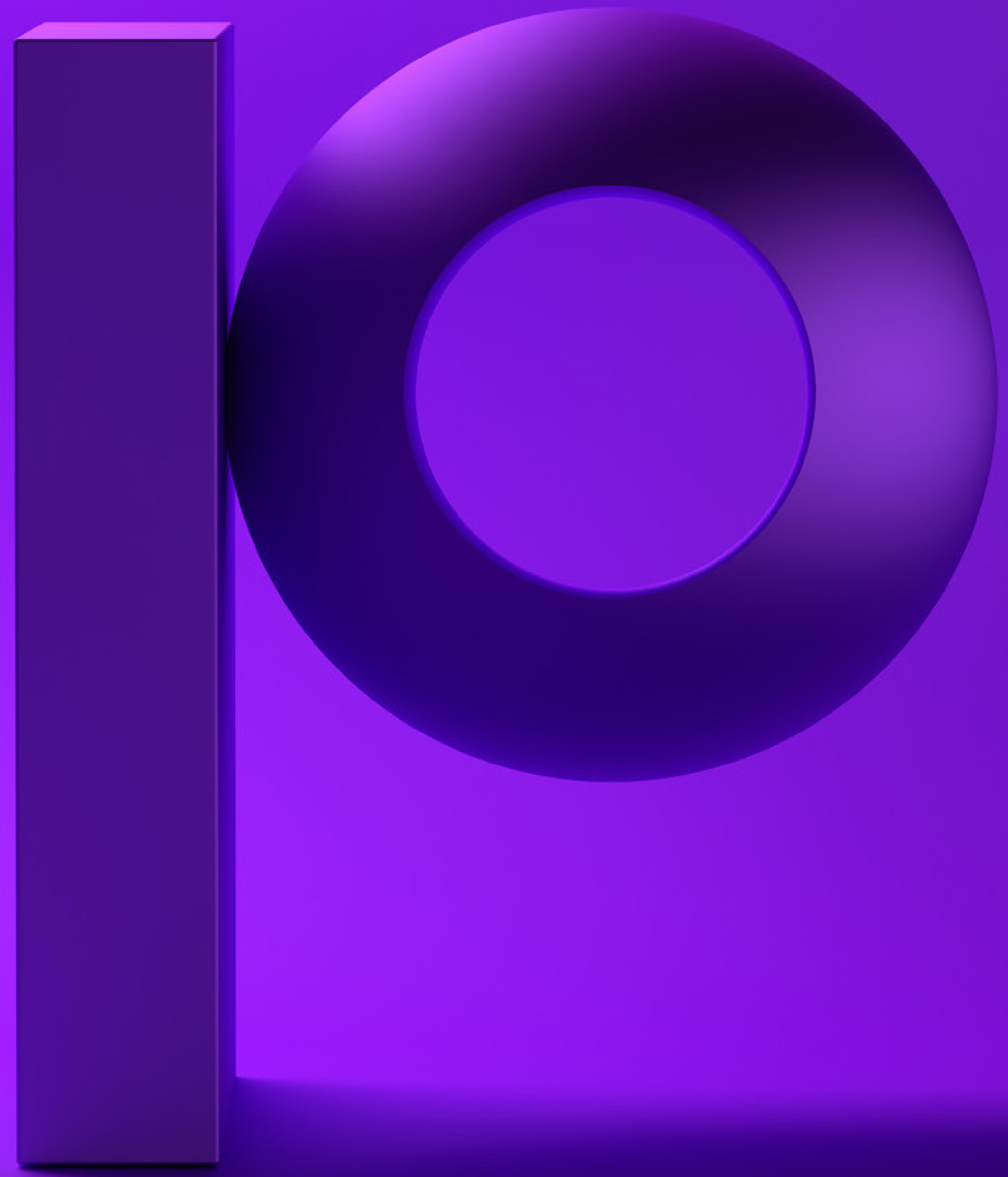
precisely

Passing Your Next Audit:

The Challenges of Properly Securing Your IBM i and Maintaining Compliance



Achieving a Secure IBM i - A Job That's Never Finished

Achieving optimal security on the IBM i isn't so much a destination as it is a journey that's marked by a continual series of efforts toward improvement. That's because security is never static - threats are constantly changing, new and expanded compliance regulations are being introduced, and there are new technologies and best practices to consider. On top of everything else, IBM i environments are in a constant state of flux resulting from changing user needs, new workloads, new interfaces to external protocols, and more. This dynamic situation creates numerous concerns for IT staff, security officers, and corporate management.

