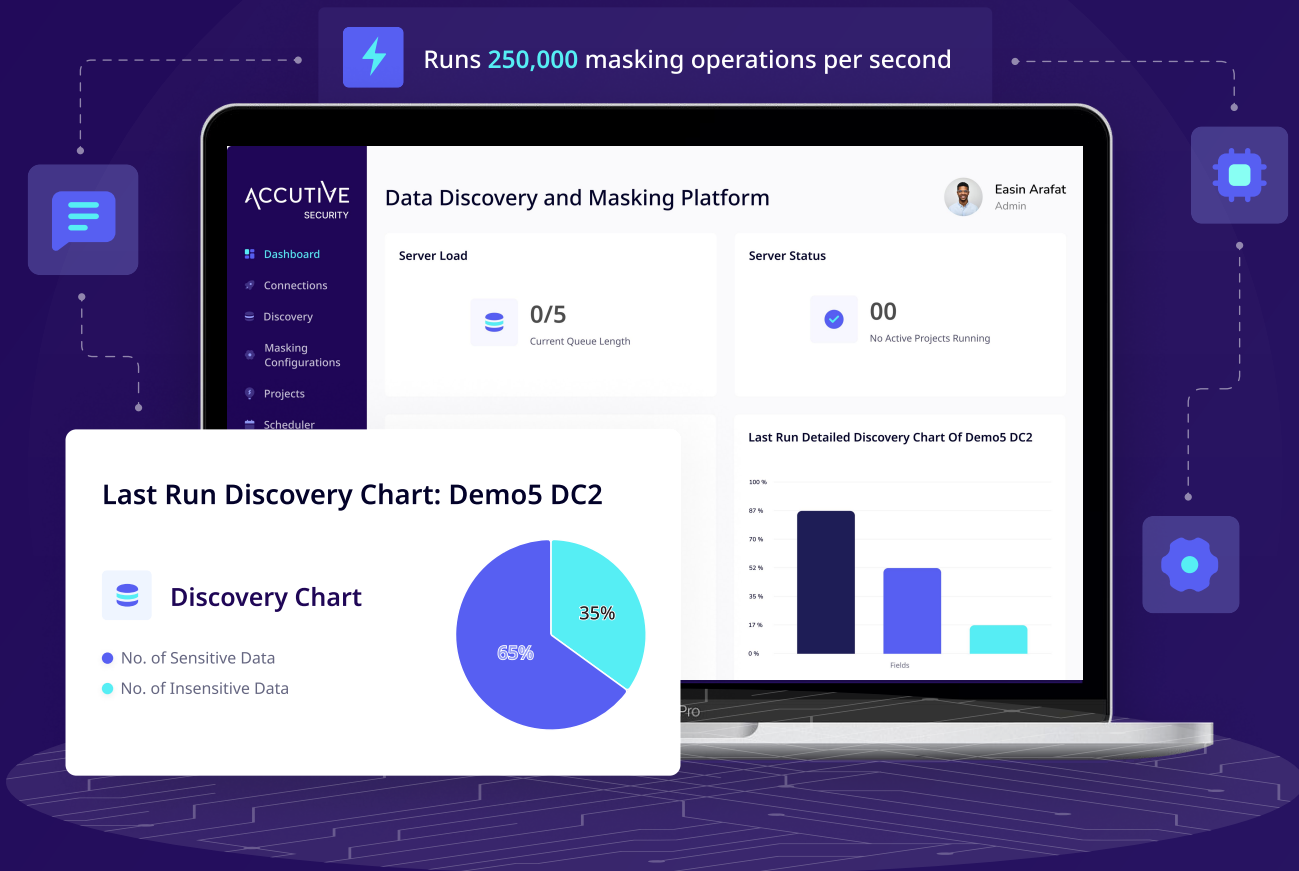


Solution brief

# ADM

## Data Masking Platform

Rapidly generate compliant, anonymized data that mimics production and maintains critical referential integrity








# The problem with discovering and anonymizing PII?

---

With organizations handling vast datasets spread across multiple systems, the need for effective data protection is more critical than ever. Sensitive information like personal and financial data must be safeguarded without interrupting workflows or compromising data usability.

