Issue 1

VARONIS

Are You Protecting Your Data or Chasing Threats?

In the face of rapidly evolving threats and rampant data growth, data-centric audit and protection products are displacing fragmented security tools.

Issue 1

Gartner

Introduction

High-profile data breaches in recent months have boardrooms shivering in their seats. First, Alphabet Inc.'s Waymo, a self-driving startup, claimed **14,000 proprietary design files were allegedly stolen** by a former Google employee and that the information found its way into the hands of competitors. Then 8,761 files **detailing the CIA Center for Cyber Intelligence's hacking abilities** were leaked online by an **allegedly disgruntled insider**. This is frightening. In addition to raising concerns about insider threats, boards have to worry that new vulnerabilities may affect personal and enterprise computing technologies, representing new vectors of attack.

Most users don't think of data they create, access and store in terms of toxicity, but the same assets that drive revenues or establish organizational goals can and do become toxic more frequently than ever before. For Waymo and the CIA, their valuable assets -- proprietary designs and cyber-espionage tools -- were stolen, devalued and turned into potential liabilities.

Data Growth and Risk Have Collided

Within a 25-year period, organizations have presumably spent billions, possibly trillions, moving almost all analog information to a digital medium. Organizations moved financial information, product plans, strategic initiatives, and confidential employee, customer or patient records from paper to digital files spread across file and email systems, on premises and in the cloud. Many enterprises have underestimated the risks involved, focusing on increased productivity without worrying whether data would be safe from hackers, insiders, competitors and other nations.

Data growth raced ahead while information security fell behind, and the collateral damage is making headlines. Data breaches like those that happened to **Sony**, **Mossack Fonseca**, the **U.S. Office of Personnel Management** (OPM) and the **Democratic National Committee** (DNC) are practically daily occurrences. Instead of increasing revenues or furthering goals, stolen files and emails disrupt and subvert plans. If an organization stores valuable data (and most store more than they realize), someone will try to steal it. Your next breach may be perpetrated by someone who has never heard of you; ransomware, a form of file extortion, is now a **$1 billion business**.

Three Big Cybersecurity Mistakes

Worldwide cybersecurity spending is expected to exceed $1 trillion over the next five years, according to **Cybersecurity Ventures**. So why do organizations still have so many breaches?

1. Organizations spend more time and attention protecting networks, systems and supporting infrastructure than they spend on protecting the data their infrastructure was created for. That's like protecting the refinery but forgetting the oil.

2. Too much focus on preventive technologies leaves organizations vulnerable to threats that either they haven't anticipated or their technologies weren't designed to prevent. They simply don't know when their preventive controls fail or when an insider is compromised. Furthermore, organizations often fail to realize the damage an insider or outsider can do.

3. The approach to data security has been fragmented and reactive instead of strategic. According to Gartner, "The exponential growth in data generation and usage across multiple data silos is rendering current data security methods obsolete, requiring significant changes in both architecture and product selection approaches."

These mistakes mean that the invaluable assets organizations spend time and money creating, using and storing become toxic liabilities to brand reputation, revenue and national security.

The Cost of Our Cybersecurity Mistakes

In 2015, a **20-year-old hacker** performed an unsophisticated infiltration of a major U.S. retailer's network and then demanded a $500 ransom to keep the documents from being publicly released. Instead of handling the incident internally, the retail company worked with the FBI, which discovered the hacker was sending stolen data that contained personally identifiable information for more than 1,000 military and federal employees to ISIS.

Like the retailer, a majority of companies wouldn't have detected the intrusion prior to the attacker's warning. If companies cannot spot suspicious activity from unsubtle, noisy attacks like ransomware, then how will they flag unusual activity from legitimate insiders or sophisticated attackers? The Waymo complaint filed against Uber and Otto details how **multiple insiders accessed** at least 9.7 GB of highly confidential data for the competition in the days and hours prior to their departure. Even the CIA's data reportedly circulated among a cadre of former U.S. government contractors and hackers before making it into the hands of Julian Assange.

Data Security as a Driver of Revenue and Growth

The alternative to neglecting detective capabilities and pursuing fragmented solutions for data security is a unified approach to data security that combines disparate functionalities, including detection. Such a solution would combine -- either within a data security platform or through tight API integration -- data classification and discovery, permissions management, encryption, user behavior analytics, advanced threat detection and response, auditing and reporting, data access governance, and data retention and archiving.

The point is to build context around data, similar to how credit card companies build context around the way we use our credit cards; they are very good at understanding which transactions look right for each person and which ones don't. These advancements in detection keep our money available and protected at the same time. Data also needs to be available and protected at the same time.

A strategic approach to data security augments detective capabilities so insiders and breaches are found and quickly stopped, reduces the risk to an organization by limiting the amount of damage a compromised insider can do and increases the efficiency of these efforts to maintain a more secure posture with current staff levels. In most cases, the potential savings are enormous when compared with the cost of a breach.

