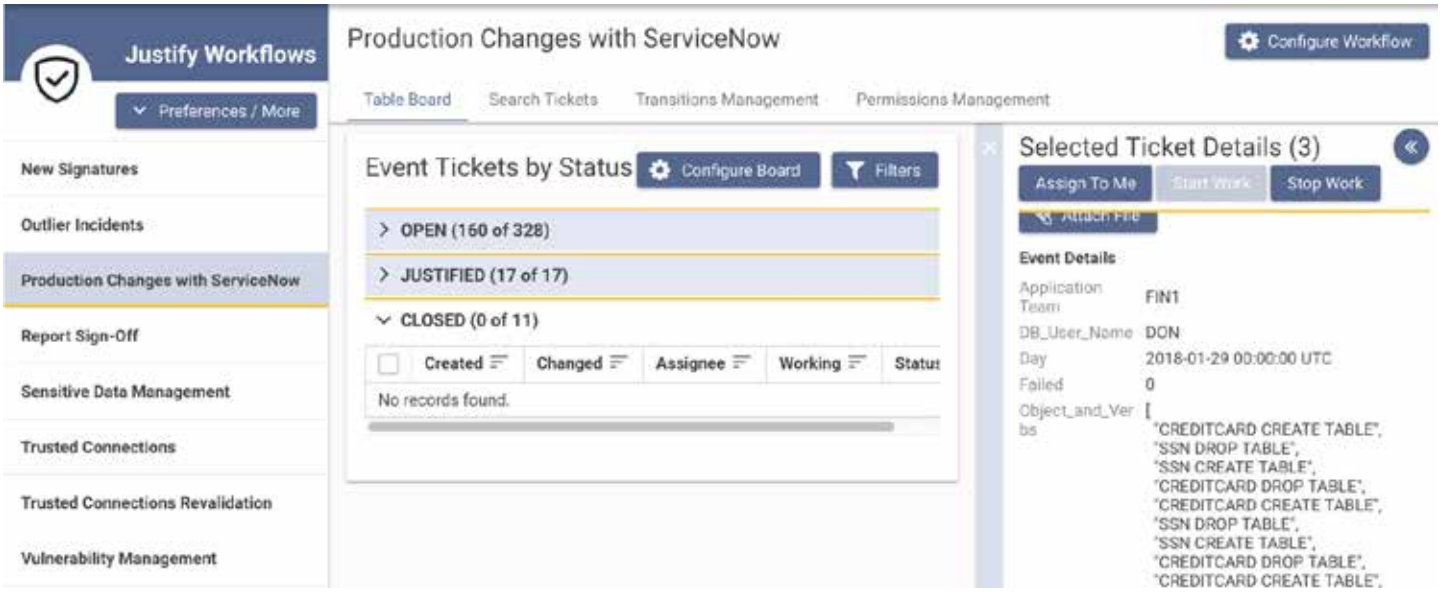


FIGURE 12 - Event Level Automation and Management

Leveraging AI and Advanced Analytics

In addition to providing a low cost facility for retaining and flexibly interacting with years of security and compliance data, DCAP Central also provides powerful analytical engines to rapidly analyze TBs of raw data to quickly convert this into actionable information. These engines are available for a broad range of use cases, including machine learning, UEBA, noise cancellation, operational insights and many others. The volumes of raw data that enterprises are collecting will continue to increase and it is critical that analytical facilities be available to assist in sifting thru TBs of data to both isolate unusual behaviors as well as to enable adjacent tools to leverage a more efficient representation of relevant security and compliance data.

For example, consider the massive volumes of SQL errors that are collected from DAM tools and the challenge associated with digesting and interpreting what can be hundreds of thousands of errors in a single day. This places a burden on the operators of the DAM tool, but also can create a substantial downstream impact on the security operations team, who may be flooded with spikes of error messages. It is simply impractical to deal with these volumes of errors and as a result they may not get the appropriate level of attention, even though a spike in error messages could easily be an indicator of unwanted behavior at the DB tier.

Figure 13 below is derived from the SQL error messages that were captured from April 1 to June 30, 2017. If you tally up the numbers in the # column you would discover that there were roughly 11.5 million errors during this period of time and this raw data would require thousands of pages to represent as a simple report, which is typically how this is presented. However, leveraging the analytical facilities of DCAP Central provides a fully-analyzed, actionable set of prioritized instructions consolidated into 14 rows that tells the organization how the 11.5 million SQL errors need to be addressed and in what order. Obviously this represents a dramatic improvement in how to deal with massive volumes of raw activity data, albeit one that is a common occurrence for more enterprise organizations.