## Common Data Management Challenges

---

-  **Data Discovery Across Diverse Sources:** Discovering sensitive data across Microsoft SQL Server, Oracle, MySQL, PostgreSQL and flat files can be inconsistent and error-prone
-  **Maintaining Referential Integrity:** Ensuring the relationships between datasets remain intact while masking sensitive information is crucial for accurate reporting and testing
-  **Growing Data Demands:** Your DevOps and SecDevOps teams need a constant supply of realistic data for development, testing, and analysis.
-  **Operational Error:** Manual test data generation can compromise the quality of your testing, introducing defects that affect system logic or even break testing environments
-  **Regulatory Compliance:** Manually ensuring compliance with global regulations like GDPR, HIPAA, and PCI-DSS is inefficient and difficult to manage across large environments.

**ACCUTIVE SECURITY**

**Data Discovery and Masking Platform**

Easin Arafat  
Admin

**Server Load**  
0/5  
Current Queue Length

**Server Status**  
00  
No Active Projects Running

**Last Run Discovery Chart: Demo5 DC2**

Discovery Chart

Category	Percentage
No. of Sensitive Data	65%
No. of Insensitive Data	35%

**Last Run Detailed Discovery Chart Of Demo5 DC2**

Field	Percentage
Marked as Sensitive	87%
Scan Field Sensitive	52%
Scan Value Sensitive	17%

**Create Connections**

Connection Name\*

Connection Description

Connection Type\*

Select One

- JSON FILE
- DB2
- MYSQL

Single thread when used as destination

Save

**Run 250,000 masking operations per second!**

# ADM


## Rapid Data Discovery + Masking


Automatically Discover and Anonymize Sensitive Data across large, scattered data sets


ADM is an automated masking platform to simplify and accelerate the discovery and masking of sensitive data across diverse environments. It ensures compliance with regulations like GDPR, HIPAA, CCPA, PCI-DSS and more while maintaining the usability and integrity of masked data for both operational and non-production environments such as testing and development.


# How ADM accelerates DevOps


---


-  **Stop wasting time with manual masking , cut it by 90%**


Manual masking is slow and full of errors. ADM automates the process, reducing masking time by 90% and eliminating mistakes, so you can focus on what matters.
-  **Integrate with multiple data sources with a single tool**


Managing multiple databases is a logistical nightmare. ADM connects to all your data sources—from Oracle to PostgreSQL—so you can manage sensitive data across all systems using just one tool
-  **Preserve data integrity across databases with consistent masking**

Inconsistent masking causes reporting errors and operational headaches. ADM ensures consistent and accurate masking across all systems, preserving data integrity without breaking anything.
-  **Apply compliance-specific masking rules with one-click**

Manually applying complex compliance rules like GDPR and HIPAA takes too much time and effort. ADM's built-in templates apply the right masking rules automatically with just one click
-  **Avoid system slowdowns with pre-scheduled masking**

Running masking during peak hours can kill performance. ADM's auto-scheduler runs jobs during low-load times, so your system stays fast and responsive without disruptions.
-  **Easily discover hidden sensitive data with smart scanners**

Manually finding sensitive data scattered across databases and files wastes time and increases the chance of missing something. ADM automatically discovers and flags all sensitive data, so you never miss a thing
-  **Protect complex data formats without breaking them**

Masking unstructured data like XML and Excel files usually causes errors and breaks file formats. ADM handles these complex formats smoothly, keeping everything intact while securing your data
-  **Stop scrambling for compliance reports with audit trails**

Scrambling to find the right logs for audits is stressful and time-consuming. ADM tracks masking operations in real-time and generates audit-ready logs automatically, so you're always prepared.



## **ADVANCED MASKING FEATURES**

---

Easily handle complex data masking scenarios while preserving data integrity

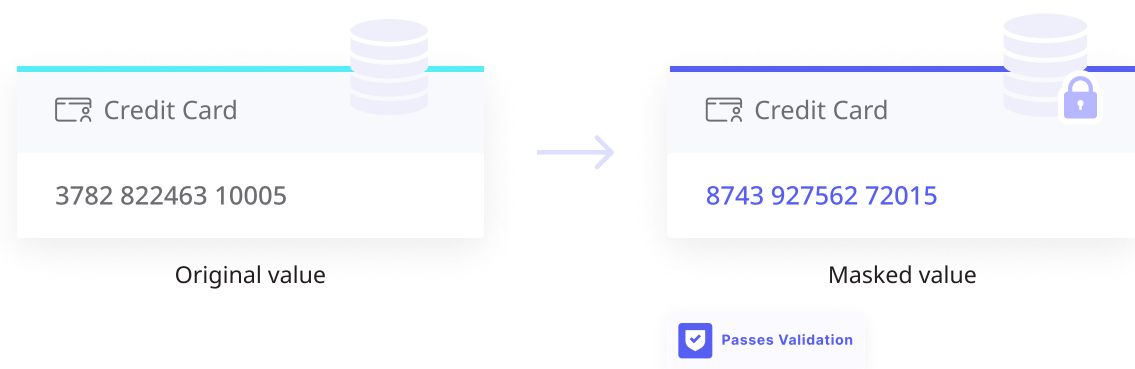
# 01

## Mask Data Without Breaking Your Systems

### SCENARIO 1

You need to mask sensitive data like credit card numbers for testing without disrupting system validation checks.

