



Autonomous AI Driven Data Security Platform

*'The data security capabilities pertaining to zero trust are data discovery and cataloguing, data access management, data encryption and data governance. These are part of the consolidated features offered by DSP'.
Gartner 2023 Strategic Roadmap for Data Security Platform Adoption*



BYTETIME

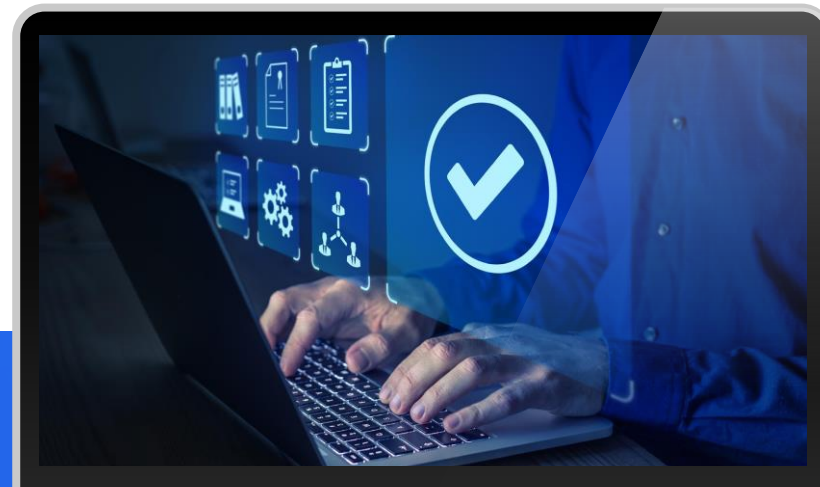
MSSP, TX,
USA
2,500 EPs

**"Thank you for an
Incredible product, plan
to deploy on every
endpoint"**



Why now?

Sensitive data is an exploding concern



Privacy Awareness

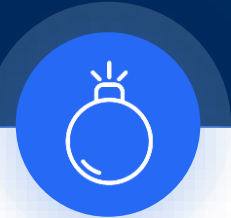


Privacy concerns extend beyond complying with regulations, but also how consumers perceive company brands

Average of \$4.2M data risk per organization, based on 5,000 assessments by our customers.



External and Internal Threats



Ransomware attacks, hybrid work mode and usage of shadow IT by employees continue to challenge businesses of all sizes.

Munich Re experts expect further diversification of extortion methods beyond encryption, continuing the shift from a focus on data for extortion towards exploitable data for sale*



Cyber Insurance



More and more insurance carriers are requiring the measurement of data risk and encryption of all sensitive data, wherever it resides.

Global cyber insurance market has reached a size of US\$ 14bn in 2023 and is estimated by Munich Re to increase to around US\$ 29bn by 2027.*

* <https://www.munichre.com/en/insights/cyber/cyber-insurance-risks-and-trends-2024.html>

Data security is broken

Current solutions are outdated, complex and expensive to maintain



Expertise – Absent



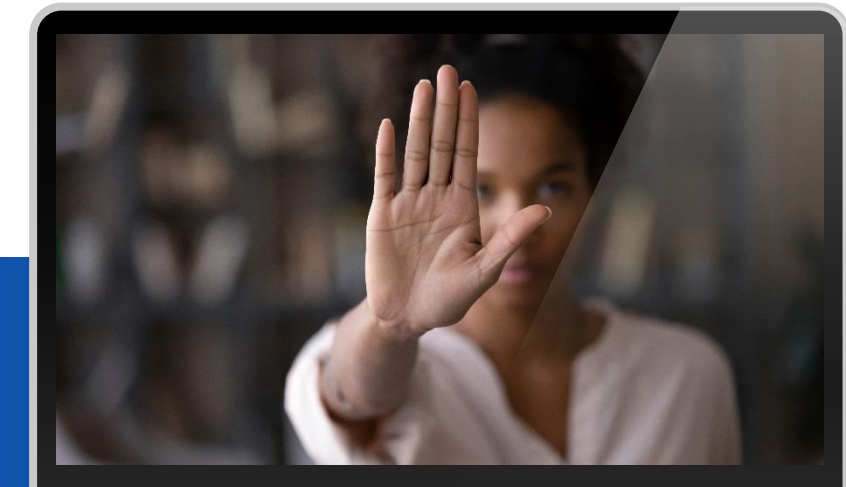
Senior Data Security Experts are critical and hard to find