How Does Varonis Factor into This?

In 2005, our founders had a vision to build a solution focused on protecting the data organizations have the most of and yet know the least about – files and emails. Executing on this vision, the Varonis Security Platform gives organizations full visibility into user behavior, identifies threats before a data breach occurs, enforces a least privilege model across core IT systems.

Source: Varonis

Research from Gartner

Market Guide for Data-Centric Audit and Protection

Security and risk management leaders must use data-centric audit and protection products to mitigate threats and compliance issues to critical data. These products monitor and respond to malicious or inappropriate user access behavior with data stored pervasively across on-premises or cloud silos.

Key Findings

- The exponential growth in data generation and usage across multiple data silos is rendering current data security methods obsolete, requiring significant changes in both architecture and product selection approaches.
- Most organizations have established separate teams for each data silo, with no coordination of data security products, policies, management or enforcement.
- Data is not constrained within storage silos but is constantly transposed by digital business processes and applications accessing structured and unstructured silos on-premises and in public clouds.
- Data-centric audit and protection (DCAP) vendors are rapidly adding capabilities organically and through acquisition, especially in response to increased data thefts and rapidly changing compliance landscape (such as the new General Data Protection Regulation [GDPR] for Europe, due in 2018). Only a few vendors have already achieved broad coverage both on-premises and in the cloud.

Recommendations

Security and risk management leaders responsible for application and data security must:

- Establish organizationwide data security governance in cooperation with key business stakeholders to develop appropriate data security policies that balance business objectives.
- Identify the data security controls required to mitigate the risks and threats to each sensitive data type, and then coordinate with each silo's management team and data owners to apply them consistently across all silos and applications.
- Ensure that data security policies take account of how data flows and is transposed by users, business processes, applications or big data analytics.
- Implement a DCAP strategy, and "shortlist" products that orchestrate data security controls consistently across all silos that store the sensitive data.

Strategic Planning Assumption

By 2020, data-centric audit and protection products will replace disparate siloed data security tools in 40% of large enterprises, up from less than 5% today.

Market Definition

DCAP is a category of products characterized by the ability to centrally monitor the activity of users and administrators in relation to specific datasets. Some vendors are developing machine learning or behavior analytics capabilities to provide a greater level of insight through monitoring and intelligence. Based upon data security governance (DSG; see Note 1) principles, this is achieved through the application of data security policies and access controls across unstructured, semistructured and structured data repositories or silos. DCAP products support several capabilities. They:

- Classify and discover sensitive data across relational database management systems (RDBMSs) or data warehouses, unstructured data file formats, semistructured formats such as SharePoint, and semistructured big data platforms such as Hadoop. These capabilities span both on-premises and cloud-based storage in infrastructure as a service (IaaS), SaaS and database as a service (DBaaS).
- Set, monitor and control privileges of unique user identities (including highly privileged users such as administrators and developers) with access to the data. The ability to provide segregation of duties, whether based on role-based access control (RBAC) or attribute-based access control (ABAC) principles, remains a critical function for access control and monitoring against specific sensitive data classifications.

- Use behavior analytics techniques to monitor users when accessing data in real time, generate customizable security alerts, and block unacceptable user behavior, access patterns or geographic access, etc.

- Create auditable reports of user access to data and security events with customizable details that can address defined regulations or standard audit process requirements.

- Prevent specific data access by individual users and administrators. This may also be achieved through encryption, tokenization, masking, redaction or blocking.

- Provide a single management console that enables the application and orchestration of data security policies consistently across multiple data repository formats (referred to here as data silos).

Segmentation

Current Gartner research refers to four market segments where products are evolving the critical cross-silo DCAP functionality: database audit and protection (DAP); data access governance (DAG); cloud access security broker (CASB); and data protection (DP), which includes encryption, tokenization, redaction and data masking. The different evolutionary tracks mean that products will inevitably have differing basic objectives and functionality in their product roadmaps. While no individual product fully meets the requirements of DCAP, the products in each of these categories are evolving capabilities across the data silos:

- **DAP** — These products have developed over several years to cover implementation of data security policies, data classification and discovery, privileged access management, data activity monitoring or behavior analytics, audit and data protection. Previously, focused on RDBMSs and data warehouses, a few products are beginning to offer support for Hadoop and unstructured file shares, and for DBaaS.

- **DAG** — This is sometimes referred to as file-centric audit and protection (FCAP). Typically, these products are focused on implementation of data security access policies, data classification and discovery, and activity monitoring and auditing of file repositories and directories services, such as SharePoint. These products are closely tied to identity and access management (IAM) approaches. Some products also are also beginning to include capabilities for cloud SaaS applications.

