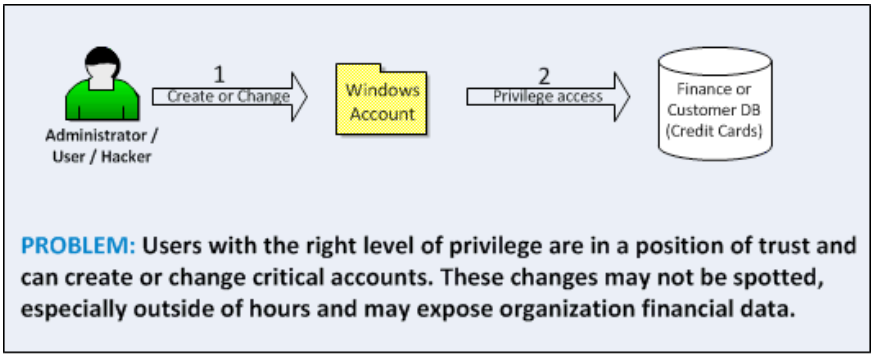
Compliance Automation Server

SECURITY

How do you monitor your administrators?

Many organizations do their best to protect their security with firewalls, Intrusion Prevention and Identity systems but when they get audited they still fail for the same old reason: "The administrators have privileges that allow them to do what they want, when they want and cover their tracks". This is mainly because organizations feel they have to ultimately place all their trust in their staff to do the right thing. How do you police your staff to make sure that they don't make important changes without change control or without the relevant people in your organization being alerted? These changes can be for valid reasons such as during an out of hours call out to prevent an application failing but quite often these changes are not logged or even worse, they may cause problems further down the track.

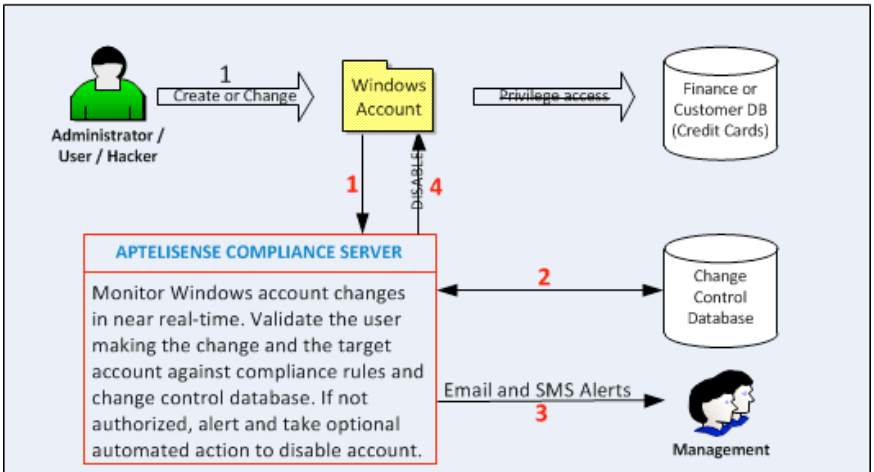


PROBLEM: Users with the right level of privilege are in a position of trust and can create or change critical accounts. These changes may not be spotted, especially outside of hours and may expose organization financial data.

Install Aptelisense Compliance

The answer is simple: Install **Aptelisense Compliance Automation Server (CAS)** to monitor, report and take automatic action when monitored changes break your rules.

A great use of CAS is to monitor all changes to accounts in your Microsoft Active Directory. You can configure CAS with rules that do the following example validation:



SOLUTION: Use Aptelisense Compliance Automation Server to monitor Windows account changes in near real-time. If the change fails compliance rules or is not authorized in change control database, alert management and take optional automatic action to disable account.

- Monitor any account deletion, creation or change
- Alert if the changed account name is one of your critical accounts (domain admin account etc)
- Validate the account name making the change against your change control system and alert if no record was found or the time of the change was invalid
- Alert if changes are taking place out of core business hours
- Take automatic action for the account making the change (run a remote program or script)

Enforce your security policy with near real-time validation

Because CAS can monitor data from many types of source such as: ODBC, log files, Microsoft Event log, LDAP, OPSEC, it has the ability to cross validate any change taking place with a mixture of static rules and dynamic data source validation. It can validate changes against values, date and time periods and dynamically against ODBC data source. This flexibility allows you to write your own form of security policy using the advanced rules that CAS provides.

Advanced security and authorization control

CAS is installed or supplied on its own server and only requires read-only access to your data with no application or system changes required. To increase the separation of duty and security, CAS provides a feature that prevents unauthorized changes to the CAS server configuration. The authorization feature allows you to control which system changes require authorization when the server is running in 'live' mode. If a change is attempted while the system is running in 'live' mode, an authorization alert will be sent to predefined users who can reject or accept the change. If rejected, the change will be automatically backed out, otherwise the change will proceed. All authorization requests are tracked, logged and escalated in the same way compliance alerts are generated.
CAS was designed to be secure and does not trust anyone with its data. It encrypts its configuration and data using a 256 bit algorithm. This means that if someone was to attempt to remove the configuration or data, there would be little risk of the data being legible.

