Enterprise Strategy Group | Getting to the bigger truth.™

White Paper

DataGravity and Continuous Sensitive Data Monitoring

By Jon Oltsik, Senior Principal Analyst

July 2015

This ESG White Paper was commissioned by DataGravity and is distributed under license from ESG.

Contents

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change from time to time. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of The Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at 508.482.0188.

Executive Summary

Ask any cybersecurity professional and she'll tell you that it's getting more difficult to prevent, detect, or respond to cyber-attacks, data breaches, and even data exfiltration. Why? The threat landscape continues to grow more dangerous while IT infrastructure becomes more complex with the addition of mobile applications, cloud computing, and new technologies for the Internet of Things (IoT).

How can CISOs possibly keep up? Many are investing in tools and technologies to collect, process, and analyze the increasing amount of internal and external security data. The goal? Use the data to improve real-time situational awareness to help them mitigate risks, detect anomalous behavior, and respond to attacks in progress. This paper concludes that:

- **Organizations are moving toward continuous monitoring.** CISOs realize that the old management saying is true: "You can't manage what you can't measure." From a cybersecurity perspective, this means that they need a real-time perspective of everything that happens on the network. Many firms are implementing tools for continuous monitoring so they can base cybersecurity decisions on data analysis rather than gut instincts alone.
- **Sensitive data remains a blind spot.** While continuous monitoring provides host-based and network telemetry, it provides limited intelligence about sensitive data. For example, continuous monitoring doesn't know which files are sensitive and who should have access to these files. And continuous monitoring tools may not be able to spot anomalous sensitive data access patterns like when a knowledge worker suddenly accesses and copies gigabytes of sensitive data.
- **CISOs need continuous sensitive data monitoring.** To gain greater visibility into sensitive data use and abuse, organizations need the ability to discover and tag sensitive data, monitor sensitive data access and usage, and keep track of data backups and the health of storage devices to preserve sensitive data availability. In this way, organizations can gain better oversight of sensitive data assets to protect them from internal and external cyber-attacks and disastrous data breaches.

Continuous sensitive data monitoring can be complex when applied to thousands of files residing on numerous file servers distributed across the network. DataGravity addresses this complexity with turnkey, data-aware, storage appliances that can help CISOs mitigate risk while streamlining security operations.