- **CASB** — The ability to protect data within SaaS applications or cloud storage environments such as Microsoft Office 365, Salesforce, ServiceNow, Box and Dropbox is growing rapidly through several products. These products encompass an evolving set of data security controls that cross DCAP, data loss prevention (DLP) and user entity behavior analytics (UEBA). CASBs are continuing to evolve varying mixes of data classification and discovery, access controls, activity monitoring, audit, and protection through blocking, redaction, encryption, tokenization and quarantine. These products are typically stand-alone and some CASBs can import policies from enterprise DLP products, but their management is not integrated with on-premises DLP.

- **DP** — These products traditionally focus on protecting data using encryption, tokenization or masking across multiple data silos (RDBMSs, data warehouses, unstructured, big data, and some cloud-based enterprise file synchronization and sharing [EFSS] tools). But a few products have innovated by adding real-time alerting, activity monitoring and audit capabilities. Whereas DAP and DAG products may offer monitoring and audit of access to all data within files or databases, these DP products are typically focused on sensitive data types only.

Products can use a variety of techniques to connect via the application layer and/or data layer. Application layer agents, interfaces or integration with privilege management tools may be required to control individual access from the application layer when connection pooling that would otherwise hide identities is used. Alternatively, products that operate at the application layer and use network monitoring or proxies may not be able to view activities of database and system administrators at the data layer without further controls.

Market Direction

Data Security Governance Is Driving Adoption of DCAP

There are many data security products available, each with different security control capabilities, but most focus on particular data silos. The challenge facing organizations today is that data

is pervasive and does not stay in a single silo on-premises, but is compounded by the use of cloud SaaS or IaaS. There is a critical need to establish organizationwide data security policies and controls based upon DSG. DSG allows an organization to achieve a balance between appropriate security and competitive advantage by classifying data and prioritizing security and expenditure for particular sensitive datasets. Each dataset has its own protection, storage and controls that will vary as a function of time (for example, sales, intellectual property and personally identifiable information [PII] datasets have different lifetimes). By using the DSG process to engage key stakeholders such as business, IT, governance, compliance/legal and risk, organizations can then approve whether each dataset merits investment in security controls that mitigate particular risks associated with compliance, data threats or to protect intellectual property.

Understanding the relationships between DCAP and DLP capabilities is critical to building an effective DSG framework. DCAP and DLP are often sourced, deployed and utilized by different teams within an organization. Separate groups might be responsible for data in one or more silos, and might have limited communication with others in the organization. Cross-silo communication is needed to build efficient and optimized policies and reporting capabilities to effectively track and measure cross-silo data flows. This problem amplifies with each new application (whether on-premises or SaaS) that touches a new data repository. The only effective answer is to look at tools and processes with which an organization can map end-to-end data flows and identify when applications or business processes deviate from the accepted methods of data movement established by DSG.

The need to apply consistent policies at the application layer and data layer is a critical challenge when the application hides the user identity, for example, due to connection pooling. Gartner predicts this will force product innovation to integrate with application layer identity governance and administration (IGA) and privileged access management (PAM) products.

Market Drivers

Organizations have experienced an increasing wave of publicized data breaches caused by external hacking, insider threats and human error, resulting in significant financial liabilities, brand damage and loss of customers. This has been evidenced by Gartner's[1] publicly available analysis of public breaches in the U.S.[2]

The advent of big data platforms, cloud SaaS and IaaS environments and the increasing adoption of IoT and digital services are driving organizations to review their strategies for data security.

Data residency and compliance issues continue to cause increasing risk to organizations when storing data sourced from different geographies in public clouds. In the EU, the new General Data Protection Regulation (GDPR) will take effect beginning May 2018 and will affect any organization across the world that processes or stores any PII from the EU; and many privacy laws around the world will impact storage locations.[3] New York state's cybersecurity regulation took effect 1 March 2017 and follows many principles of the GDPR.[4] Security and risk management (SRM) leaders will need to ensure that they understand and comply with all relevant and required regulations in all jurisdictions that they conduct business in.

Traditional data security approaches are limited because the manner in which products address policy is siloed, and thus the organizational data security policies themselves are siloed. For example, the approach to structured database security governance is frequently different from the approach taken for unstructured or semistructured data in an organization. Transposing data from one silo to another (for example, through analytics or extracting data for reporting or sharing) creates an interrelated data processing environment that lacks consistency and synchronization of security policies. This leads to security chaos because SRM leaders have not developed processes to deal with it.

These critical risks are forcing SRM leaders to urgently prioritize their security strategy across all silos containing sensitive data. SRM leaders must

develop a comprehensive policy — based on data security governance principles — and apply security controls that are appropriate and in balance with organizational business objectives across all affected data silos. This may require the purchase of more than one DCAP product to match the targeted silos, as well as the development of management structures that coordinate and align data security policy and accountability across silos.