Time - Intensive



Months long integration and tuning projects, with high ongoing maintenance



Complexity – Drives Cost

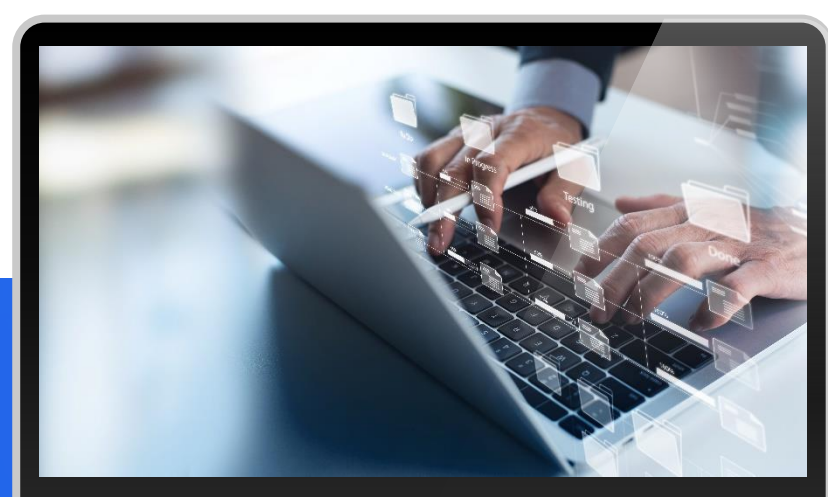


Data is everywhere. Cloud, hybrid, on-premise and hybrid work environments, all contribute to complexity and cost prohibitive

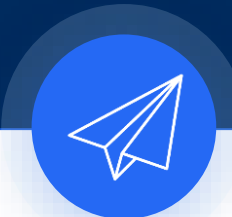


The future is about radical simplicity

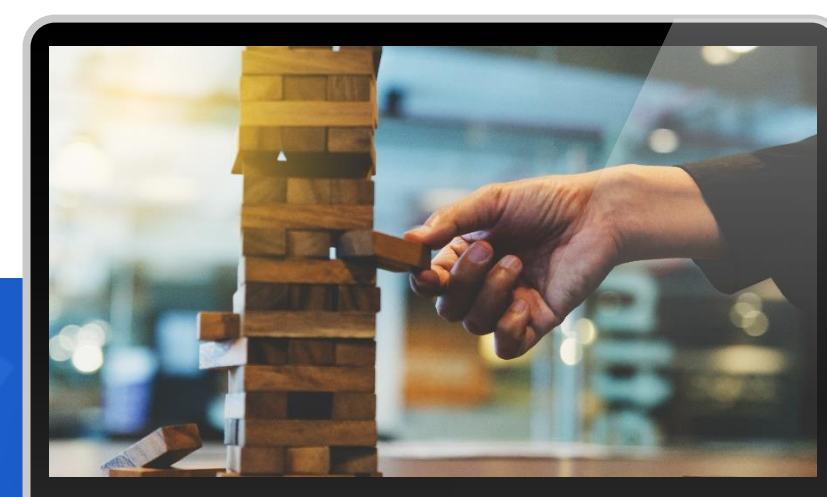
Requiring instant enablement data security solutions



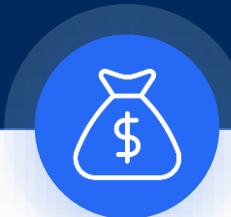
Rapid Deployment



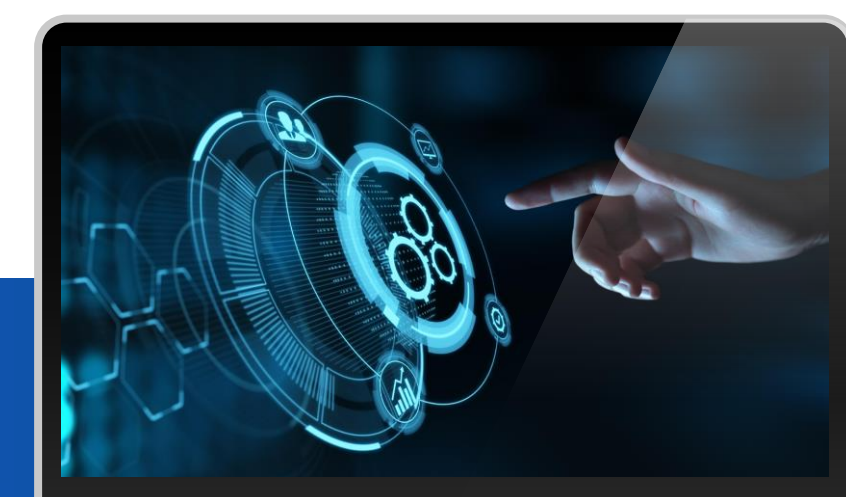
From deployment and discovery in minutes to secured data and compliance in 3 days