The Push Toward Continuous Monitoring

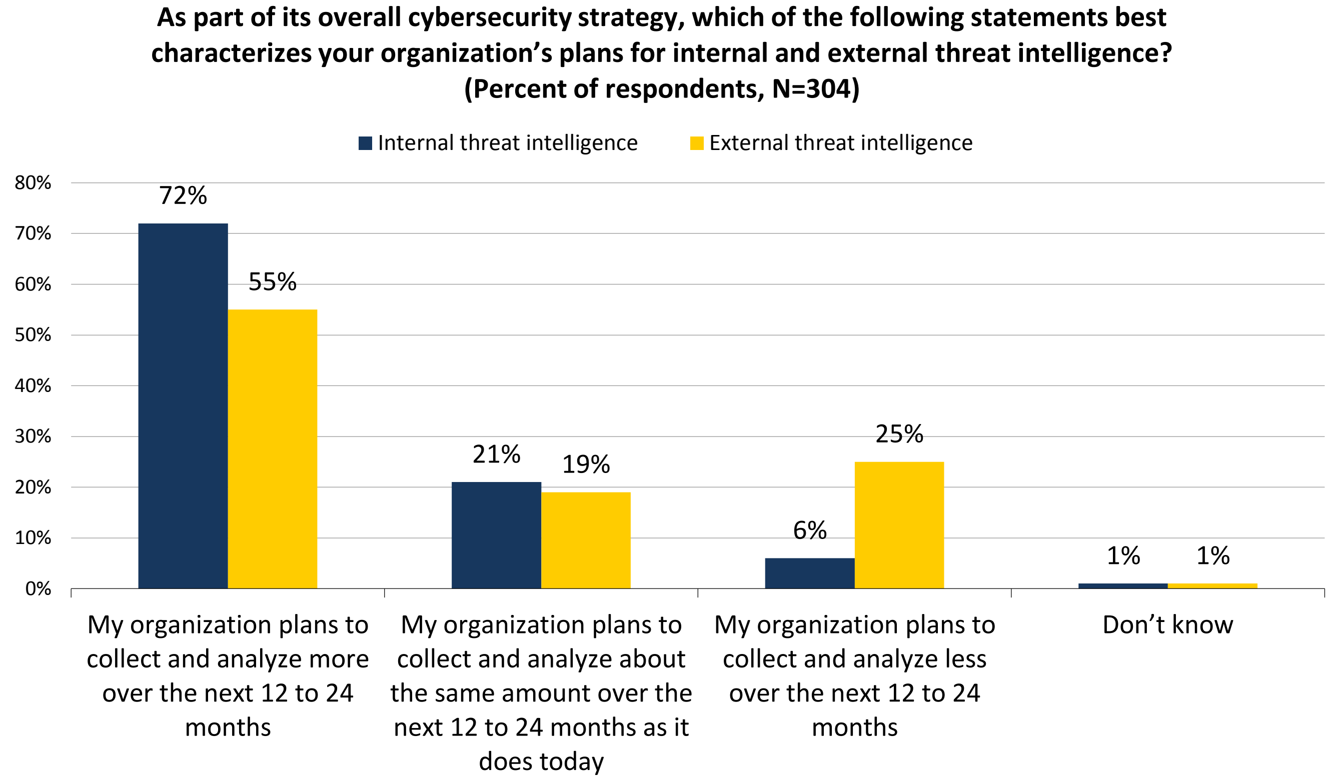
Cybersecurity has often been addressed on an as-needed basis. When new types of attack vectors like advanced persistent threats (APTs), malicious e-mail attachments, and web threats arose, security professionals added gateways and endpoint security software to their existing defenses. While each security countermeasure provided incremental protection, it also created a disjointed and complex cybersecurity infrastructure over time.

Recognizing the shortcomings of this behavior, many CISOs are now engaging in a different cybersecurity strategy based upon comprehensive continuous cybersecurity data collection, processing, and analysis. This approach really mirrors the famous quote attributed to management consultant and author Peter Drucker: "You can't manage what you can't measure." From a cybersecurity perspective, the goal here is to move from reactive to proactive by basing risk management decisions and incident response on real-time intelligence and data analytics. This type of information-driven security strategy has led to rise of:

- **Endpoint profiling tools.** These tools can provide security professionals with detailed information about the devices connected to the network, the configurations of these devices, the applications installed on each system, and the security controls in place. Armed with this information, CISOs can make more informed risk management decisions while the security operations center (SOC) team has additional telemetry for investigations and incident response (IR).

- **Forensic capture and analysis.** In addition to profiling, many organizations are also investing in technologies to capture, process, and analyze endpoint and network forensic data. Security analysts use this information to identify suspicious and/or malicious behavior that may indicate a cyber-attack in progress.
- **Increasing use of internal and external threat intelligence.** CISOs are also increasing their use of a wide assortment of internal and external threat intelligence about threat actors; attacker tactics, techniques, and procedures (TTPs); anomalous employee access patterns; sensitive data monitoring; and indicators of compromise (IoCs). SOC teams use internal and external threat intelligence to establish real-time situational awareness and make analytics-driven decisions for risk management and incident detection and response. ESG research indicates that a majority of CISOs plan to increase the amount of internal (72%) and/or external (55%) threat intelligence data they collect and analyze over the next 12 to 24 months (see Figure 1).[1]

Figure 1. Organizations' Plans for Internal and External Threat Intelligence



Source: Enterprise Strategy Group, 2015.

