precisely

Customer Case Study:
US food processing company

Critical Issue

Any company involved in food processing, packaging and distribution knows that the purity and safety of its products cannot be compromised. Beyond the extremely high costs of recalls, regulatory fines and potential litigation, the greatest cost of any failure to maintain absolute food safety is the loss of their most valuable asset – customer trust.

So, it is no surprise that food manufacturers must focus intensely on controlling every aspect of their production operations and must be able to prove compliance through a myriad of procedural documents, inspection logs, and lot control and logistics records.

For this food processing company's highly-automated operations, that focus must extend to how they manage the safety and security of their information systems and data. The company responded immediately when they recognized a vulnerability in the control of internal access to its core IBM i systems and data.

Results

- Control of internal and external access to systems and data via detailed exit point monitoring. Over 30 IBM i commands and more than 25 exit points are now continuously monitored, and access events are logged.
- Real-time email alerts for all rejected attempts to access the IBM i system through means such as FTP or Client Access (ACS) file transfer.
- Explicit user permissions (role security via group profiles) are required for any ODBC access.
- Greater visibility into IBM i security via logs, alerts (emails/texts) and reports generated for key QAUDJRN events.

Company Name

US food processing company

Industry:

Produce processing and distribution

Business Environment:

Deeply integrated farm-to-table operations

Highly regulated production and distribution processes

Customer Base:

Major food retailers, restaurants and institutional food services globally

Precisely Product:

Assure Security

> "Some folks slip into the mindset that their IBM i systems are naturally protected through 'Security by Obscurity.' But it is just not true. In fact, such thinking is probably the single greatest threat to IBM i security you can have."
>
> – Software Development Manager,
> US food processing company

Copyright ©2020 Precisely. All rights reserved worldwide. All other company and product names used herein may be the trademarks of their respective companies.

Technologies

- Assure System Access Control
- Assure Monitoring and Reporting

Business Challenge

With quality and operational efficiency being the key drivers of its global success, the company maintains tight control over every link in its products' farm-to-table chain. Intense involvement with their grower partners includes strict oversight of organic farming practices as well as harvesting and transport procedures. All manufacturing facilities are certified SQF Level 3, USDA Organic, OU Kosher, Allergen Free and NON-GMO Project Verified.

Key parts of its business run on IBM i servers, including ERP systems, BI/reporting and analytics, and agriculture management applications. Highly automated processing and packaging operations are also driven by numerous in-house developed applications and methods.

Because of its total dependency on advanced IT for both production and business operations, the company must maintain the highest possible levels of systems and data security.

Not long after joining the company, the company's Software Development Manager conducted a full review of its IBM i systems, with special focus on security issues. What he found caused him serious concern.

"It did not take long to determine that, while our IBM i systems and data were basically well secured against hacking and other threats from outside the company, the level of exposure to potential threats from the inside was not acceptable."

His greatest immediate concern was that IBM i exit points were not effectively secured against being used as "entry points" into IBM i applications and systems. This vulnerability meant that anyone with more than the lowest levels of assigned access authority could, with the right knowledge and a little effort, compromise the system and even gain All Object (*ALLOBJ) authority, enabling them to alter database files or change, remove or grant object control to other users.

At the next meeting on IBM i security he brought up his concerns, but many in the room were skeptical that securing IBM i exit points was necessary.

"To prove my point, I went 'White Hat' while they watched, going into the system with lower level authorization. By leveraging exit points, within five minutes I had *ALLOBJ authority. I then proceeded to make a few tiny changes to the system. Suddenly, printers all over the building stopped working, and all the time clocks in the production plants went offline. At that moment exit point security went to the top of the list."

Solution

To address the IBM i security issues, the company implemented the exit point control and security monitoring features of Assure Security.

It first addressed internal access controls with Assure System Access Manager, locking down over 25 exit points and 30 IBM i commands. In addition to continuous monitoring and logging of access attempts with Assure System Access Manager, it implemented Assure Monitoring and Reporting for real-time alerts and reports on critical security events, including rejected access attempts, such as Client Access or FTP attempts, and key QUADJRN events.

The deep visibility that Assure Security provides into the company's IBM i systems also enables it to more effectively review and standardize all IBM i operations across their multiple plants and logistics operations.

"Over time, we have acquired other food processing companies. Going on site and grilling the recently-acquired IT team about how they have managed their systems is naturally stressful, both for them and for me," the Software Development Manager explains. "Assure Security has made the critical task of assessing how they have been handling IBM i access control much quicker, more thorough, and much, much less confrontational."

Next Steps

The company knows that security and compliance is a continuing process. In addition to locking down additional exit points, it is considering expanding its use of Assure Security to refine its security stance to one based on the principle of "least privilege." It is also considering Assure Security's multi-factor authentication capabilities for all higher-level internal access requests involving *ALLOBJ service accounts, such as QSECOFR.

Whenever he can, the Software Development Manager offers a sage bit of advice to his fellow IBM i professionals. "Because the IBM i platform is not as pervasive across IT shops as are Windows or other open source platforms, some folks slip into the mindset that their IBM i systems are naturally protected through 'Security by Obscurity.' But it is just not true. In fact, such thinking is probably the single greatest threat to IBM i security you can have."

> "So to prove my point, I went 'White Hat' while they watched, going into the system with lower level authorization. By leveraging exit points, within five minutes I had *ALLOBJ authority."
>
> – Software Development Manager,
> US food processing company

Copyright ©2020 Precisely. All rights reserved worldwide. All other company and product names used herein may be the trademarks of their respective companies.