Risk Focused



Measuring your deemed data risk monetarily illustrates liability, and facilitating ongoing monitoring and de-risk remediation



Automatic Encrypt/Decryption



One click, preemptive, self automated feature of securing data wherever it is resident and wherever it travels.

Reduce maximum data risk w/o changing how people work



Legacy 'Catch Me' Approach

Method: Analyze each potential leakage event and decide if to block or not



How: Build and maintain blocking rules for each event type



Result: Every event is a decision, time consuming, complicated and prone to security overreach



Data Risk Based Approach

Method: Discover data in near real-time, assess risk per data classification and apply remediation



How: Automated preemptive encryption per data risk classification



Result: Data lifecycle visibility, quick time to ROI, very low maintenance and any data exfiltration is secure.



Classify and Encrypt



Classify files and group by individual classifications

File Content

File Type

File Folder

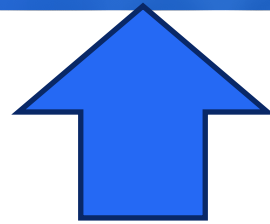


Per classification

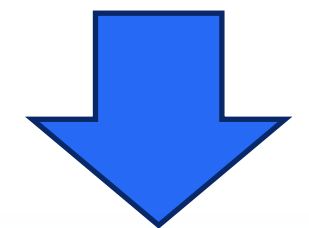
Assess data risk

Continuous Data Risk Assessment

Encrypt Decision



220+ 'Out-of-box' Classifiers/ Classifications



AI Based Classification

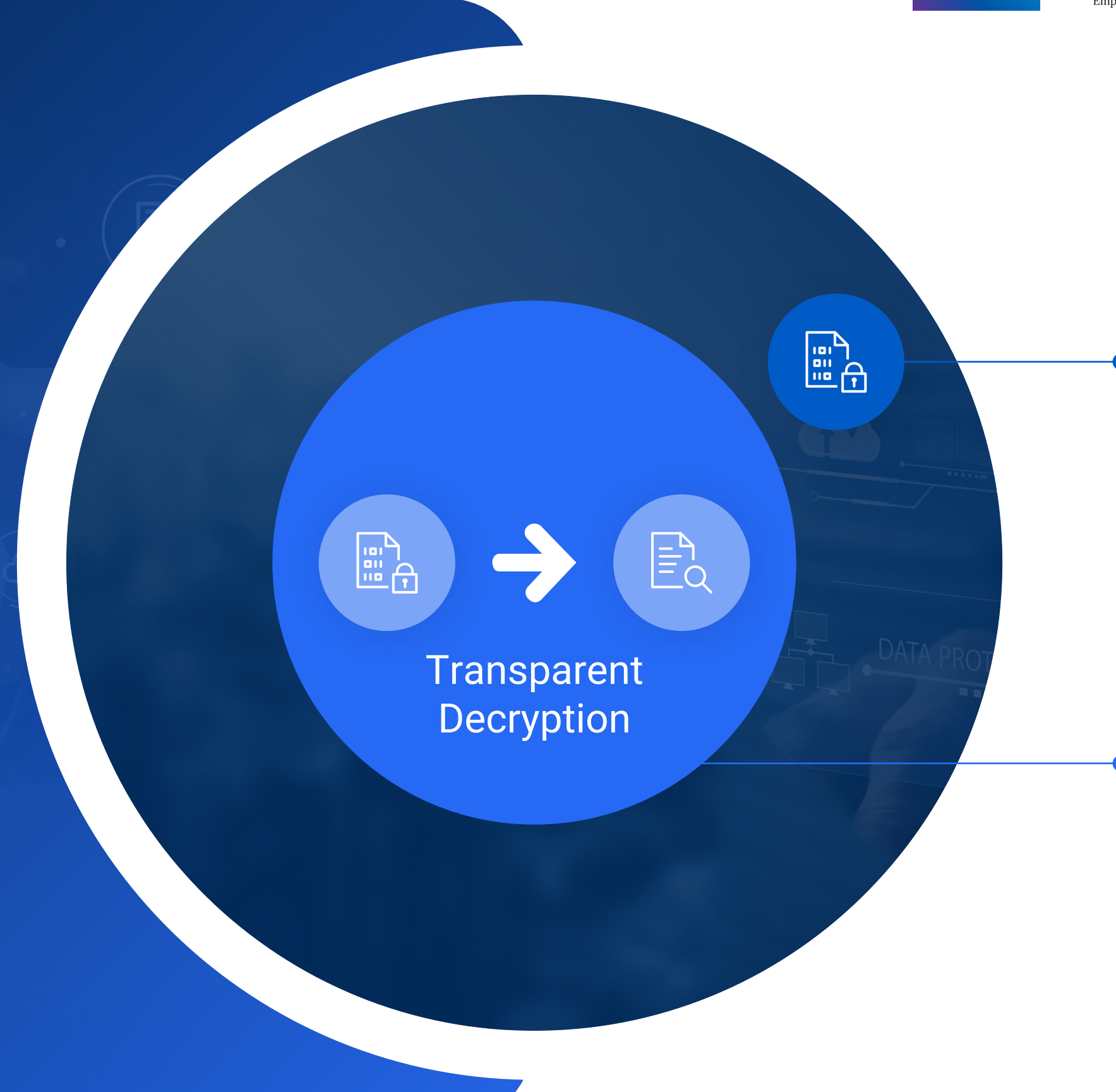
Classifier Template Library



Contextual Encryption

Automated Encrypt/Decryption

Internal data risk
reduced quickly
and efficiently,
with no changes
to how users
work.



Outside the virtual organization, files stayed encrypted and can **not** be accessed

Inside the virtual organization, users **continue** working as usual

Methods for sharing sensitive data externally

Designated per data classification and non mutual exclusive



Option 1:

Decrypt by outgoing channel

Designate an outgoing application to decrypt attached files by default

Risk Impact: Medium



Option 2:

Delayed Encryption

Apply delayed encryption per data risk classification (also next slide)

Risk Impact: Medium



Option 3:

Decrypt per user

Enable specific users to decrypt limited # of files (per classification, audited)

Risk Impact: Low



Option 4:

Use Actifile Application

Provide Actifile to 3rd party users

Risk Impact: Low

Continuous sensitive data auditing

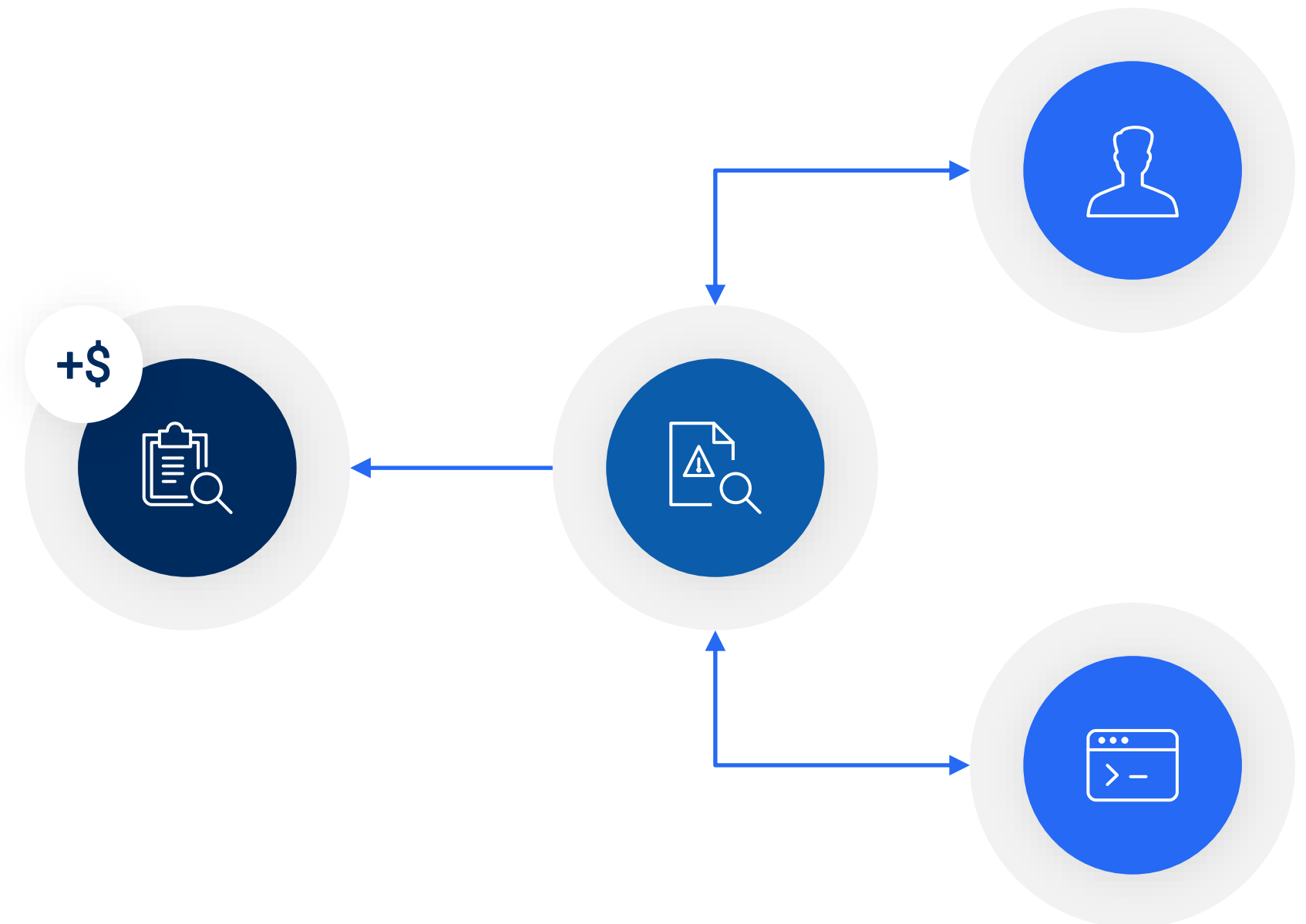
Required for compliance, needed for digital forensics and auditing, helpful to limiting access



Method: Each user, device and application interaction with sensitive data is auditable, enabling specific actions to de-risk the data accordingly



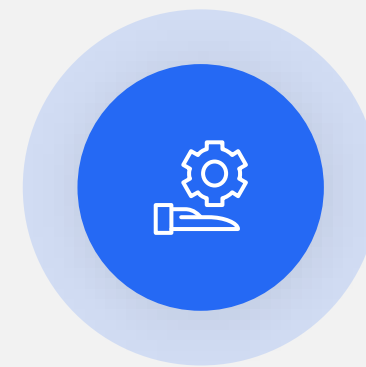
Optional: Whitelist certain applications to decrypt specific sensitive data, allowing current policies to run uninterrupted. No need for blanket policies that lack risk awareness and may inhibit normal operations.



Delayed encryption as data risk reduction method, per data risk classification



Most sensitive files are dormant (at rest) and not used for a long periods, sometimes months or years.



Example:

Files with Automated Clearing House (ACH) sensitive data are out of use and dormant for 1,000 days but are in high use in the first 10 days of their life cycle, sharing with external customers.