### FORMAT-PRESERVING MASKING



ADM's format-preserving masking anonymizes values while retaining the original data structure. For example, a masked American Express card number will still follow the 15-digit format, ensuring that system validation works seamlessly without errors.

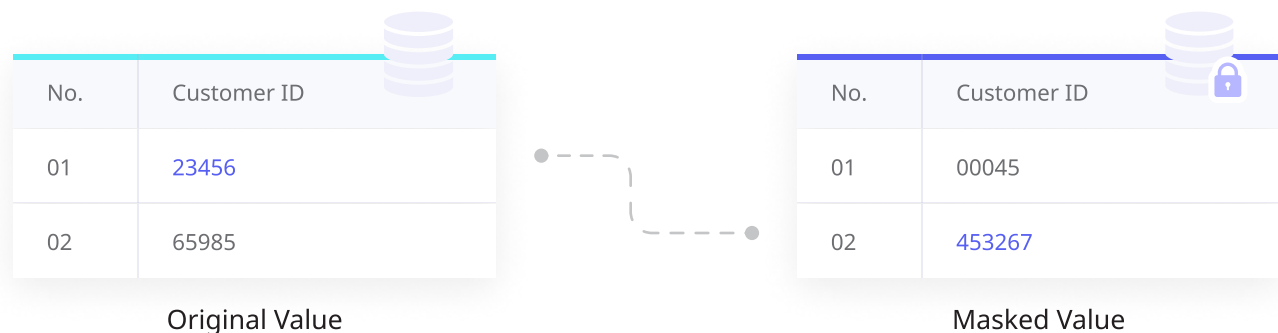
# 02

## Ensure Consistent Masking Across Multiple Systems

### SCENARIO 2

You're dealing with multiple systems that store the same sensitive data, and masking inconsistencies are causing mismatches between them.

### CONSISTENT MASKING ACROSS SYSTEMS



ADM ensures customer IDs, SSNs, or similar data are masked consistently across all databases and applications. For instance, a customer ID masked in the CRM is also consistently masked in the billing system, keeping all systems in sync.

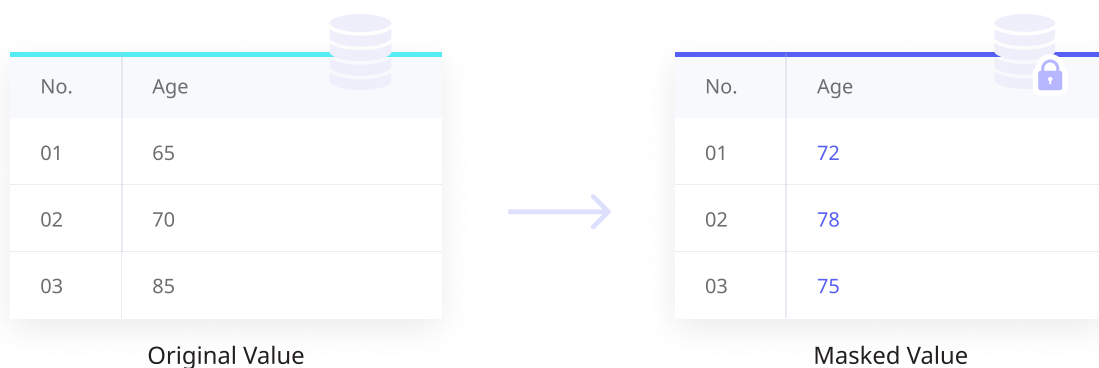
# 03

## Maintain Logical Data Categories for Testing

### SCENARIO 3

You need to anonymize data like age while keeping the logic behind categories intact, such as ensuring senior citizens remain in their age group for testing or analytics purposes

### CATEGORY-PRESERVING MASKING



ADM's category-preserving masking keeps sensitive data anonymized while ensuring it remains within the appropriate logical group. For example, a senior citizen's masked age still falls within the senior category, preserving segmentation accuracy.