Market Dynamics

The DCAP market is on track to become a very different market by the end of 2018, with repositioned and more comprehensive product offerings. Several vendors will offer full DCAP products, covering all of the data silos, while many other vendors will continue niche strategies that will limit their coverage to one or two silos. However, Gartner estimates the total market grew rapidly in 2016, more than 20% to exceed $1.2 billion.

Gartner has seen several vendors already stretch into adjacent silos, and, in the near term, many of these vendors will continue to develop capabilities across adjacent silos and across cloud and big data platforms, either organically or via partnerships. While CASB vendors lack support for on-premises data silos, this is beginning to change due to acquisition activity. The innovation through cross-siloed product offerings and the important shift to address identity management at the application layer are changing the dynamics and attractiveness of separate market segments into one larger market. Currently, the DCAP, DLP and data protection markets are typically serviced by different vendors. But this will change through 2018, with increasingly converging capabilities, especially through the addition of CASB and behavior analytics. As on-premises structured and unstructured product capabilities naturally converge and integrate with NoSQL and cloud products, innovation and product diversification will intensify in the following ways:

- Many vendors will offer machine learning or behavior analytics as a feature to improve real-time intelligence and monitoring of user access to data. This will be critical to tackle the risks from growing compliance requirements and security threats.
- Most of the DCAP vendors will offer centralized management platforms that can directly control data security policies across multiple data silos.
- DCAP will extend capabilities across data and application layers to avoid connection pooling issues. The application layer is the new battleground for product differentiation, with potential for acquisitions, mergers and new entrants.
- Competition between vendors will intensify through support for newer NoSQL DBMSs, such as Hadoop or MongoDB, requiring the integration of policy enforcement functionality across multiple platforms.
- Vendors will expand capabilities to the rapidly emerging DBaaS platforms.
- More vendors will either directly integrate their own data protection functionality within the management console or will develop functionality where it is lacking.

The Market Is in Flux

There are new entrants, as some vendors have been subject to acquisition and even demerger. Some notable changes to the DCAP competitive landscape include:

- Forcepoint acquires Skyfence from Imperva (January 2017)
- Huawei acquired HexaTier (December 2016)
- Elliott Management and Francisco Partners acquired Dell Software Group business and renamed it Quest (November 2016)
- Symantec acquired Blue Coat (June 2016), which had previously acquired Elastica and Perspecsys
- Cisco acquired CloudLock (June 2016)
- Oracle acquired Palerra (September 2016)
- Imperva announces CounterBreach — an integrated DCAP behavior analytics product integrating its Skyfence CASB and on-premises SecureSphere products (March 2016)
- Blue Coat acquired Elastica (November 2015)
- Symantec sold Veritas to an investment group led by The Carlisle Group with DLP remaining with Symantec and DCAP moving to Veritas (August 2015)

- SailPoint acquired Whitebox Security (July 2015)
- Blue Coat acquired Perspecsys (July 2015)
- Imperva acquired Skyfence (February 2014)

SRM leaders should expect these activities to continue and increase as compliance issues relating to data privacy and financial regulations escalate and the risk of data breaches intensifies, resulting in increasing need for DCAP products.

Market Analysis

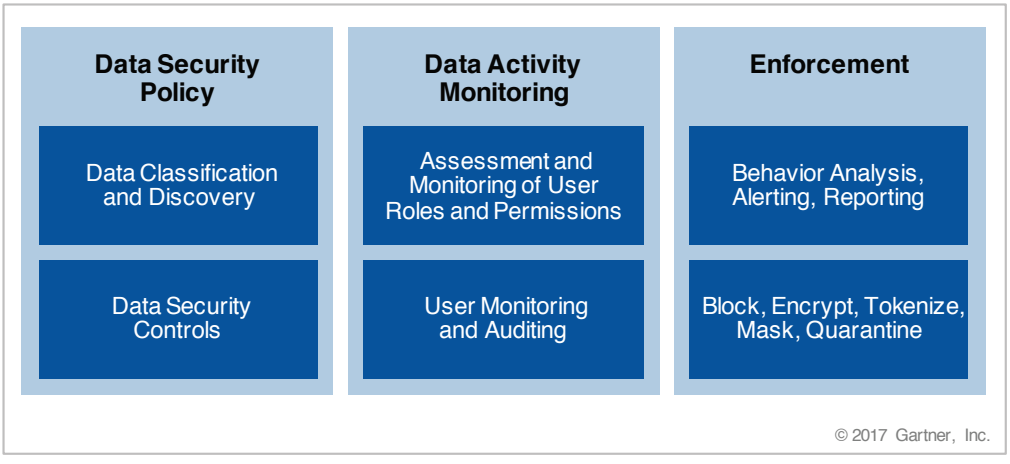
The market segments that contribute to DCAP have evolved over vastly different time scales with different security focal points and business drivers. Convergence of product capabilities toward NoSQL, from vendors previously focused on database and unstructured files, has created a surge of interest in a much larger market opportunity through the combined segments. Convergence of these adjacent markets is driving current organic developments, but has also attracted new entrants from the DP market. The continued growth in adoption of cloud services is driving market exposure to existing CASB vendors that have been developing data protection and activity monitoring functions.