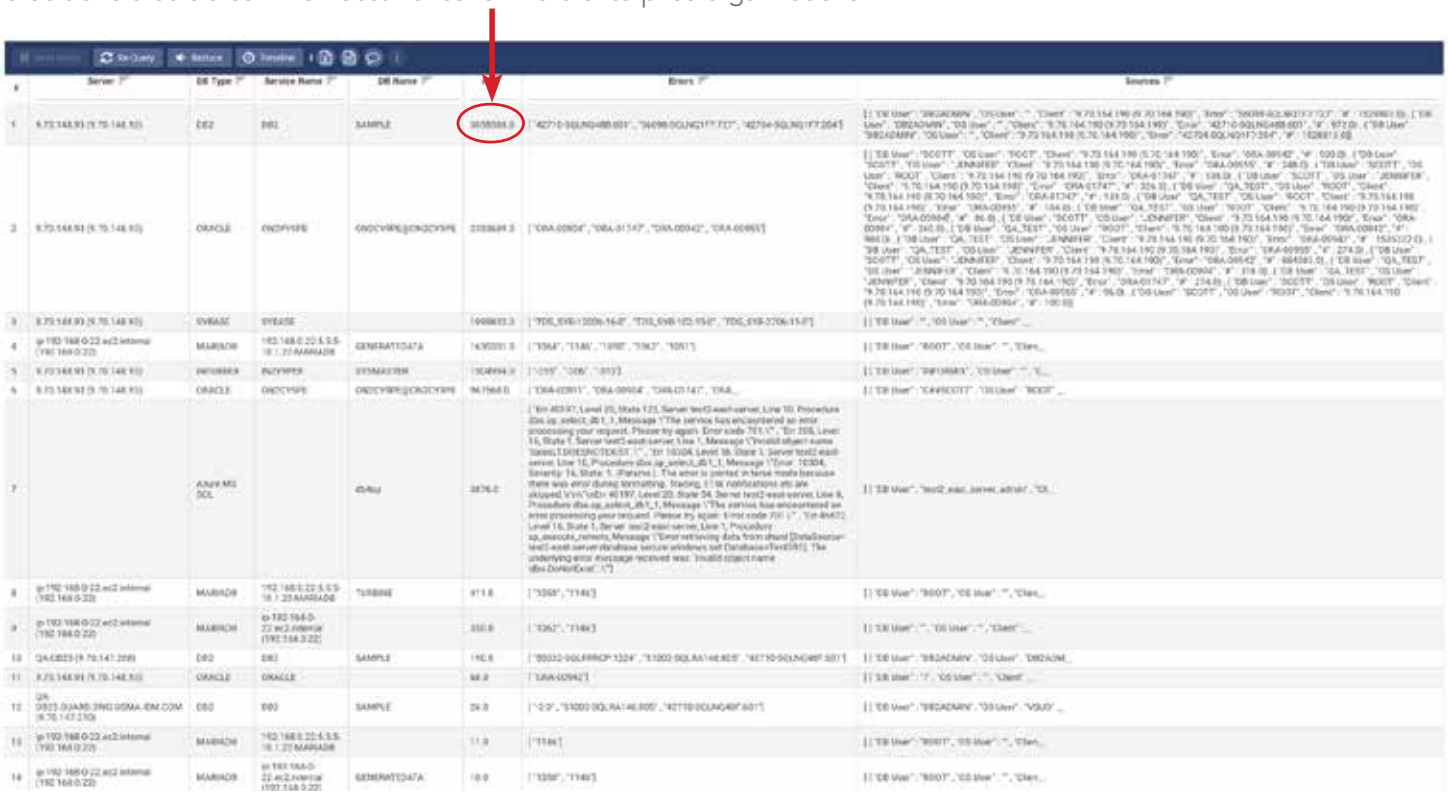


FIGURE 13 - Intelligent Analytical Perspective of SQL Errors

jSonar provides a variety of embedded analytical engines within the DCAP Central product and continues to expand this library. At the same time, DCAP Central exposes the interfaces needed for customers to apply their own analytical algorithms to the data that resides within the repository.

The underlying architecture that powers DCAP Central is hyper-efficient in terms of storage, HW and compute power. As the industry's first native-JSON, compressed-columnar data store, the architecture is ideally suited to execute analytics across large volumes of data, but without requiring large clusters of machines as is typically the case with Hadoop-based offerings. A high performance 300TB DCAP Central Data Lake can be built on a single cloud instance or commodity server and offers performance and flexibility that far exceeds clusters with 10-20X more machines.

SUMMARY

Adoption of a data-centric model is the logical evolution for information security and compliance, as traditional perimeters, data sources and application delivery models dissolve into an increasingly complex web of data interaction that is abstracted away from traditional underlying technologies. The Gartner Group's Data Centric Audit & Protection framework provides a promising vision for how to ensure security and compliance across this emerging landscape and enterprise organizations will no doubt adjust their strategies to reflect this new paradigm.

But adopting this new strategy will require substantial changes to existing processes that will likely take years to achieve. Rather than attack this as a highly disruptive migration, DCAP Central provides a powerful facility for achieving both strategic and tactical benefits. At a strategic level, DCAP Central delivers key architectural components of the DCAP vision that enable organizations to start to incorporate the critical capabilities necessary for achieving the DCAP model.

At a tactical level, DCAP Central enables organizations to solve a broad range of operational challenges that directly limit the effectiveness of the tools being relied upon to achieve security and compliance goals. The integrated DCAP Central Data Lake solves multi-year data retention and consumability issues, while at the same time streamlining numerous processes via data enrichment, analytics and automated workflows. The net result is an improvement in security and compliance effectiveness, while at the same time driving down the seemingly runaway costs of compliance.