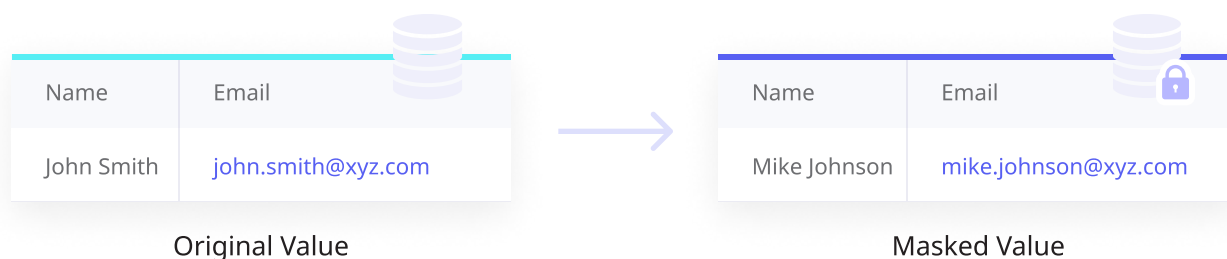
# 04

## Mask Data Without Breaking Relationships

### SCENARIO 4

You're working with interconnected data such as names and email addresses, and masking them separately is breaking relationships between fields.

### COMPOUND MASKING



ADM's compound masking ensures that linked data fields, like names and email addresses, are masked together. For instance, if a customer's name is masked, the corresponding email address is adjusted accordingly, preserving data integrity across all systems

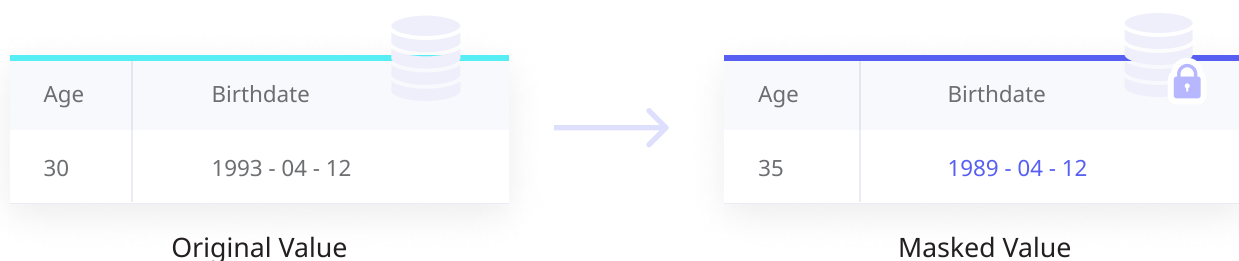
# 05

## Masking Linked Fields Without Losing Data Consistency

### SCENARIO 5

You're masking fields like age, but related fields, such as birth dates, also need to be updated to maintain logical consistency.

### SYNCHRONIZED FIELD MASKING



ADM's synchronized masking ensures that when one field, such as age, is masked, related fields like birthdate are automatically adjusted. For example, if you mask a user's age from 30 to 35, ADM automatically adjusts their birthdate to match, maintaining logical data consistency across all records.

# 06

## Mask Embedded Data Without Breaking Them

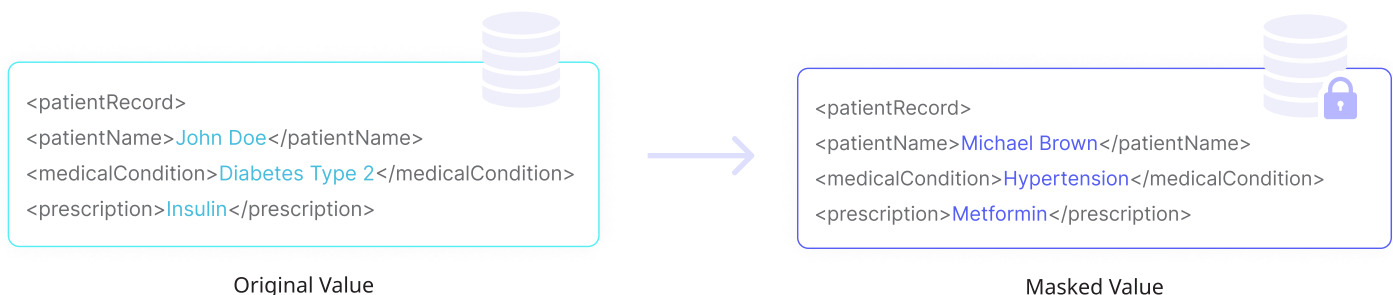
### SCENARIO 6

---

You're working with sensitive data embedded within an XML file, like patient info nested in medical records, and need to mask it without disrupting the file's structure or schema validation.