A recent survey by Precisely, of organizations with IBM i systems in their IT infrastructure, shows the impact that security and compliance have on IT priorities*:

- Security is the most frequently reported IT priority for the coming year
- 36% say security is their number one IT priority in the year ahead
- 70% say they are only somewhat confident or less in the effectiveness of their security program
- 25% say the growing complexity of regulations presents a challenge to ensuring security

In this eBook, we'll look at several specific security challenges commonly faced by staff at IBM i shops in their efforts to harden security and pass compliance audits. These challenges include enforcing security and compliance policies, defending against unauthorized access (particularly via open-source protocols), auditing and tracing suspicious activity, keeping sensitive data away from prying eyes, limiting powerful profiles, and more. In addition to presenting challenges, this eBook describes some of the technologies and best practices that can provide much needed solutions.

Challenge

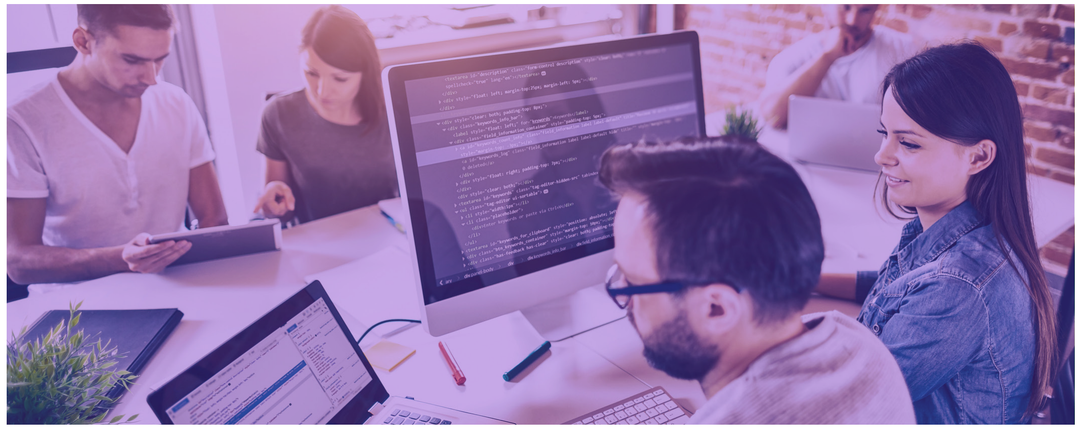
Continually monitor and enforce IBM i security in an environment of ever-changing internal security policies and compliance requirements

IT security initiatives have always been driven by the imperative to prevent the misuse, manipulation, corruption, and theft of valuable or sensitive information, but in recent years this has been compounded by the need for companies to meet everincreasing regulatory compliance requirements, whether from PCI DSS, SOX, HIPAA, GDPR, or numerous others.

The demands that come with meeting compliance regulations can be complex and challenging. First, is the process of defining internal security policies that specify how IT systems are to be secured so as to reduce the risk of security incidents and compliance violations. Next, these policies need to be implemented within the configurations of IT systems. Yet, what makes this endeavor particularly daunting in IBM i environments is that there are typically thousands of objects and configuration settings that have accrued over many years.

Finally, once object security is implemented, system administrators and security officers should regularly monitor the environment to ensure new objects and settings are properly secured and existing object-level authorities are not altered in ways that could cause unauthorized access.

Without the right tools and processes, making sure that system and object configurations are within compliance parameters can be enormously time-consuming - not to mention being prone to errors and oversights.