Organizations Need Continuous Sensitive Data Monitoring

As described, many organizations are collecting, processing, and analyzing an increasing amount of cybersecurity data related to endpoints, networks, and external threats. It is somewhat ironic, however, that continuous monitoring efforts rarely include real-time visibility of sensitive data access and usage. After all, many targeted attacks are intended to culminate in the exfiltration of sensitive information including customer data, financial data, electronic patient health information (ePHI), and intellectual property (IP). Furthermore, insider attacks conducted by credentialed users can have devastating results—think Bradley (i.e., Chelsea) Manning and WikiLeaks (2010) as well as Edward Snowden and the NSA (2013). Comprehensive sensitive data oversight could certainly help improve risk management and accelerate incident detection and response to internal or external cyber-attacks.

[1] Source: ESG Research Report, *Threat Intelligence and Its Role Within Enterprise Cybersecurity Practices*, June 2015.

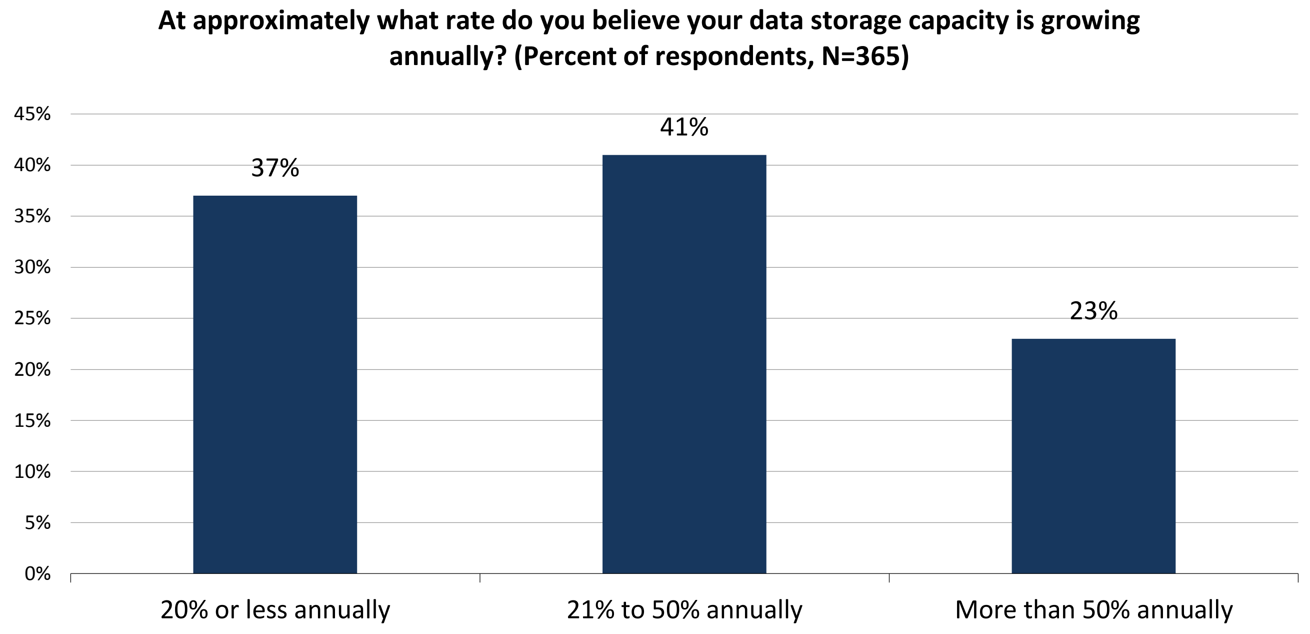
Continuous Sensitive Data Monitoring Defined

The term “sensitive data” has different meanings to different organizations, but as a general rule, sensitive data includes things like customer personally identifiable information (PII), social security numbers, financial information like credit card numbers, regulated data (i.e., sensitive data defined in regulations like the European Union Privacy Directive, FISMA, GLBA, HIPAA/HITECH, PCI-DSS, state regulations, etc.), intellectual property (IP), and any other data deemed as company confidential (i.e., employee data).

