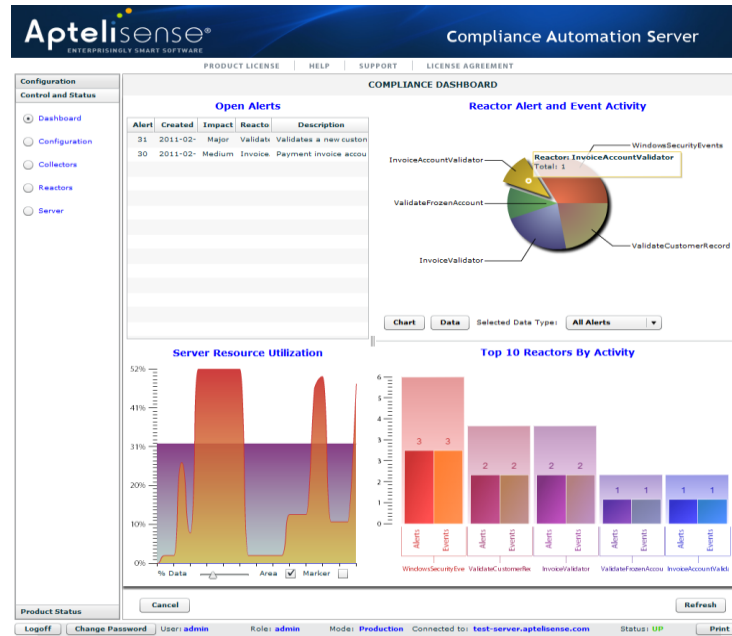


Aptelisense

Expose fraud in live data instantly without adding risk



Compliance Automation Server
for Database Access Monitoring

Administrators have full access

Because of the role that Administrators play, they typically have privileges that can allow them to view or change any data they want. This has always been seen as a position of trust but often highlighted as a risk by auditors which can expose an organisation to:

- Sensitive data being viewed, modified or given to other parties;
- Accidental damage caused by the impact of a wrong action;
- Incorrect configuration causing security exposure.

How can you monitor data access and prevent this risk?

Compliance Automation Server (CAS)

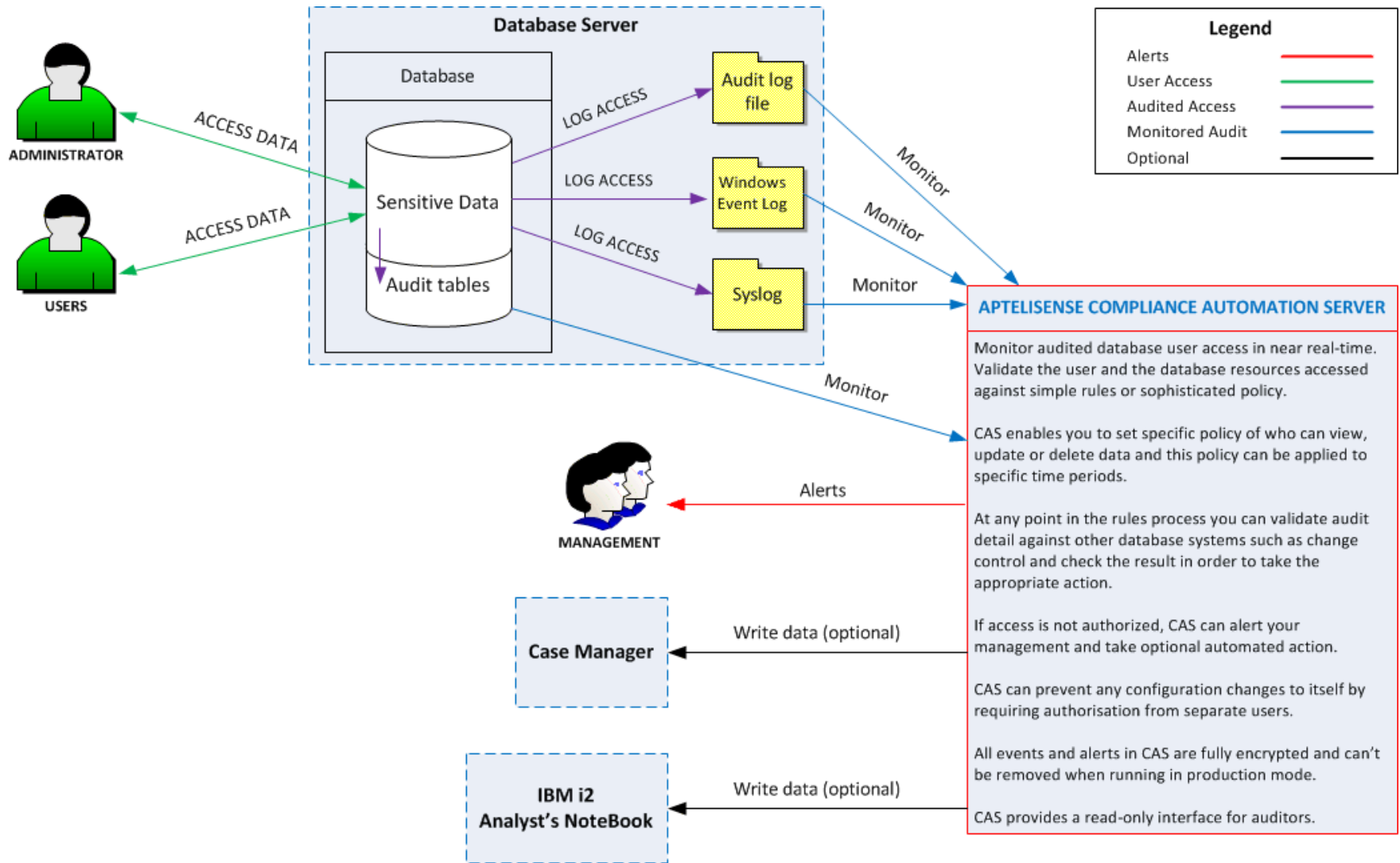
- CAS is an expert Windows Server application
- Enables organizations to monitor and enforce policy thereby ensuring everyone transacting on their systems, whether internal or external, follows and obeys the rules.
- Monitors and validates live data in near real time against business rules autonomously 24/7/365.
- Can be configured to flag or block suspicious transactions.