Solution

Tools that simplify the process of comparing IBM i system and object configurations to your organization's security policies while bringing exceptions to the attention of administrators and security officers

Starting with an innovative, template-based approach, security technologies from Precisely streamline the process of defining your corporate security policies as compliance definitions within IBM i environments. With your policies tightly tied to the configuration of objects and system settings, administrators and security officers can get notified through dashboards, alerts, and reports whenever system and object configurations are out of alignment with security policy definitions. Plus, additional reports can be produced in multiple formats that demonstrate to auditors and management that the system is operating within compliance definitions.

With real-time security and compliance monitoring of your system, administrators and security officers are able to respond quickly whenever a deviation from policy occurs. In fact, our technologies also make it possible to implement automated responses whenever system or object configurations differ from compliance definitions. These responses can include calling a custom program or sending a message to a data queue, message queue, SNMP trap, or syslog server.

Challenge

IBM i shops must contend with a wide range of security vulnerabilities caused by the proliferation of data-and-system-access methods, including open-source protocols

Traditional object-level security, built within the IBM i operating system, defines how user authorities can access designated objects. Years ago, simply managing object-level security might have been sufficient for protecting the IBM i, but today, relying only on this method is grossly insufficient given the many network protocols that must be secured, including FTP, ODBC, JDBC, OLE DB, DDM, DRDA, NetServer, etc. However, it is also insufficient to only protect against unauthorized access from these traditional network protocols. That's because PASE and new open-source protocols, such as JSON, Node.js, Python, Ruby, etc., are on the rise due to the influx of young techies who are introducing new technologies and innovative ways to integrate IT processes within IBM i shops. Open-source protocols can create discomfort for veteran IBM i administrators, who are often not aware of how these will impact IBM i environments, particularly when it comes to protecting against unauthorized access.

As if contending with network and open-source vulnerabilities weren't enough, the IBM i (and its valuable business data) is now firmly on the radar of hackers as evidenced by the first-ever presentation about IBM i at the DEF CON hacking conference in 2015.

When all of the above is combined with ever-changing regulations and the demands of auditors, enormous pressure is placed on administrators and security officers to proactively find vulnerabilities and implement the necessary protections.

Solution

Tools that comprehensively secure systems and data from any vector of unauthorized access

Exit points were created by IBM as a way to enhance object-level security for traditional network protocols on IBM i. But in order to utilize exit points, IT shops must implement exit programs that monitor, analyze, and restrict access via exit points. In fact, it is only through exit programs that it's possible to control all network activity and record a complete audit trail. Nonetheless, developing and managing exit programs can be a significant undertaking if done in-house. Furthermore, exit programs can negatively impact system performance if not designed correctly.

Precisely's advanced IBM i access-control solutions are built to streamline the job of protecting exit points with minimal impact on system performance. Our technologies go a step further by making it possible to protect against any open-source protocols through a dynamic, data-centric, rules-based approach. For instance, anytime a file is opened, regardless of the protocol that made the request, an exit program is invoked that provides or denies permission based on the file-access rules that you define. This data-centric approach provides a comprehensive way to protect against unauthorized access as it doesn't require administrators to know about — or find solutions for — each new open-source protocol that might affect their IBM i environments.

Challenge

Ensure only authorized users can view sensitive data

With dramatic instances of corporate hacking on the rise, organizations with business-critical applications on the IBM i are finding themselves increasingly in the crosshairs of hackers because of the valuable business data that often resides on these systems.

The first line of defense is to protect the IBM i against unauthorized access. But then, depending on its sensitivity, data may also need to be encrypted or otherwise rendered unreadable should first-line protections fail to stop unauthorized access or should someone inside the organization attempt to access sensitive data in an unauthorized manner. It's no surprise that a growing number of compliance regulations are forcing companies to harden their security in numerous ways, including through technologies that encrypt, mask, or scramble data. Most notable of these regulations is Requirement 3 of the PCI DSS requirements that define how credit card information is to be stored and protected by retailers and processing companies.