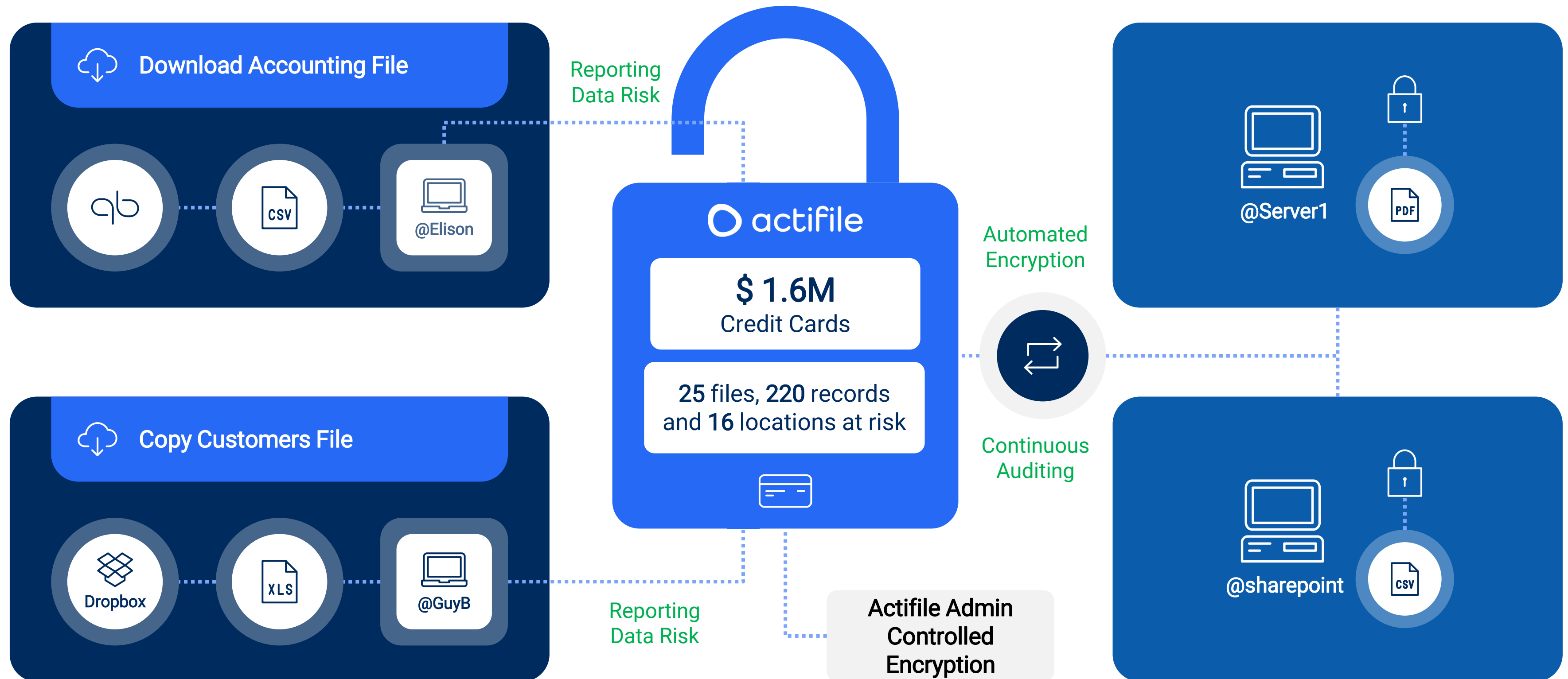


Actifile is set for 10 days delayed encryption
10 Days of out 1,000 Days is 1 %

Result: Actifile will reduce ACH related risk by 99%, without changing how users work, while still available for ongoing auditing.

Actifile in action: high level overview

Across 3 deployment options: endpoints, on prem file repositories, office 365





Solution Differentiators

Current solutions are outdated, and event based. Their overreach impacts operations (thus alienating employees) and are resource heavy to maintain



Risk Focused

Full understanding of data, focus on securing ONLY sensitive data with minimally intrusive controls, avoiding overreach and “alert fatigue”.



Low Cost of False Positives

Automated encryption and transparent decryption dramatically reduces false positives translating into low-impact.



Easy Exceptions Handling


Multiple ways to handle exceptions, white-listing and one-click delayed encryption and right-click decrypt