### SCHEMA-PRESERVING MASKING

---



ADM's schema-preserving XML masking ensures that even deeply embedded data within complex XML structures is securely masked without disrupting the schema or breaking the application logic. This feature maintains the integrity of the hierarchical data relationships, so your XML files remain functional during testing and development

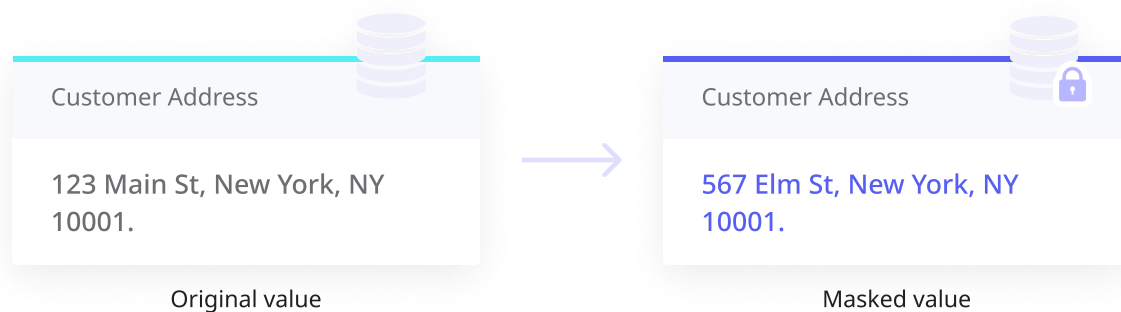
# 07

## Preserve Location Data While Masking

### SCENARIO 7

You need to mask address data but maintain location information for testing purposes

### LOCATION-PRESERVING ADDRESS MASKING



ADM generates masked addresses that preserve key location details, such as postal codes or zip codes. This allows location-based testing or analysis to continue without compromising sensitive address data.

# 08

## Custom Masking Rules for Specific Use Cases

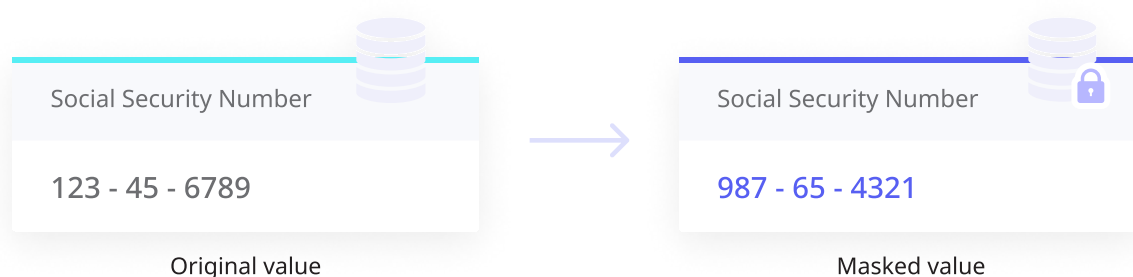
### SCENARIO 8

---

You need to create custom masking rules for specific use cases not covered by standard masking techniques

### CUSTOMIZABLE MASKING

---



ADM allows users to create their own masking logic using groovy (programmable) scripts, giving full control over how sensitive data is anonymized to meet unique testing or business requirements

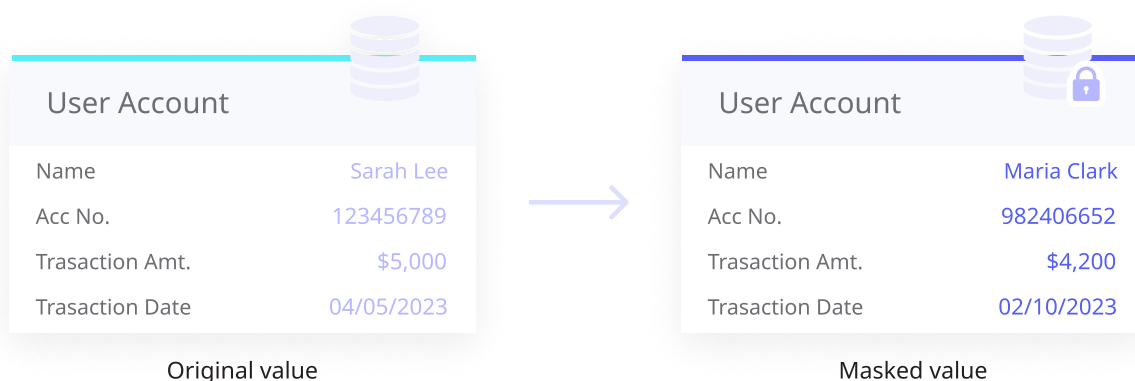
# 09

## Maintain Data Consistency between databases

### SCENARIO 9

You need to mask interconnected fields, such as multiple records tied to a single customer, without breaking the relationships between them