Most vendors have developed a common functionality to classify and discover data, manage and monitor access, provide auditable reports, and provide some form of protection (see Figure 1). However, these capabilities are not created equally, and care should always be taken to ensure that the selected products properly address your data security governance policy and control requirements.

A vendor's ability to integrate these capabilities across multiple silos will vary between products and also in comparison with vendors in each market subsegment. Below is a summary of some key features to investigate:

- **Data Classification and Discovery** — Many products come with built-in dictionaries or search algorithms tailored for use with compliance regimes such as PCI, HIPAA or GDPR. But the search capabilities of different products will vary, for example, in terms of speed and false-positive performance. The ability to search within a specific DBMS, file type, Hadoop or cloud will vary from vendor to vendor. If you are planning to use the product with DBMS silos, note that some products may only search the column/table metadata or within fields. Also, check if data can be searched within a binary large object (BLOB) or character large object (CLOB) that may be stored within the database. Some vendors may only have a capability to search within unstructured files and rely on tagging through the attachment of metadata to each file. If data is encrypted or tokenized, then discovery may not be possible unless that protection product is integrated with the DCAP product and it is provided with access privileges via automatic decryption.

FIGURE 1 Summary of the Core DCAP Capabilities Offered by Vendors in Each Segment



Source: Gartner (March 2017)

- **Data Security Policy Management** — The ability to offer a single management console that controls policy across each silo is the desired goal, and it will evolve as vendors encompass more silos. Most products will split this functionality, or separate vendor products will be required. In either case, separate software interfaces or separate management consoles will be required. Coordination of roles and responsibilities against the underpinning data security governance will be important. The application of policy is typically based on user identities and business roles as authenticated through third-party products such as active directory (AD) or LDAP. Membership of groups can help define access to particular data within a silo, or even multiple groups when granting access to multiple silos. The ability to identify individual users at the application level can be a differentiator if applications use connection pooling to provide a more efficient group access account. This can sometimes be enabled by communication with the application through authentication protocols such as Kerberos, but not all applications provide this capability. Other products may use application layer agents to gather identities, correlate logs from application tools, or use proxy-type technologies to intercept and analyze network commands from the application or web servers. Application-layer-focused tools will not have a view of administrator access at the data layer. Care should be taken that additional controls are also in place to address this, such as additional agent software monitoring agents or encryption at the data layer.

- **Monitoring User Privileges and Data Access Activity** — Security policies are specified to manage and monitor the privileges for all application users and administrators with access to specific datasets. It is important to monitor for changes to AD membership or changes to individual privileges to ensure they match requirements associated with business role, data type or geographic location. The ability to detect changes and create alerts for privilege escalation or for changes to data is important to detect potential malicious insider or external hacking activities and to meet certain compliance mandates. However, not all products operate at the storage level, and they may not offer the ability to assess highly privileged users such as database administrators, system administrators or developers. Therefore, it is also important for a product to be able to intercept access by various administrators at both the data and application layers. Products need to demonstrate continuous operation during peak loading of servers or network communications congestion. If intensive monitoring is required while infrastructure is highly loaded, consideration must be given to the network architecture and to the demands required of products. This can lead to latency or, in extreme cases, failure to monitor some activity.

- **Auditing and Reporting** — As the data analysis requirements continue to grow, the demands on the reporting capabilities will grow also. Auditors in various regulatory environments will require an ability to produce insights into the activity of users on a historical basis, which can require at least one month of accessible data. Compliance will also require an audit trail of various monitoring capabilities, such as unusual user behaviors, changes to data, policy violations or changes to privileges. In the event of a breach or security incident, it is important to be able to use the audit logs as a forensic analysis aid to investigate all activities including access, data changes or privileges.