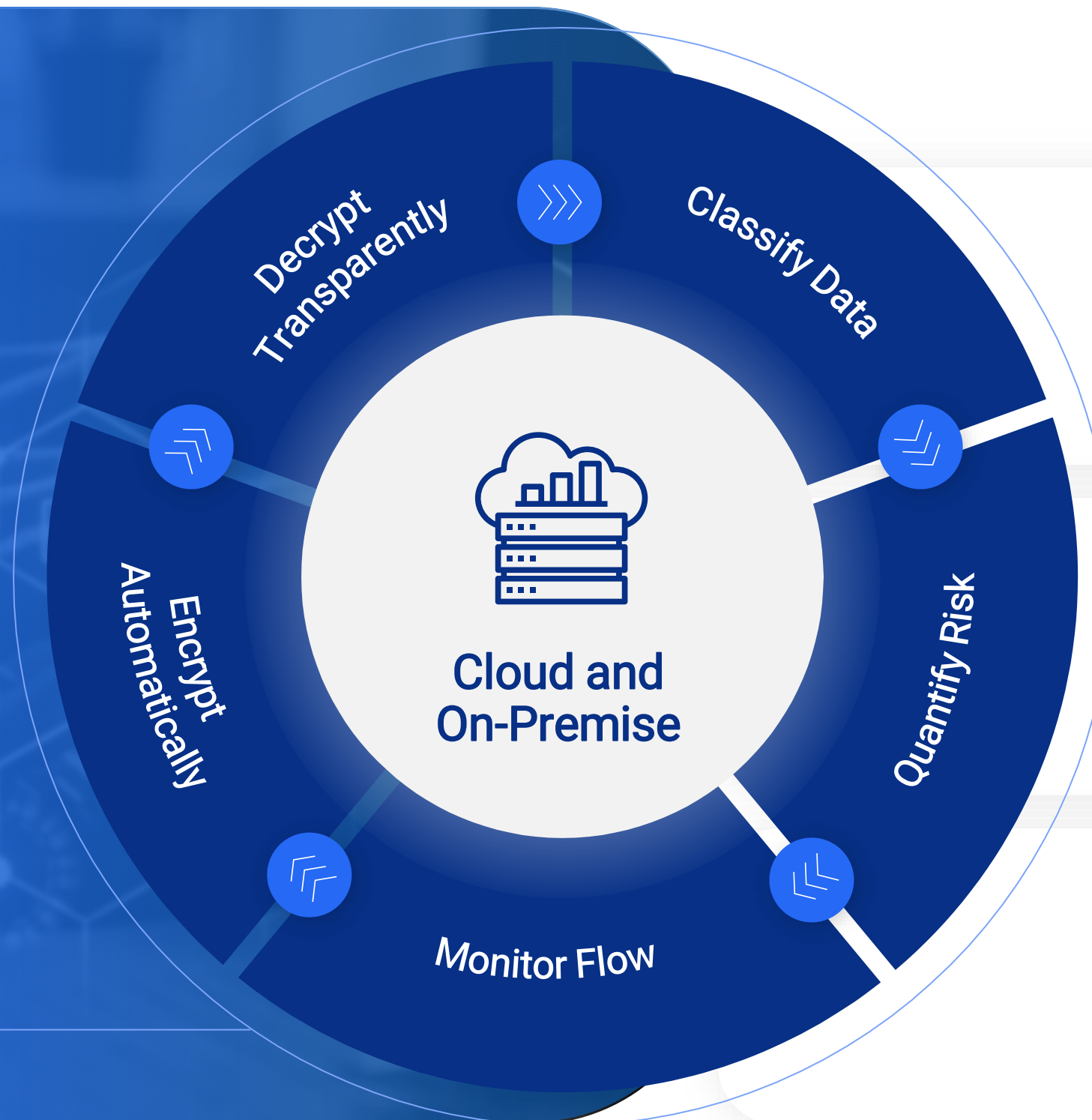


The solution: Actifile Data Security Platform

Immediate discovery, automated security, single pane of glass and ease of management for any IT admin



1

Actifile discovers and monitors all data, identifying all types of sensitive data in real-time.
Display visibility of monetary data risk per device, application, user.



Actifile helps organization's

Prevent data compromise by external (ransomware) and internal threats (insiders) by preemptively encrypting data.



Help establish, maintain and adjust with existing and new industry compliance and privacy regulations.