Many organizations use a data classification taxonomy or data tagging tools to help them monitor and protect sensitive data assets. For example, the US government typically classifies data into six distinct categories: top secret, secret, confidential, restricted, official, and unclassified. Other organizations find this process too cumbersome and simply divide their data assets into two categories: sensitive and non-sensitive.

Continuous sensitive data monitoring should extend across all types of structured and unstructured data assets. This alone can be difficult given the current state of explosive data and storage growth at many organizations. According to ESG research, nearly one-quarter (23%) of midmarket and enterprise organizations report that data storage capacity increases by more than 50% on an annual basis, so security professionals must have tools and processes that scale to address this massive capacity growth (see Figure 2).[2]

Figure 2. Annual Data Storage Capacity Growth Rate



Source: Enterprise Strategy Group, 2015.

Structured data (i.e., database data) if often managed by a team of DBAs and tends to get more oversight than unstructured data (i.e., files and documents). Given this, many CISOs will want to focus their efforts on the unstructured data residing in an army of insecure file stores across the network.

Once the infosec team identifies all of its file servers, continuous sensitive data monitoring should include (see Table 1):

- **Continuous data scanning for sensitive data discovery.** Many organizations face a fundamental problem in that they don’t know which of their thousands of stored files contain sensitive information or where the copies of these sensitive files actually reside. Given this, the first step toward continuous sensitive data monitoring is data discovery. Security personnel need the tools and capabilities to scan all of their file

[2] Source: ESG Research Study, *2015 General Storage Trends Survey*, conducted in May 2015.

shares, discover the locations of these sensitive data files, and present this information to the security team in comprehensive and intuitive reports.

- **Automated data tagging.** Upon the discovery of sensitive data files, CISOs need the ability to tag these files so they can be tracked over time. Data tagging should be associated with homegrown taxonomies so organizations can use tags for risk management and governance purposes. Furthermore, tagging should be associated with regulatory compliance mandates by tagging specific files containing customer PII, ePHI, credit card information, etc.
- **Tracking sensitive data file lifecycles.** Once sensitive data files are classified and tagged, continuous sensitive data monitoring tools should track file lifecycle activities as file names, locations, content, and backup statuses change. Furthermore, the security team should monitor actual sensitive data file activities such as changes, deletions, downloads, etc. These capabilities are intended to protect sensitive file integrity and availability at all times and in all locations.
- **Mapping between sensitive data assets, user identities, and access patterns.** Once sensitive data files are classified and tagged appropriately, the security team must be able to associate sensitive files with users and groups that access and use the data for business purposes. Mapping sensitive data files to users is essential to the security team for monitoring, assessing, and fine-tuning security policies in order to balance risk with business productivity. Once CISOs understand who has access to sensitive data files, they should move on to gain in-depth visibility regarding data access and usage patterns to detect anomalous and suspicious user behavior. When an administrator suddenly downloads hundreds of sensitive files over a weekend, continuous sensitive data monitoring tools should be instrumented to detect this anomaly and alert the security team immediately.
- **Operational system health monitoring.** Continuous sensitive data monitoring must include real-time visibility into data confidentiality, integrity, and availability across software *and* hardware. This must include the capability to monitor the health of storage devices where sensitive data actually resides. To accomplish this, CISOs need to form a cooperative relationship with the storage operations team to maintain visibility into the health of storage devices as part of their overall sensitive data oversight.
- **Correlation across all aspects of continuous monitoring.** Continuous sensitive data monitoring should be combined with similar activities for monitoring networks, hosts, and applications. For example, continuous sensitive data monitoring telemetry should be correlated with identity analytics, malware detection systems, and network monitoring to provide additional context to anomalous user behavior or the unexpected creation of an IT administrator account. In this way, organizations should be better prepared to mitigate risk and identify threats to their sensitive data assets up and down the entire technology stack.