It's one thing to be required to encrypt or mask data, but it's something else entirely to implement the required technologies to accomplish this. For instance, with encryption there are algorithms to sort out, there is the need to encrypt data both at rest (stored on disk) and in motion (when sent to or from an external application or process), and there is the need to have a well-defined process that properly manages encryption/decryption keys.

Solution

Tools that make it easy to implement and manage the encryption, masking, or scrambling of sensitive data

IBM i security technologies from Precisely provide an easyto-use, comprehensive platform for implementing field-level encryption. Through a variety of algorithms, including AES 256, AES 192, AES 128, TDES 24, TDES 16, TDES 8, and DES, numeric or alphanumeric data can be encrypted at the field level in such a way that even users with powerful profiles will not be able to view the unencrypted data, including if accessed through journals.

With the ability to encrypt data at rest or in motion, our application independent encryption technologies can be implemented without incurring a large impact on performance and typically without requiring any changes to program source code or database file structures. In addition to field-level encryption, we also provide the ability to fully encrypt IFS documents and save files (*SAVF). And as an added benefit, your tape backups that contain files with encrypted fields, encrypted IFS documents, and encrypted save files are kept safe should those tapes end up in the wrong hands.

Precisely technologies also provide complete masking and scrambling capabilities. With field masking, full or partial masks can be applied to any database field, while field scrambling can be used on either alpha or numeric data, which is particularly beneficial to organizations that use live data when developing and testing applications.

Challenge

Quickly and accurately audit and trace any type of system or database activity on the IBM i that might be suspicious

When determining if user behavior on your system is suspicious and may possibly be causing fraud or theft, it is critical to document a complete picture of the activity. In fact, many compliance regulations require an unalterable logging process that captures a wide range of user activity and system events. Within IBM i environments, the types of events that should be logged include (but aren't limited to):

- **System events**
  - Object changes (system values, user profiles, authorization lists, etc.)
  - Access attempts (authentication and object access)
  - Powerful user activity (*ALLOBJ and *SECADM)
  - Real command-line activity of user profiles
  - Access to, or use of, sensitive objects (files, programs, menus, etc.)
- **Database events**
  - Changes made via programs from outside standard applications (SQL, DFU, etc.)
  - Modification to sensitive field values (credit limits, price lists, discount rates, etc.)

Many compliance regulations require an unalterable logging process that captures a wide range of user activity and system events

Solution

Utilize IBM i journals for auditing and tracing with special tools that make it easy to filter, read, and report the data

The IBM i journaling function is fully integrated within the operating system and, when activated, will log any system and user activity so that it can be reviewed in the event of suspicious activity on your system. Any IBM i shop that is serious about preventing fraud and theft, as well as meeting its compliance requirements, will have journaling enabled on its systems. Journals are reliable, they collect everything within their defined scope, and they cannot be falsified or otherwise manipulated by any user or process. Because of these qualities, journals are the one source that auditors trust when tracing security events within IBM i environments. In fact, journaling is required to provide a true segregation of duties between system administrators and auditors— again, because the data contained in journals can't be manipulated.

The comprehensive IBM i journal-reporting technologies from Precisely make it easy to search the massive amounts of data contained in journals as well as to decipher its cryptic information. Not only do our technologies help administrators and security officers quickly find the information they need, but we make it easy to turn this critical system and database change information into the kinds of meaningful, actionable reports that management and auditors demand.

Challenge

Gain control over powerful profiles and other risky user capabilities within IBM i environments

Powerful profiles with authorities such as *ALLOBJ, *SECADM, command-line access, and other potentially dangerous capabilities create a significant security exposure to organizations if improperly managed. In the hands of the wrong person, a powerful profile can cause significant damage, whether that damage is done intentionally or otherwise. This is why auditors (not to mention security best practices) require that powerful profiles be tightly controlled. But in many IBM i shops, these good intentions hold true only until a situation arises in which a user without sufficient authority needs to solve a critical problem or complete an important project. Before long, there is a slow proliferation of powerful profiles and capabilities among users, which is often followed by an auditor raising red flags, or worse, an incident in which significant damage occurs.