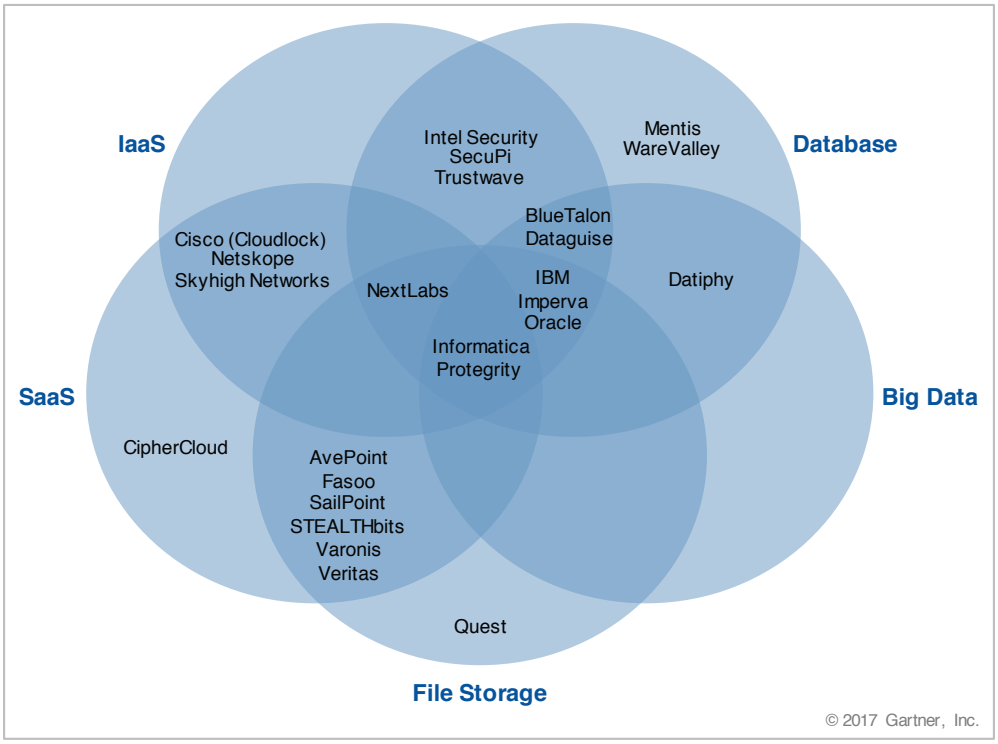
- **Behavior Analysis, Alerting and Blocking** — An ability to create security alerts based upon preselected monitoring criteria is critical, and this might result in different levels of alert that range from policy violations to suspicious behavior in relation to the data accessed. Mechanisms for alerting include console displays and automatic messaging to key security staff, data owners or business staff. Other functionalities may be enabled, such as automatic blocking of a process, access or removal of privileges. Extreme responses might include shutting down all access in the event of very large data downloads. Future products may even correlate rules to detect unusual behaviors. The ability to analyze historical access trends will provide increasingly important forensic insights to detect inappropriate behaviors. Products vary in the ease of use of the management console interfaces to manage and report security alerts, and in the granularity of reporting within the different data storage platforms. For example:

- In relation to databases, there may need to be a trade-off between the number of commands that can be inspected against the ability of software/hardware technology to process and communicate the results for analysis. This can happen if servers or network communications are already heavily loaded and the ability of local monitoring agents to process the large volume of commands is then constrained. Data access can be blocked based upon data content and group membership or privileges.

- When consoles are overseeing multiple silos through agents or software with devolved policy management or different monitoring capabilities, there may be different false-positive results.

- **Data Protection** — Some vendors offer separate data protection tools using encryption, tokenization or data masking, while others do not offer any tools and will require the purchase of separate vendor products. In either case, these protection products may not be integrated into a single management console and will require careful coordination with data security policies. The selection of these tools requires careful assessment of the threats and risks that each can offer. For example, implementing transparent, database-level encryption can prevent access by system administrators, but database administrators would still have access. Applying dynamic data masking through an agent on the database server, and linked via AD, can be used to prevent access by database administrators. However, the data is not protected when stored at rest; it may still be accessible by system administrators. Encrypting or tokenizing fields can protect the data elements in use and at rest, but care must be taken that this does not affect the operation of applications. Management of data protection tools is also critical, but will produce its own overheads.

FIGURE 2 Schematic Diagram for the DCAP Market Showing a Sample of Vendor's Coverage of Overlapping Data Silos



Source: Gartner (March 2017)

Representative Vendors

The vendors listed in this Market Guide do not imply an exhaustive list. This section is intended to provide more understanding of the market and its offerings.

The DCAP market is characterized by vendors with product strategies covering DBMSs; unstructured file stores (files); semistructured environments such as SharePoint, NoSQL, MongoDB and Hadoop; and cloud services. Some innovative data protection vendors are developing a centralized management console approach across multiple silos, but lack comprehensive DCAP capabilities. A representative mapping is shown in Figure 2, but note that none of these vendors can currently be assessed as yet offering a complete DCAP product.