Aptelisense Compliance - one product providing multiple solutions

The advanced features and flexibility of **Aptelisense Compliance Automation Server (CAS)** provide concrete benefits across multiple problem domains, enabling customers to continually increase their return on investment by leveraging the capability of CAS across many business areas but specifically:

Compliance Monitoring

CAS is an independent watchdog that enables you to intelligently monitor, identify, validate, report and take action on changes to your data within your IT systems infrastructure, automatically and 24/7! Designed from the ground up to securely track and store details for reporting via a simple to use web interface, CAS uses your rules to ensure that changes to your data and documents conform to your internal and external requirements. CAS can be configured with simple or complex rules that define what can (and can't) take place. Rules can dynamically validate any data value across one or more systems so you can be sure that the 'who, what, when and where' are monitored automatically, and around the clock!
Installing CAS is quick and easy because it does not require any changes to your systems or applications and requires only read-only remote access to your current data to continually monitor your live data.

Fraud Detection and Prevention

Each year the cost of compliance is increasing. One of the major factors in this cost can be attributed to the additional involvement required by auditors to ensure organizations are not vulnerable to fraud. This cost can be reduced if you can implement automated systems for monitoring and preventing fraud. Another factor of the increased costs is the time it takes for an organization to provide external auditors with the required information and statistics, in a format the auditors understand.
CAS monitors your key systems as an independent watchdog using your rules to ensure that your financial systems do not suffer from unauthorized changes and transactions. CAS can be configured with simple or complex rules that define what can and can't take place. These rules can validate any value or variable across one or more systems so you can be sure that the who, what, when and where are monitored automatically around the clock. When a rule or set of rules triggers an alert, one or more of your key employees will be sent an email or additionally a mobile phone text message. If the alert is not responded to it will be resent using an escalation work flow.

Intelligence

There are lots of choices when it comes to reporting Intelligence. Most organizations use a mash-up of individual products, scripts and spreadsheets. Although no single product can claim to provide a total solution, because CAS is not aligned with any product, it can monitor most of your types of data source in near real-time and alert you when any of your key performance indicators has crossed a boundary.
Using CAS, you can monitor your deliverables to your customer or your suppliers deliverables to you straight from your contract documents. Why not monitor how many units are being shipped (in near real-time) against the number defined in your contract and if the total doesn't match for the previous period, alert you? Why not automatically monitor your stock levels too and receive alerts when certain levels are exceeded? You could do the same with your suppliers!
Use CAS to monitor your customer performance. For example, you can monitor their debt level against their payments and receive alerts when too much debt is accumulating with each invoice or over a certain period.

Security

Many organizations do their best to protect their security with firewalls, Intrusion Prevention and Identity systems but when they get audited they still fail for the same old reason: "The administrators have privileges that allow them to do what they want, when they want and cover their tracks". This is mainly because organizations feel they have to ultimately place all their trust in their staff to do the right thing.
How do you police your staff to make sure that they don't make important changes without change control or without the relevant people in your organization being alerted? These changes can be for valid reasons such as during an out of hours call out to prevent an application failing but quite often these changes are not logged or even worse, they may cause problems further down the track.

The answer is simple: Install CAS to monitor, report and take automatic action when monitored changes break your rules.

A great use of CAS is to monitor all changes to accounts in your Microsoft Active Directory and validate these changes in near real-time against your change control system. If no matching change control record was found or the time was wrong, alert your management and take optional automated action.

Replace your manual monitoring and auditing for fast immediate benefits

One of the greatest benefits of **Aptelisense Compliance Automation Server (CAS)** is to allow your organization to automate your compliance scenarios that used to take one or several staff considerable time. This benefit enables you to move from a reactive mode to a more proactive one, freeing your resources to focus on other priorities.

Reduce your risk without introducing additional risk

CAS is installed or supplied on its own server and only requires read-only access to your data. Because CAS does not require any application or system changes, it does not introduce any risk to your current systems or impact your business insurance. CAS operates on your live data and removes the risk of using old or stale data.

Simple to use and requires no programming skills

CAS has been designed to be simple and easy to use. The target users of CAS are less technical business users who may feel comfortable using Microsoft Excel. CAS removes the need for any programming and provides a simplified configuration interface that hides the normal programming skills that are required when using other tools. Because of this simplicity, CAS can be operated by your business users rather than your IT department. Once your users have been trained, they should be able to develop their own rules without any further help. To further assist your users becoming self sufficient, every field on each of the CAS screens has context sensitive help.

Works with your live data using your rules

CAS operates on your live data and removes the risk of using old or stale data because it does not use copies or historical data. CAS can be configured with simple or complex rules that define what can (and can't) take place. Rules can dynamically validate any data value across one or more systems so you can be sure that the 'who, what, when and where' are monitored automatically, and around the clock!

Provides near real-time monitoring, validation and reporting

One of the main advantages of CAS is its ability to monitor, validate, report and take automated action on changes to your data in near real-time. This means that your staff can move from a reactive mode to a more proactive mode. CAS provides a graphical interface for your users to view alerts and event data in a network map that can highlight unknown and suspicious connections between the data and events that triggered the alerts.