Without the right tools to manage powerful profiles and control the use of commands—as well as to closely audit all of the activity of powerful users—big headaches can be in store for administrators and security officers.

Solution

Tools that make it easy to manage elevated user authorities and command access through a rules-based process

Technologies from Precisely give administrators and security officers the ability to easily manage the process of temporarily granting elevated authority to users within tightly controlled parameters. And it does this while providing detailed audits of all activity performed by the user who has the elevated authority.

Administrators can provide higher authorities to selected users through a very granular, rules-based approach under either a "swap" or an "adopt" methodology. For instance, an administrator can give a user increased authority based on any combination of time duration, access to specific commands, and type of job, such as 5250, SQL scripting, etc.

Once the elevated authority is granted, all activity of the user is meticulously recorded, right down to the screens the user sees—whether or not any data was changed. Auditing is done via job logs, SQL statements, screen captures, and system and database journals (if enabled).

In addition, Precisely's security solutions make it possible to control where and how users are able to execute commands. Our technologies simplify the process of controlling command exit points through an innovative, rules-based approach that limits the use of commands to very specific parameters while closely auditing all command activity.

Challenge

Stay aware of all security vulnerabilities within your IBM i environment

You may implement all available technologies and best practices to properly secure your system and meet compliance requirements, but a comprehensive IT security program for IBM i also requires taking proactive steps to seek out and remove security vulnerabilities.

In fact, many compliance regulations such as PCI DSS and HIPAA require that companies execute a security risk assessment on an annual basis. But not all auditors understand the special security features of IBM i, and not all IBM i administrators have the necessary knowledge or time to conduct a rigorous security assessment. Besides, it is often a requirement (and a general best practice) that risk assessments are conducted by a person or process that's independent from those who manage or use the system.

Not all auditors understand the special security features of IBM i, and not all IBM i administrators have the necessary knowledge or time to conduct a rigorous security assessment.