Database audit monitoring with CAS

Most relational databases have some form of audit functionality which can be used to log access to data and store the detail into a variety of repositories: database tables, file, syslog and Windows Event Log.

CAS can be configured to monitor any of these standard audit repositories in near real-time using simple to configure but powerful rules.

Monitor database access with CAS



CAS benefits

- Data and system agnostic – not tied to any problem area
- Runs in read-only mode by default – no risk
- Does not require programming
- Requires zero system or application changes
- Maintenance free and has a small foot print.
- Fully encrypted and tamper proof
- Has strong authorization control built in to prevent collusion
- Can be switched in to fully reactive mode (dynamic data updating)
- Point and click operation with graphical reporting
- Designed for business users
- Installs in minutes, configured in hours, productive in days

Scalability and cost

- CAS is scalable and can be deployed in many configurable sizes
- Can be networked securely together using CAS to CAS dynamic queries (one CAS can pass data at any point to another CAS for further testing and receive the result).
- Licensing options range up from an individual server in a particular business unit to a full enterprise license
- Licensing and implementation costs are calculated by the number of users, databases, data sources, queries, CAS to CAS connections and rules required for each installation, which is driven by use cases.

Alert response and analysis

Aptelisisense
ENTERPRISINGLY SMART SOFTWARE

Compliance Automation Server

PRODUCT LICENSE | HELP | SUPPORT | LICENSE AGREEMENT

Alerts | Network | Support

Alert	Created	Impact	Reactor	Resent	Prior	Since	Action	Receivers	Status	Updated	Modifier	Description	History
23	2011-08-01	Severe	ValidateE	0	0	0	None	steveauth;	Review	2011-08-01	davido	Purchase order details	[davido : 2011-08-02 16:54:39] This is under review
24	2011-08-01	Medium	ValidateE	0	1	1	None	steveauth;	Investi	2011-08-01	davido	An Employee bank ac	[davido : 2011-08-02 16:55:04] This is under investigation - shouldn't happen
25	2011-08-01	Medium	ValidateE	0	1	1	None	steveauth;	Investi	2011-08-01	davido	An employee phone n	[davido : 2011-08-02 16:55:20] This is also under investigation!
26	2011-08-01	Medium	ValidateE	0	0	1	None	steveauth;	Fixed	2011-08-01	davido	Supplier phone numb	[davido : 2011-08-02 16:57:44] Supplier wife works for us and specified the same num
27	2011-08-01	Medium	ValidateE	0	2	0	None	steveauth;	Suspici	2011-08-01	davido	An Employee bank ac	[davido : 2011-08-02 16:56:43] Case closed - suspicious - employee action taken
28	2011-08-01	Medium	ValidateE	0	1	0	None	steveauth;	Suspici	2011-08-01	davido	Supplier bank account	[davido : 2011-08-02 16:56:57] Case closed - suspicious - employee action taken - lin