Independent, secure, tamper proof and prevents unauthorized changes and collusion

CAS provides a feature that prevents unauthorized changes to the CAS server configuration. This allows you to control which CAS configuration changes require authorization when the server is running in 'live' mode. If a change is attempted while the system is running in 'live' mode, an authorization alert will be sent to predefined users who can reject or accept the change. If rejected, the change will be automatically backed out, otherwise the change will proceed. All authorization requests are tracked, logged and escalated in the same way compliance alerts are generated. CAS encrypts its configuration and data using a 256 bit algorithm. This means that if someone was to attempt to remove the configuration or data, there would be little risk of the data being legible.

Enables you to monitor and protect areas that were seen as too hard before

Because of its flexibility, CAS can be deployed across many business problem domains (compliance, fraud, intelligence, security etc). This will allow you to extend the reach of CAS, reducing your risk on a continual basis and increasing your return on investment. CAS will enable your organization to audit areas that were previously too hard or involved manually intensive methods. CAS finally enables your organization to solve the "What we don't know" question across many areas.

Protects your brand and reputation and provides assurance to your stakeholders

PWC reported in its 2009 PWC Global Economic Crime survey that the impact of fraud on employee morale, brand, investors, customers and suppliers was considered far more damaging by a third of respondents than the actual cost of the fraud.
Use CAS to provide your organization with assurance that any surprises are not hidden from your management team, stakeholders or external regulatory bodies. This will also protect your reputation and brand.

Reduce your external auditor costs

Each year the cost of compliance is increasing. One of the major factors in this cost can be attributed to the additional involvement required by auditors to ensure organizations are not vulnerable to fraud. Another major factor is the time it takes for an organization to provide external auditors with the required information and statistics, in a format that the auditors understand.
Use CAS to automate monitoring, validation and reporting and provide your external auditors with access to your compliance information and reduce your costs.

Compliance Automation Server

KEY FEATURES

Intelligent data monitoring, validation and reporting

Aptelisense Compliance Automation Server (CAS) provides comprehensive monitoring, validation and reporting of data changes to ensure that your systems are being effectively monitored and managed according to your rules and policies. From an intuitive web interface using context sensitive help, you can monitor and report on simple to complex sequences of data changes. CAS is flexible enough to handle your requirements, such as detecting when database record dates or values change to monitoring sequences of database updates and validating how much was transferred and by whom and taking automatic action. The list of scenarios that CAS can be used for is infinite. CAS is quick and easy to install on a Windows server and also comes with a secure client that provides advanced flexibility, security and reach when monitoring changes and events on remote servers (Windows, Linux, Solaris and HP-UX).

Intuitive web interface with role-based access control

The CAS dashboard has been designed with ease of use in mind. The dashboard displays context sensitive help for most fields (which can be turned off) so you will rely less on the documentation and be able to spend more time on what matters to you. User access to the dashboard is tightly controlled by role-based access. It also offers separation of duty by controlling what functions can be performed by the different system roles.

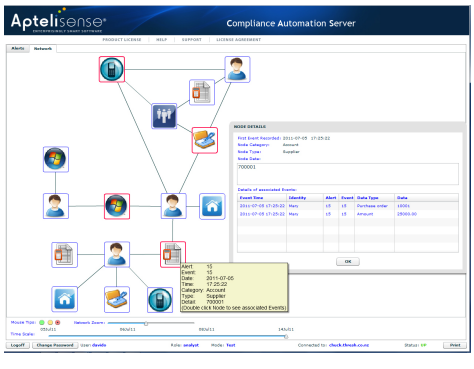
CAS has all the usual security features you would expect, such as account lockout, password aging and ensures that only one administrator user can make changes at a time while allowing others to log in using read only mode.

Secure configuration change authorization control

To increase the separation of duty and security, CAS provides a feature that prevents unauthorized changes to the CAS server configuration. This authorization feature allows you to control which CAS configuration changes require authorization when the server is running in 'live' mode. If a change is attempted while the system is running in 'live' mode, an authorization alert will be sent to predefined users who can decline or accept the change. If declined, the change will be automatically backed out, otherwise the change will proceed. All authorization requests are securely tracked, logged and escalated in the same way compliance alerts are managed.

Advanced correlation and visual analysis

CAS automatically monitors your data using your rules and alerts you when you need to know something is wrong. CAS also provides an advanced feature that automatically analyzes associations and connections across alerts and the data that triggered the alerts. The CAS analyst Workbench interface will allow your users to display these suspicious associations and connections on a network map. The network map clearly highlights suspicious connections in red and allows analysts to visually drill down to the important data using the mouse. Because CAS operates in near real-time, your organization can move from reacting to historical data to proactively responding to instant information.



Automated action and response

CAS enables you to take an automatic action when a condition fails your compliance rules. This is achieved by installing one of the Aptelisense Pro secure clients on your target server(s) and configuring CAS to run a script, program or command file on the target system using the secure client. This will allow you to fully automate responses to serious conditions which require instant action to be taken. This is especially useful when dealing with situations outside of normal office hours where the appropriate staff may not be available to take action. An action could be as simple as running a report, blocking an account, flagging a database record or shutting down a server.