Table 1 shows a sample list of DCAP vendors that are categorized by the main capabilities outlined in this research (see the Market Analysis section). The following bullet points should be used when reviewing the list of capabilities:

- This table does not compare the extent of each vendor's capabilities, nor how they compare across each of the data silos — DBMS, file stores, big data, DBaaS, SaaS or IaaS.
- Vendors must offer all of the DCAP capabilities before being considered to have a "Y" in any particular silo.
- Vendors may require the installation of more than one product to provide their full set of capabilities. For example, tools for data classification and discovery may not be integrated with the core activity monitoring product, or the vendor may rely on another vendor's product.
- Management of privileges such as read/write or access must be based upon specific classified datasets. Privilege management of individual users may not always be possible at the application level due to connection pooling, and vendors may only be able to enforce controls broadly across all users or none.
- Activity monitoring of users and administrators may be limited to monitoring access to certain classified datasets, and some products focus on only classified datasets. Products that are based in the application layer, monitor network traffic or use proxies may not be able to monitor activity by administrators in the data layer. Additionally, due to connection pooling, monitoring application users directly from the data layer may not be possible.
- Audit and reporting capabilities are typically focused around specific compliance requirements.
- Data protection can be one, or a combination, of the capabilities of blocking, encryption, tokenization and data masking. Quarantine is an additional useful feature, but not considered sufficient by itself. Only a few vendors currently integrate policies for data protection with activity monitoring and access privileges.

Table 1. Sample List of DCAP Vendors Against Capabilities for Five Data Silos

	DCAP Capabilities						Data Silos				
	Behavior Analytics	**Simple Monitoring & Alerting**	**Integrates Policies Across All Silos Covered**	**Integrated Data Discovery or Structured (S) or Unstructured (U) Only**	**Appli-cation User Access Control**	**Data Protection Policy Enforce-ment**	**Data-base**	**Files**	**Big Data**	**SaaS**	**IaaS**
AvePoint		Y	Y	Y	Y	Y		Y		Y	
BlueTalon		Y	Y	Y		Y	Y		Y		Y
CipherCloud		Y		Y	Y	Y				Y	
Cisco (Cloudlock)		Y	Y	U	Y	Y				Y	Y
Dataguise	Y	Y	Y	Y	Y	Y			Y		Y
Datiphy	Y	Y	Y	S	Y		Y		Y		
Fasoo		Y		U	Y	Y		Y		Y	
IBM	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y
Imperva*	Y	Y	Y*	S		Y	Y	Y	Y	Y*	Y
Informatica	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y
Intel Security		Y		Y			Y				Y
Mentis		Y		Y	Y	Y	Y				
Netskope		Y	Y	U	Y	Y				Y	Y
NextLabs		Y	Y	Y	Y	Y	Y	Y		Y	Y
Oracle		Y		Y	Y	Y	Y	Y	Y		Y
Protegrity		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Quest		Y	Y	U	Y			Y			
SailPoint		Y	Y	U		Y		Y		Y	
SecuPi	Y	Y	Y	S	Y	Y	Y				Y
Skyhigh Networks		Y	Y	Y	Y	Y				Y	Y
STEALTHbits		Y	Y	U	Y	Y		Y		Y	
Trustwave		Y		S		Y	Y				Y
Veritas		Y	Y	U	Y			Y		Y	
Varonis	Y	Y	Y	U	Y	Y		Y		Y	
WareValley		Y		S	Y	Y	Y				

*Note — Imperva's monitoring of SaaS is achieved using its CounterBreach product, but also requires a separate license of the Forcepoint CASB product.

Source: Gartner (March 2017)

Note, the capabilities of products from each vendor can vary significantly in relation to breadth and depth of functionality, integration with applications and data silos, and even the policies or analytics. Therefore, SRM leaders need to select products that suit their data governance strategy and security requirements. For example, if there are compliance requirements to provide full auditable assessments of users accessing a database, then DAP vendors will have the most comprehensive RDBMS abilities to inspect all SQL commands.

Market Recommendations

- Establish a data security governance strategy supported by DCAP that is approved by key business stakeholders, which should include business, IT, security, compliance and risk. The main outcomes will be a classification of sensitive data types, compliance requirements, risks and threats. These will be balanced against any necessary trade-offs to business access through, for example, IT systems, staff locations or customer needs.

- Establish and develop data security policies that set out the necessary security controls for specific datasets and storage locations. This will require coordination and cooperation with the data owners and various security management teams that are deployed for each of the data silos to coordinate the controls that will be implemented by the DCAP products.

- Evaluate the data controls required and which silos need protection, and decide if any DCAP product options meet these requirements against each category. The early market trends have shown that some vendors already cross silos (see Figure 2 and Table 1).

- If you only have one RDBMS platform or file storage type, such as SharePoint, you may be able to provide basic controls through native capabilities and extraction of log data to other network security tools, such as security information and event management. Note that reliance on SIEM tools for monitoring typically loses the context of which sensitive data is the subject of activity.

- Identify applications that extract data or transfer data to adjacent silos, given certain user privileges. Any new user access to the data must be understood within the new silo to verify if the privileges are appropriate, given the original data sensitivity. Decide if privileges need to be managed for the application as a whole (connection pooling) or if individual access controls are required. Therefore, identify how the controls need to be implemented, with appropriate DCAP product or products to address each silo.