AlertID: 23 Created: 2011-08-01 22:52:42
Impact: Severe Prior: 0 Since: 0
Receivers: steveauth;davido Updated: 2011-08-01 22:54:40 By: davido
Description: Purchase order details failed to match any defined suppliers
Response:

Change Alert Status:
 Under REVIEW
 Under INVESTIGATION
 Close as FIXED
 Close as UNKNOWN
 Close as SUSPICIOUS

For a Reactor: Type: Alerts by Status Category: All

Mouse Tips: [Color indicators] Network Zoom: [Slider]
Time Scale: [Slider]

Logoff Change Password User: davido Role: analyst Mode: Test Connected to: test-server.aptelisisense.com

Automatic fraud detection across alerted data

Alerts require response from Authorizer or Analyst users

Aptelisisense
ENTERPRISINGLY SMART SOFTWARE

Compliance Automation Server

PRODUCT LICENSE | HELP | SUPPORT | LICENSE AGREEMENT

Alerts | Network | Support

Network diagram showing connections between various nodes (users, devices, services). Several nodes are highlighted in red, indicating suspicious events.

Alert: 27
Event: 27
Date: 2011-07-07
Time: 18:19:16
Category: Account
Type: Checking
Detail: 400001
(Double click Node to see associated Events)

Mouse Tips: [Color indicators] Network Zoom: [Slider]
Time Scale: 04Jul11 05Jul11 07Jul11 19Jan12

Logoff Change Password User: davido Role: analyst Mode: Test Connected to: test-server.aptelisisense.com Status: UP Print

Suspicious events highlighted in red

Configuration update control

PRODUCT LICENSE | HELP | SUPPORT | LICENSE AGREEMENT

COMPLIANCE SERVER POLICY

Network | Date & Time | License | Proxy | Accounts | Authorization | Alerts

Change Authorization Policy Configuration Panel

Order	Userid	Role	Description
2	madge	authorizer	Authorizer
1	steveh	authorizer	Authorizer
	barryw	authorizer	authorizer.

Minimum number of authorizers: Refresh

Minutes to wait before escalating an authorization:

Which of the following configuration changes require authorization (when running in Production mode):

- User changes: Add Delete Update

- All other changes: Add Delete Update Save

Start Stop Restart Pause Shutdown

NOTE: Authorization requests are sent as a type of Alert using the server configuration values on the Alerts panel.

Can configuration objects be updated while they are in use by other objects:

Yes

NOTE: The default is no. Setting this to 'yes' will allow you to modify (update) objects that are in use but will change the status of the object to non-live. The configuration must be saved to push it back as live. If you require to delete an object which is in use, you will have to remove the dependency first.

Advanced authorisation control over any configuration change

Server Message

Request to stop Collector:
'WindowsSecurityEvents' is currently waiting on authorization ticket: 10

OK

Changes can require authorisation if configured

You can authorise or reject any change before they go live

Ticket: 10 Created: 2011-03-15 02:59:06 Start: End:

Type: EARIP Status: In progress

Requester: steve Updated:

Reason: user: steve is attempting to Stop a Collector object named: WindowsSecurityEvents

Response: There is no change control for this - rejected!

Cancel Authorize Reject Update Selection Criteria: Open Refresh

Simple and intuitive to use

Open Alerts

Alert	Created	Impact	Reactor	Description
25	2011-08-	Medium	ValidateEmployee	An employee phone number matched
24	2011-08-	Medium	ValidateEmployee	An Employee bank account matched a
23	2011-08-	Severe	ValidateEmployee	Purchase order details failed to match

Reactor Alert and Event Activity

ValidateSupplier, ValidatePurchaseOrder, ValidateEmployee

Server Resource Utilization

Top 10 Reactors By Activity

Reactor	Alerts	Events
ValidateEmployee	3	3
ValidateSupplier	2	2
ValidatePurchaseOrder	1	1
ValidateInvoice	0	0
SecurityAccountChanger	0	0

PRODUCT STATUS: User: admin, Role: admin, Mode: Test, Connected to: test-server.aptelisense.com, Status: UP

Simple and clear reporting with easy to understand alerting in real-time.