### MULTI-FIELD MASKING



ADM's multi-field masking ensures related fields are masked consistently, preserving logical connections between records. For example, if a name is masked, related fields such as account numbers and transaction histories will be masked in sync.

# Built for Enterprise Compliance

ADM seamlessly integrates into your IT infrastructure to ensure data security and protection



## Multifactor Authentication (MFA)

Integrates seamlessly with MFA solutions to secure access to sensitive environments.



## Role-Based Access Control (RBAC)

Ensures only authorized users can access or configure masking settings.



## Active Directory Integration

Integrates with Microsoft Active Directory for streamlined user management and authentication.



## Tamper-Resistant Secure Logging

It uses blockchain technology to generate tamper-resistant logs for all masking activities



## HSM Integration

Supports Java-standard key stores and KMIP-compatible HSMs for secure key management.



## Audit-Ready Logging

Automatically creates comprehensive logs for all data discovery and masking activities.



## Smart Address Masking

Customizes how addresses are masked (real or fake, original location or altered).



## API-Driven Platform

Seamless integration with Salesforce, MuleSoft, and other platforms for automated data masking.

# Find the Right Plan

Get a 6-month money-back guarantee on all plans, no questions asked

Starter Platform	Professional Platform	Enterprise Platform
<p><b>Core Features</b></p> <ul style="list-style-type: none"> <li>✓ Discovery</li> <li>✓ Masking</li> </ul>	<p><b>Core Features</b></p> <ul style="list-style-type: none"> <li>✓ Everything in Starter</li> <li>✓ Automation</li> </ul>	<p><b>Core Features</b></p> <ul style="list-style-type: none"> <li>✓ Everything in Professional</li> <li>✓ Subsetting</li> <li>✓ Tokenization</li> </ul>
<p><b>Advanced Features</b></p> <ul style="list-style-type: none"> <li>✓ Referential Integrity - In Database</li> <li>✓ AI - Powered Masking Configuration</li> </ul>	<p><b>Advanced Features</b></p> <ul style="list-style-type: none"> <li>✓ Everything in Starter</li> <li>✓ Enterprise wide Referential Integrity</li> <li>✓ Derived Multi-field Masking</li> </ul>	<p><b>Advanced Features</b></p> <ul style="list-style-type: none"> <li>✓ Everything in Professional</li> <li>✓ Programmable Masking</li> <li>✓ Smart Address Masking</li> <li>✓ Proximal Address Generation</li> <li>✓ Synthetic Data Generation</li> </ul>
<p><b>Basic Support</b></p> <ul style="list-style-type: none"> <li>✓ Email</li> </ul>	<p><b>Standard Support</b></p> <ul style="list-style-type: none"> <li>✓ Ticket</li> <li>✓ Telephone</li> <li>✓ Email</li> <li>✓ Live Support</li> <li>✓ 7am to 6pm</li> </ul>	<p><b>Standard Support</b></p> <ul style="list-style-type: none"> <li>✓ 24/7 comprehensive support with immediate access</li> <li>✓ Support Tickets</li> <li>✓ Telephone</li> <li>✓ Email</li> <li>✓ Live Support</li> </ul>



# Take the Next Step

---



**See detailed pricing** to find the right option for your organization.



**Request a demo** with our data security expert to see ADM's capabilities in action.



**Have a specific question?** Write to use at [info@accutive.com](mailto:info@accutive.com)

## About Accutive Security

---

Accutive Security combines deep industry expertise with over 15 years in cybersecurity, focusing on the unique challenges of data protection in sectors like finance and healthcare. This experience has shaped ADM, its flagship data masking and discovery platform, built to handle complex, regulated environments. ADM stands out by automatically identifying and masking sensitive data, ensuring compliance without compromising functionality. It's designed to support the high precision, scalability, and regulatory standards that growing enterprises demand.