- Given the shortlist of relevant DCAP products, analyze the internal architectural loading and network communication constraints to determine each product's ability to deliver the necessary monitoring and data protection.

Evidence

[1] Over the past year, Gartner has spoken to more than 300 clients to discuss requirements for data protection and activity monitoring. These discussions have highlighted the shortcomings of existing siloed products and their lack of a coordinated data security policy across silos. Discussions with many vendors have also highlighted their desire to address unmet needs for data security governance and data security policy through a DCAP approach.

[2] Identity Theft Resource Center **Data Breaches**.

[3] **"Data Protection Laws of the World."** DLA Piper.

[4] **"Cybersecurity Requirements for Financial Services Companies."** New York State Department of Financial Services.

Note 1

Data Security Governance

Data security governance refers to a subset of information governance that deals specifically with protecting corporate data (in both structured database and unstructured file-based forms) through defined data policies and processes, and implemented via technologies that are drawn from products such as DCAP, CASB and data loss prevention, among others.

Source: Gartner Research, G00298197, Brian Lowans, Marc-Antoine Meunier, Brian Reed, Deborah Kish, Merv Adrian, David Anthony Mahdi, 21 March 2017

Varonis Case Study: The City of San Diego

Background

Gary Hayslip, hired by the City of San Diego as its first CISO in 2013, has been involved with cybersecurity for nearly 30 years and co-authored the book, "The CISO Desk Reference Guide." In his current role, he is responsible for the development and implementation of the city's information security strategies, policies, procedures and internal controls. For a city of more than 1.3 million people, Hayslip advises the city's executive leadership and protects a network that blocks about half a million cyber-attacks a day.

After a careful evaluation, the City of San Diego chose to implement the data security platform from Varonis, which includes Data Classification Framework, DatAdvantage for Windows and Directory Services and DatAlert solutions.

Hayslip said, "The more I began to examine the cybersecurity landscape, the more I realized that the traditional perimeter security strategy was inadequate for the threats we currently face today. In my present enterprise environment, we don't have one network. We have 24 networks, with about 40,000 endpoints spread across the county, and we have employees on mobile devices like smart phones and laptops in the field. It's this disparate view that brought me to the conclusion I needed to move security from the edge down to the data level, where my data flows are at, and actually start tracking who's accessing it and what's being done with it."

Ransomware

Hayslip continued, "We have 14,000 desktops, in everything from police cars to trash trucks, sitting in city buildings or laptops out in the field, and they get phishing emails. In the last year, we've gone from averaging five ransomware attacks a month to now around 10-15 times a day – all because someone clicks on something they shouldn't have. The growth in malicious activity is largely due to the fact that ransomware makes cyber criminals money. Varonis DatAlert helps us to identify and stop these breaches. It helps us better understand if the ransomware was successful and whether it reached any of our share drives. We need this context so we can respond quickly and stop it from expanding and destroying folders."

Data-Centric Audit and Protection

"We process everything from credit card payments to trading municipal bonds. There are several different regulatory verticals that our data, accounts and business practices fall into, and I wanted to build a data security platform to look at all the various types of data the city has, who is accessing it and the practices we have for processing it. Varonis is that platform for us."

Hayslip added, "As we started using Varonis, particularly the Data Classification Framework and DatAdvantage for auditing and protection, we were able to see data that was stale and hadn't been touched in years. The interesting thing about cities is that if a technology works they will keep that technology and its data forever. Unfortunately, that can mean cities won't innovate and try a new technology unless the old one breaks or they are forced to change. Currently, we estimate we have more than five petabytes of data – copies of copies of copies of copies. We estimate that we can probably reduce that amount by about 30% through understanding how our data is used and identifying what we truly need for operations. One of the most valuable things that Varonis has been able to do for us is to identify stale data that isn't needed for business operations. We're able to store it in less expensive facilities and remove unnecessary duplicates, freeing up a lot of critical space and saving money."

Source: Varonis

About Varonis

Varonis is a leading provider of software solutions that protect data from insider threats and cyberattacks. Through its innovative Data Security Platform, Varonis allows organizations to analyze, secure, manage, and migrate their volumes of unstructured data. Varonis specializes in file and email systems that store valuable spreadsheets, word processing documents, presentations, audio and video files, emails, and text. This rapidly growing data often contains an enterprise's financial information, product plans, strategic initiatives, intellectual property, and confidential employee, customer or patient records. IT and business personnel deploy Varonis software for a variety of use cases, including data security, governance and compliance, user behavior analytics, archiving, search, and file synchronization and sharing. With offices and partners worldwide, Varonis had more than 5,500 customers as of March 31, 2017, spanning leading firms in financial services, healthcare, public, industrial, insurance, energy and utilities, media and entertainment, consumer and retail, technology and education sectors.

Click **here for a free data risk assessment** to find and fix your data security risks.