Armed with real-time visibility of sensitive data files and who is using these files, CISOs can move on to fine-tune business policies and data security controls to maximize sensitive file data protection and accelerate incident detection and response. For example, organizations can:

- **Move sensitive data to hardened file servers**. Once scanning and tagging cycles are completed, the security team can locate sensitive files stored on file servers with minimal security controls and then move them to security-enhanced file servers with more appropriate security defenses and monitoring capabilities.
- **Harden business and security policies**. Business managers may discover that current sensitive data access controls violate the principle of least privileges by providing access to a much larger pool of employees than expected. Once this risk is identified, the security team can modify entitlements and restrict sensitive data file access privileges to a much more limited group of users.
- **Implement data security controls.** Once infosec pros know which files are sensitive and where these files reside, they can then create a strategic plan for data security controls. For example, they can increase the frequency of backup cycles or undertake a phased implementation of storage and file encryption. These controls can greatly improve data confidentiality and integrity.

Table 1. Continuous Sensitive Data Monitoring Highlights

Continuous Sensitive Data Monitoring Activity	Description	Benefit
Continuous data scanning for sensitive data discovery	Provide the security team with an accurate and up-to-date analysis that identifies sensitive file names and locations, along with full forensics on the ownership and activity of those files.	The security team can take appropriate remediation steps such as moving sensitive files to file servers with the appropriate security controls, and alerting the sensitive data owner of a policy violation and subsequent corrective action.
Automated data classification	Scan files to look for sensitive content such as customer data, regulated data, or intellectual property (IP). Apply tags to sensitive files.	Classified and tagged sensitive data files can be tracked throughout their lifecycle. Organizations can also create and enforce security policies for sensitive data files with specific classification tags.
Tracking sensitive data lifecycles	Monitor moves, additions, and other changes associated with sensitive data files.	Protect the confidentiality and integrity of data file versions regardless of their location. Search through backup archives to recover sensitive data that is lost or maliciously altered.
Mapping between sensitive data assets, user identities, and access patterns	Identify which users have access to sensitive files and how they interact with these files.	Security team can monitor data usage and work with business managers to fine-tune business and security policies. Security team can also accelerate the detection of anomalous activities.
Operational system health monitoring	Monitor the health of server and storage hardware. Instrument alerts when logs indicate a potential hardware failure.	Security team can be alerted to an impending problem and take the appropriate actions to preserve sensitive data file availability.
Correlation across all aspects of continuous monitoring	Integrate continuous sensitive data monitoring data with other security operations intelligence and analytics tools.	SOC team has holistic visibility of the organization's security status up and down the technology stack. This can help them mitigate risks and accelerate incident detection and response processes.

Source: Enterprise Strategy Group, 2015.

