A Data Centric Approach to Security

Minimize data, reduce business risk

Challenge

- Accumulated data brings risk for both security and compliance. Identifying excess data that does not need to be kept.
- Cloud providers can't ensure removal of all remnants of data. This increases supply chain risk.
- Regulatory compliance (CCPA, GDPR, FISMA) requires the mapping of risks to data elements.
- Lack of a data lifecycle process, continuous monitoring, and minimization introduces risk.

Solution

- Ardent identifies unnecessary data and minimizes it on a continuous basis.
- Ardent disposes of sensitive data securely.
- Ardent searches, discovers, and maps PII data for disposal.
- Ardent continuously monitors excess data.

Outcomes

- Reduce financial liability from excess data.
  Data centric security approach.
- Lower third party vendor risk.
  Enhance cloud data security.
- Automate key compliance tasks.
  Enhance consumer trust.
  Avoid regulatory fines.
- Increase security posture.
  Improve efficiency.

Today organizations collect and retain vast amounts of extensive personal data. Exposure of highly sensitive data presents financial and reputational risks universally understood across business and government. Increasing exposure of data accessed through phishing emails, malware, and ransomware attacks underscores the resolve of threat actors to weaponize private data. Data protection officers and compliance managers need an effective strategy to address these risks and meet privacy regulations. Addressing unauthorized access is only one part of the solution. Reducing available data for access is critical. It is vital to assess critical data assets and design a data centric security architecture to make your organization resilient to common attacks. Implementing effective data minimization and elimination procedures and continuous monitoring is another critical aspect to protecting personal data.

Regulatory Mandates

GDPR[1]

Article 17: Right to be forgotten.
Article 5: Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimization'); The controller shall be responsible for, and be able to demonstrate compliance.
Article 15: Right of access by data subject. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed.

CCPA[2]

Cal. Civ. Code § 1798.110: A consumer shall have the right to request that a business that collects personal information about the consumer disclose to the consumer.
Cal. Civ. Code § 1798.105: Right to deletion. A consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer.

FISMA PRIVACY CONTROLS[3]

DM-1. Minimization of personally identifiable information collection. Locate, remove, redact, anonymize PII.
DM-1. c. Conducts an initial evaluation of PII holdings and establishes and follows a schedule for regularly reviewing those holdings.
DM-2. Data retention and disposal schedule.
DM-3. Minimization of PII used in testing, training, and research.

Ardent Capabilities

- ◉ Discovery & Identification
- ◉ PII mapping
- ◉ Minimization
- ◉ Secure non-recoverable deletion
- ◉ SDLC and data protection in testing environments
- ○ On-Going Monitoring
- ○ Secure Data Life Cycle Management

- ◉ Discovery & Identification
- ◉ PII mapping
- ◉ Minimization
- ◉ Secure non-recoverable deletion
- ○ SDLC and data protection in testing environments
- ○ On-Going Monitoring
- ○ Secure Data Life Cycle Management

- ◉ Discovery & Identification
- ◉ PII mapping
- ◉ Minimization
- ◉ Secure non-recoverable deletion
- ◉ SDLC and data protection in testing environments
- ◉ On-Going Monitoring
- ◉ Secure Data Life Cycle Management

Reduce Risk with Ardent

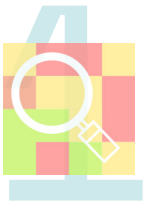
Ardent reduces an organization's risk by minimizing the footprint of data available. Ardent combines machine learning and data analytics to rapidly identify excess personal identifiable information (PII), unused data, and uncover files that are ideal candidates for minimization and/or deletion. Ardent recommends a three-step process to data security:

1. Identify & Map 2. Minimize and 3. Automate compliance.

"We must pass laws that require data minimization, ensuring companies do not keep sensitive data that they no longer need."

- MARK WARNER

US SENATOR & VICE CHAIRMAN OF SENATE INTELLIGENCE



IDENTIFY & MAP

The initial step toward reducing business risk is to complete a data inventory at the file level. Most organizations do not have a comprehensive view of where PII data is located and it can be dispersed across IT teams. Ardent discovers files located across the organization and the machine learning engine analyzes the files to determine which files are candidates for minimization. Essential attributes include: creation, modification, used, bytes, document type and classified by sensitivity. Ardent applies machine learning to categorize risk producing a list of suitable candidate files for permanent disposal. Ardent identifies excess data in seconds, including PII, using metadata of files. Machine learning processes are much faster than traditional methods of content scanning. The results are summarized a heat map of Key Risk Indicators (KRI) of discovered and identified candidates.

MINIMIZE

The second step after data discovery and identification are completed is initiating the remediation process. Remediation options include secure deletion of data, moving data to another location, and archiving it making it off-line. Ardent's software-based deletion solution utilizes DoD compliant algorithms and sanitizes data on an on-going basis and not just at the end of its life. Partial data cleansing is necessary to reduce unwanted data. A record of disposition is available to demonstrate regulatory compliance outlined in FISMA, CCPA and GDPR. Data minimization should be a standard data management practice as it reduces PII exposure and associated financial liability.

Data threat remediation options include deletion and relocation to more secure locations. Ardent uses a software-based deletion process based on algorithms compliant with U.S. Dept. of Defense. Data-at-risk is sanitized beyond end of life tagging. Most importantly, Ardent summarizes document deletions to provide evidence of compliance outlined in FISMA, CCPA and GDPR.

AUTOMATE COMPLIANCE

After initial identification and remediation steps Ardent automates continuous monitoring. Excess data is minimized at regular intervals providing full data lifecycle support. The Ardent scanning process eliminates unwanted data at the end of the SDLC and DevSecOps life cycle thus securing the supply chain. Testing and validation environments benefit by removing often misplaced PII data. Compliance processes are streamlined by automating regularly scheduled scans and remediations.

Ardent: Your Data Security Partner

Ardent is a risk compliance manager's secret weapon in the battle to comply with mandates outlined in GDPR, CCPA and FISMA. CCPA regulation takes effect July 2020 so organizations need to prepare for it immediately. Ardent helps risk compliance managers implement and automate compliance tasks for ease of mind. The 3-phased approach outlined above is based on a data centric security architecture that provides better protection of data and reduces risk. Contact us to discuss how Ardent can enhance your organizations' data security and compliance.

LOWER COST

REDUCE RISK

ENSURE COMPLIANCE

1. https://gdpr.eu/tag/gdpr/
2. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml
3. https://www.cio.noaa.gov/itmanagement/pdfs/Privacy_Control_Allocation_with_NOAA_implementation_statements.pdf

Contact Us
www.ardentsec.com
advisor@ardentsec.com