Alerts Associated with Reactor: ValidateEmployee

Alert	Created	Impact	Resent	Prior	Since	Action	Receivers	Status	Updated	Modifier	Description	Response
24	2011-08-	Medium	0	0	2	None	steveauth;	Investig	2011-08-	davido	An Employee bank ac	
25	2011-08-	Medium	0	1	1	None	steveauth;	Investig	2011-08-	davido	An employee phone r	

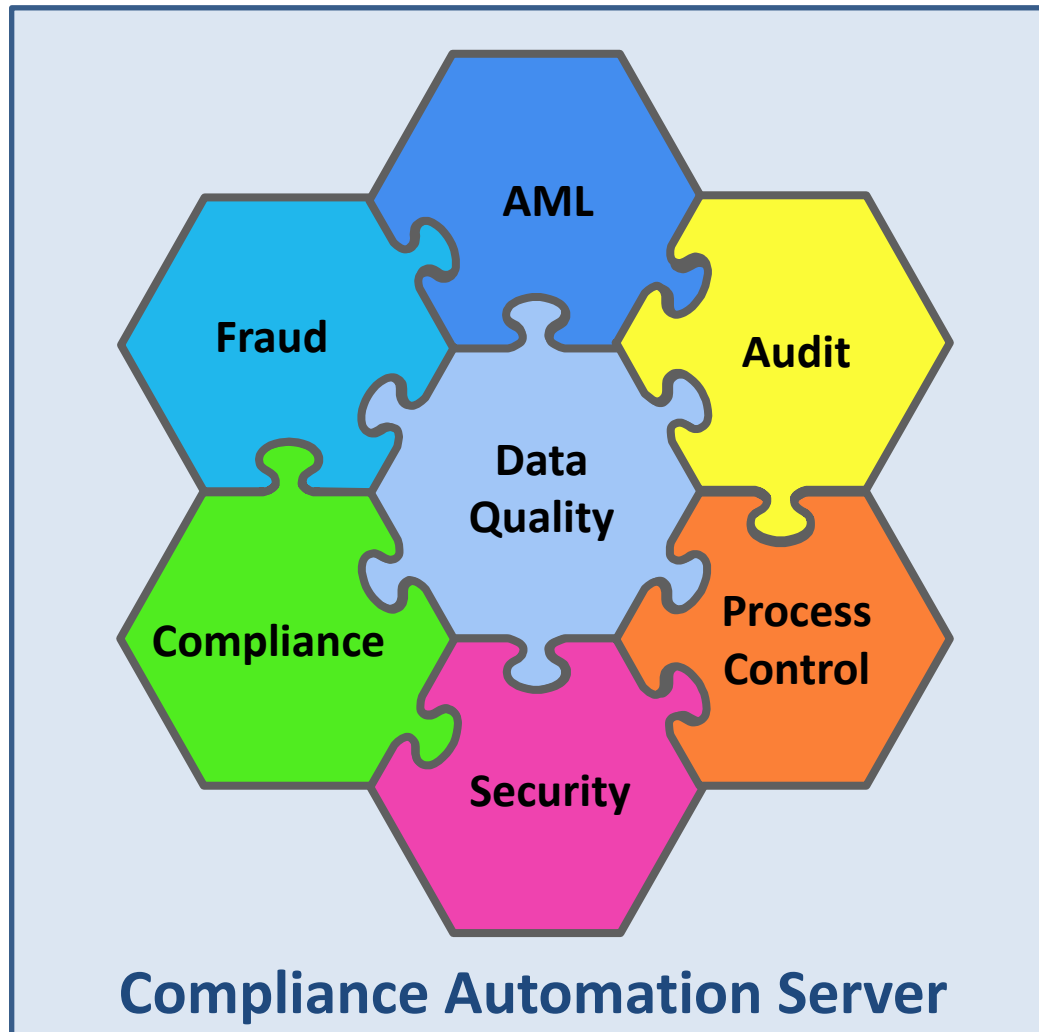
Click to cancel this panel

Every field has optional mouse help tips

The many silos of Risk



CAS monitors risk across all silos



Compliance Automation Server

Expose fraud in live data instantly without adding risk

Installs in minutes, configured
in hours, productive in days

Aptelisense.com

sales.enquiry@aptelisense.com