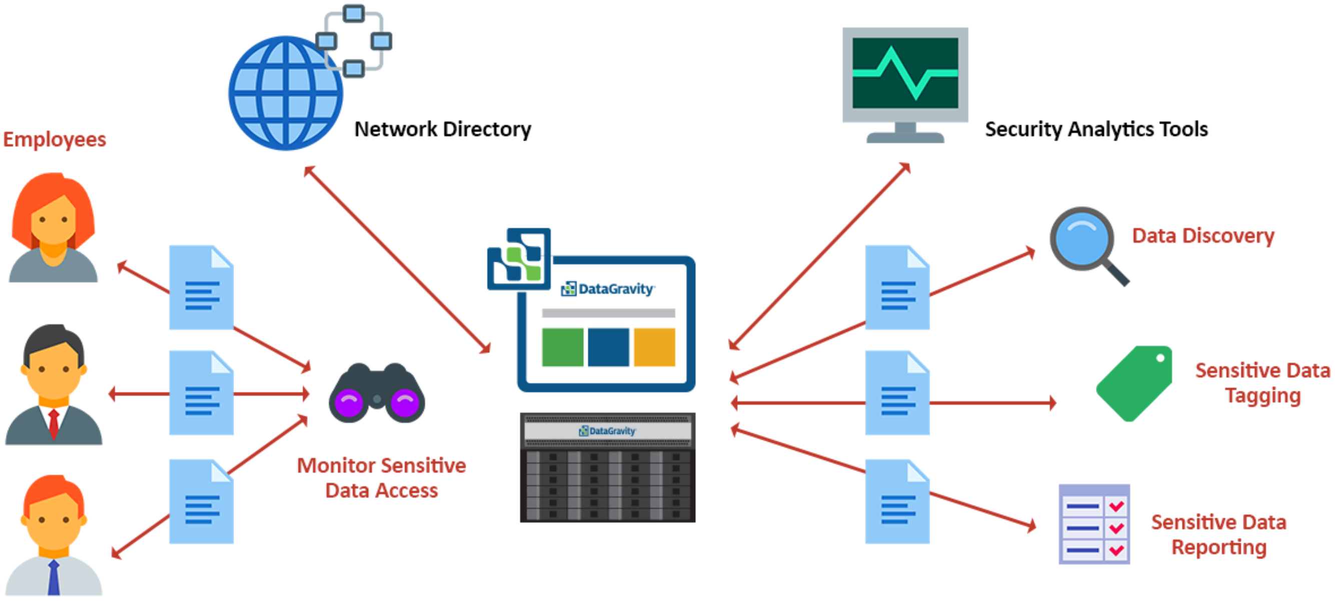
DataGravity and Continuous Sensitive Data Monitoring

Continuous sensitive data monitoring is a critical component of cybersecurity, but organizations are often overwhelmed by the scale and scope involved with the oversight of thousands of potentially sensitive files spread across dozens of file stores throughout the network. In fact, file shares have proliferated across companies for years as repositories for a variety of files from a massive network of stakeholders. These shares tend to be treated as an afterthought when it comes to business continuity as well. This unstructured data can be some of the most valuable information to a business, yet it can be the least inspected when it comes to sensitive data detection, resulting in a large and poorly understood business risk.

While many security administrators seem acutely aware of this problem, many organizations don't have the continuous sensitive data monitoring tools that can readily see what's in the data without the use of numerous, desperate tools. Those who try to mitigate sensitive data security risk tend to address this problem with an army of assorted continuous sensitive data monitoring point tools, but this approach can be expensive and cumbersome to implement, and it lacks the level of granular visibility necessary to enable rapid action on detected anomalous activities.

DataGravity provides an intriguing alternative to the current state of continuous sensitive data monitoring chaos. The company's Discovery Series storage systems are described as "the industry's first data-aware storage platform." From a CISO perspective, DataGravity storage devices can be considered a hardened file server that offers a number of continuous sensitive data monitoring capabilities including the ability to discover, tag, and monitor the use of sensitive data to improve risk management, streamline compliance audits, and accelerate incident detection and the response process.

Figure 3. DataGravity Provides a Turnkey Appliance for Continuous Sensitive Data Monitoring