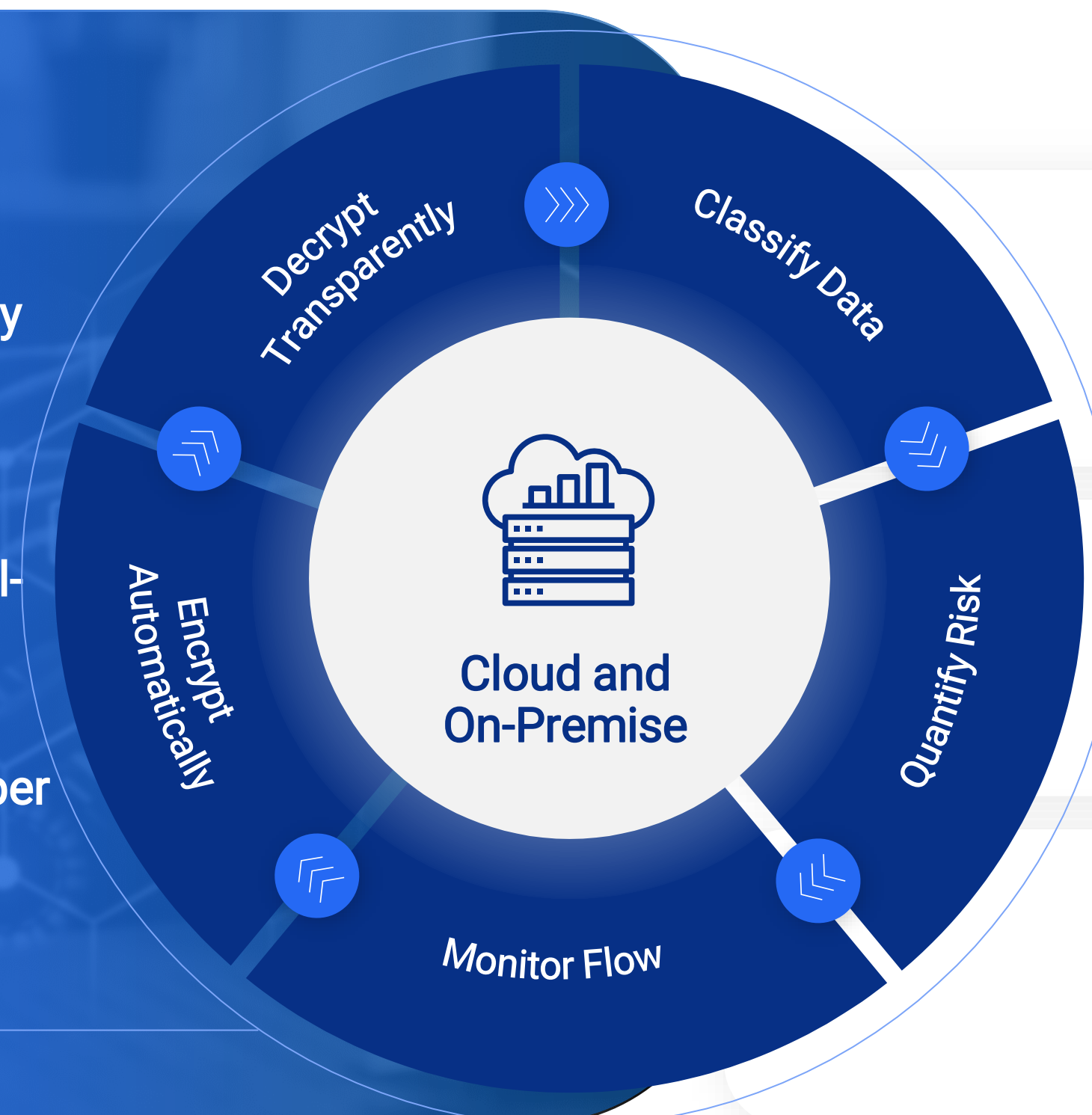


Provides detailed forensics evidence post breach and allows real-time auditing across the entire infrastructure.



The solution: Actifile Data Security Platform

- 1**
- Actifile automatically discovers and monitors all data
 - Classify all types of sensitive data in real-time.
 - Display visibility of monetary data risk per device, application, user.



Actifile – Secure Data Visibility

Prevent data compromise by external (ransomware) and internal threats (insiders) by preemptively encrypting data.



Help establish, maintain and adjust with existing and new industry compliance and privacy regulations.



Provides detailed forensics evidence post breach and allows real-time auditing across the entire infrastructure.





Solution Benefits

Current solutions are outdated and too expensive to maintain



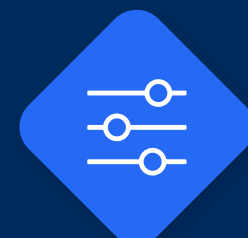
Short time to Value

Our customers deploy Actifile using a cloud based multi-tenant platform in hours and can start securing their customers data immediately



Easy and Intuitive

Most of our customers do not have data analysis and security experience, still they use Actifile efficiently in a matter of days



Set & Forget

Our customers and tell us that Actifile's unique encryption method, secures data without heavy resourcing effort on their side



Thank You



Edward Millington – Managing Director/Principal Security Consultant
edwardm@carisec.global