Solution

Conduct an in-depth security risk assessment

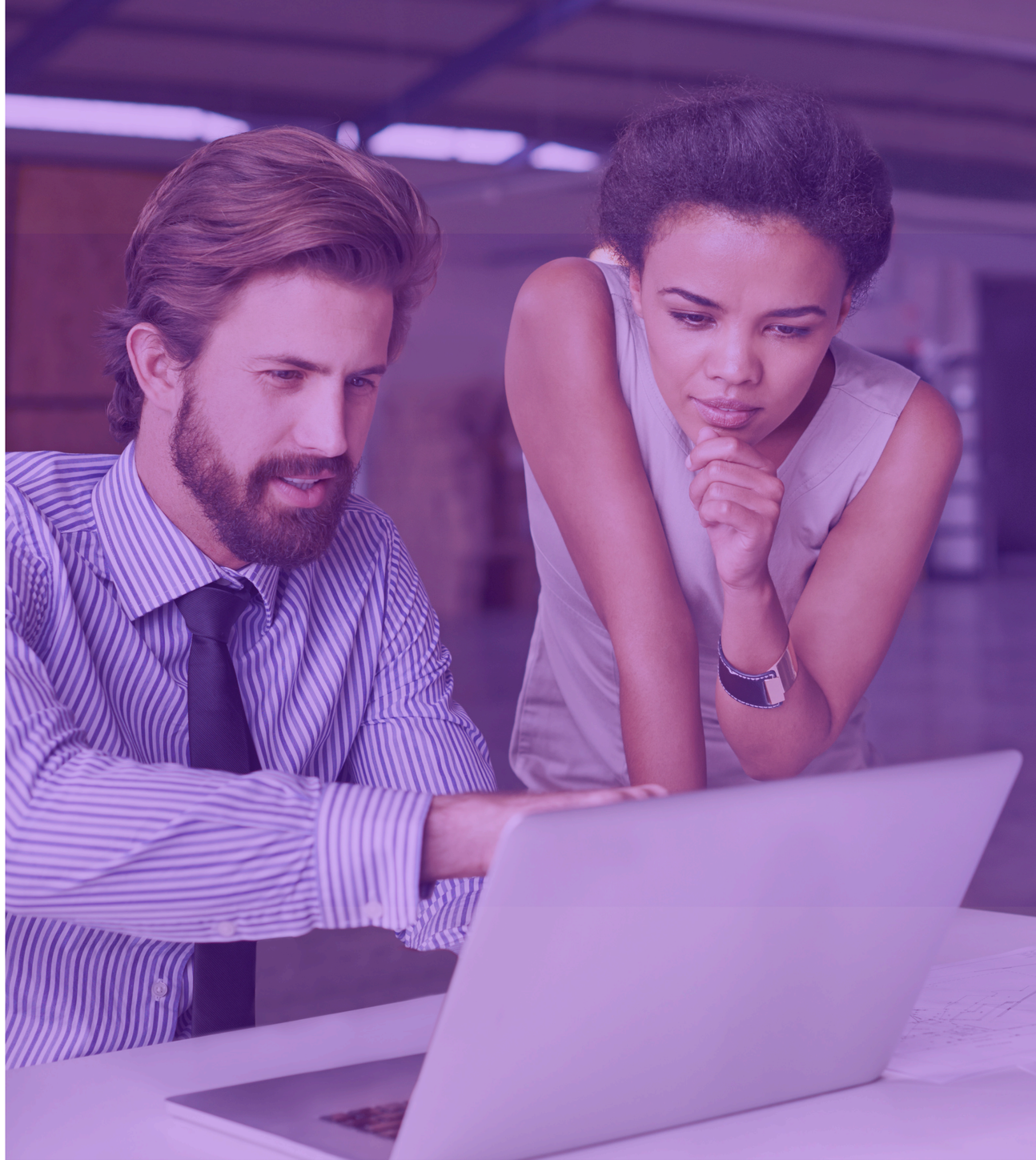
Security Risk Assessment Services from Precisely are designed to help system administrators, security officers, and management objectively identify potential security vulnerabilities within IBM i environments. Our security experts deeply analyze your IBM i, comparing system definitions with known security best practices and come back to you with a clear picture of your security vulnerabilities and specific recommendations for remediation. The reports you receive include a management summary that helps even non-technical administrators and managers understand the state of IBM i security while also providing a variety of detailed, actionable information that technical staff can use to address problem areas.

By utilizing Security Risk Assessment Services from Precisely, your company fulfills the important requirement of separation of duties between security auditing and risk assessment processes and the IT staff that manage your system.

Summary

Organizations that run business applications on IBM i must adequately secure their systems to meet compliance regulations. However, being in compliance doesn't mean your IBM i is fully secured. To achieve a security posture that is a real deterrent to theft or fraud—whether perpetrated by external or internal actors—a determined, consistent effort is required that combines the right mix of technologies, expertise, and best practices, all of which must be able to adapt to rapidly changing threats and regulations. The information presented in this eBook, although far from exhaustive, is intended to give you some insights in this direction.

Precisely is here to help. We've brought together best-in-class IBM i security solutions along with an outstanding team of experts in all aspects of IBM i security. In fact, a growing number of customers that use our security technologies choose to enlist our experts under a managed services arrangement to monitor and optimize their security. In addition to freeing staff to focus on other IT priorities, our managed services offerings help administrators and management rest easy, knowing that IBM i security is overseen by experts whose only job is to focus on this critical area of technology. Contact us to learn more about our different levels of managed services for IBM i security, which in addition to monitoring and optimization can include the execution of periodic security risk assessments and having our experts be available to work with your auditors as needed.



precisely

Precisely is a global leader in data integrity, providing accuracy and consistency in data for 12,000 customers in more than 100 countries, including 90 percent of the Fortune 100. Precisely enables companies to integrate, verify, locate, and enrich their data to power better business decisions. To learn more, visit www.precisely.com.

www.precisely.com