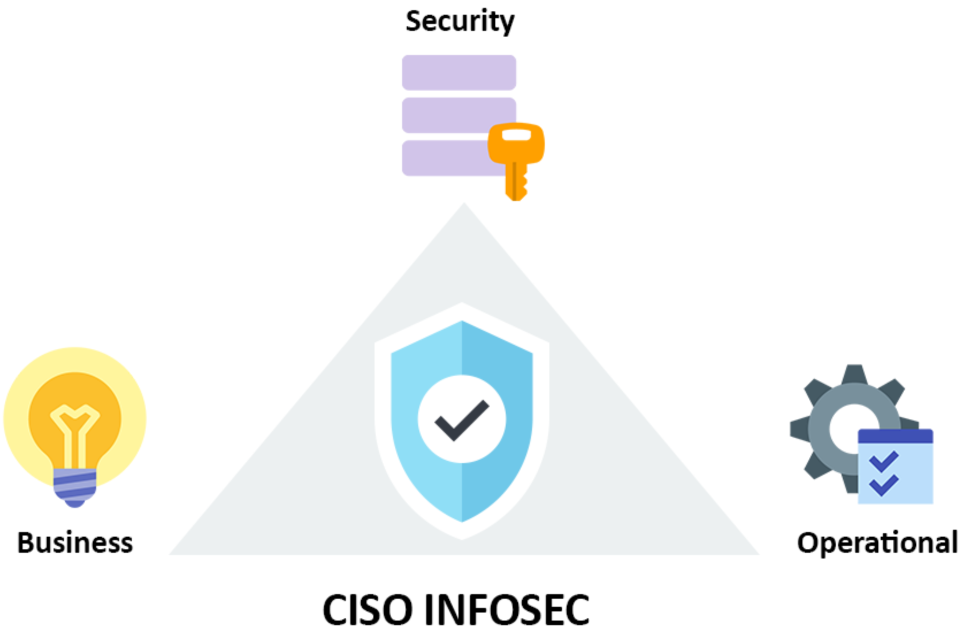
Source: Enterprise Strategy Group, 2015.

Rather than implement numerous continuous sensitive data monitoring tools and technologies, CISOs can deploy DataGravity storage appliances as a turnkey solution. Once files are moved to DataGravity, the security team can then identify, monitor, and protect sensitive data files henceforth while also sharing continuous sensitive data monitoring telemetry with SIEM and security analytics tools to enhance security across the organization. In this way, sensitive data can go from dark and obscure to traceable and actionable. The product is also designed to receive data from other storage systems and monitor that data for the types of information sensitivities that could cause harm if discovered or misplaced. Storage gains a whole new level of intelligence in protecting sensitive data.

In summary, DataGravity can help organizations address the three aspects of the CISO triad (see Figure 2):

1. **Security efficacy.** DataGravity's continuous sensitive data monitoring can help organizations mitigate risk and identify anomalous behavior that could indicate a cyber-attack in progress.
2. **Operational efficiency.** DataGravity centralizes continuous sensitive data monitoring into a turnkey storage appliance. The security team has one system to monitor and manage, streamlining security operations.
3. **Business enablement.** DataGravity can help organizations secure business processes by monitoring access patterns for sensitive data and enforcing the principle of least privilege.

Figure 4. The CISO Triad



Source: Enterprise Strategy Group, 2015.

The Bigger Truth

Cybersecurity can be extremely difficult due to the volume and sophistication of insider and external threats, so CISOs need the right level of situational awareness to assess risks, detect anomalous behavior, and react to cyber-attacks in progress. Staying on top of this demands an unprecedented degree of visibility across the enterprise.

Over the past few years, many organizations have addressed the need for comprehensive visibility with continuous monitoring projects focused on host and network activities. This involved log collection, monitoring network flows, and capturing device and network activities with forensic tools. Yes, these actions are a step in the right direction, but ESG believes that continuous monitoring should also extend to sensitive data—tracking where it resides, who uses it, whether it is backed up and available, etc. Given this situation, this paper highlights several requirements for continuous sensitive data monitoring that should be coordinated with traditional host-based and network continuous monitoring processes and procedures.

With today’s tools, continuous sensitive data monitoring can be difficult—especially when sensitive files are hidden among thousands of others and are stored on an army of file servers distributed across the network. DataGravity offers the capability for continuous sensitive data monitoring as part of the storage array itself, allowing for seamless data monitoring as data is ingested into the storage. Data-aware storage systems are designed to discover, tag, monitor, consolidate, and protect sensitive data files. Since continuous sensitive data monitoring is built into the storage array, this solution allows security staff to monitor sensitive data simply and efficiently, therefore helping to secure the organization’s data from internal and external threats.

Enterprise Strategy Group | **Getting to the bigger truth.**

20 Asylum Street | Milford, MA 01757 | Tel: 508.482.0188 Fax: 508.482.0218 | www.esg-global.com