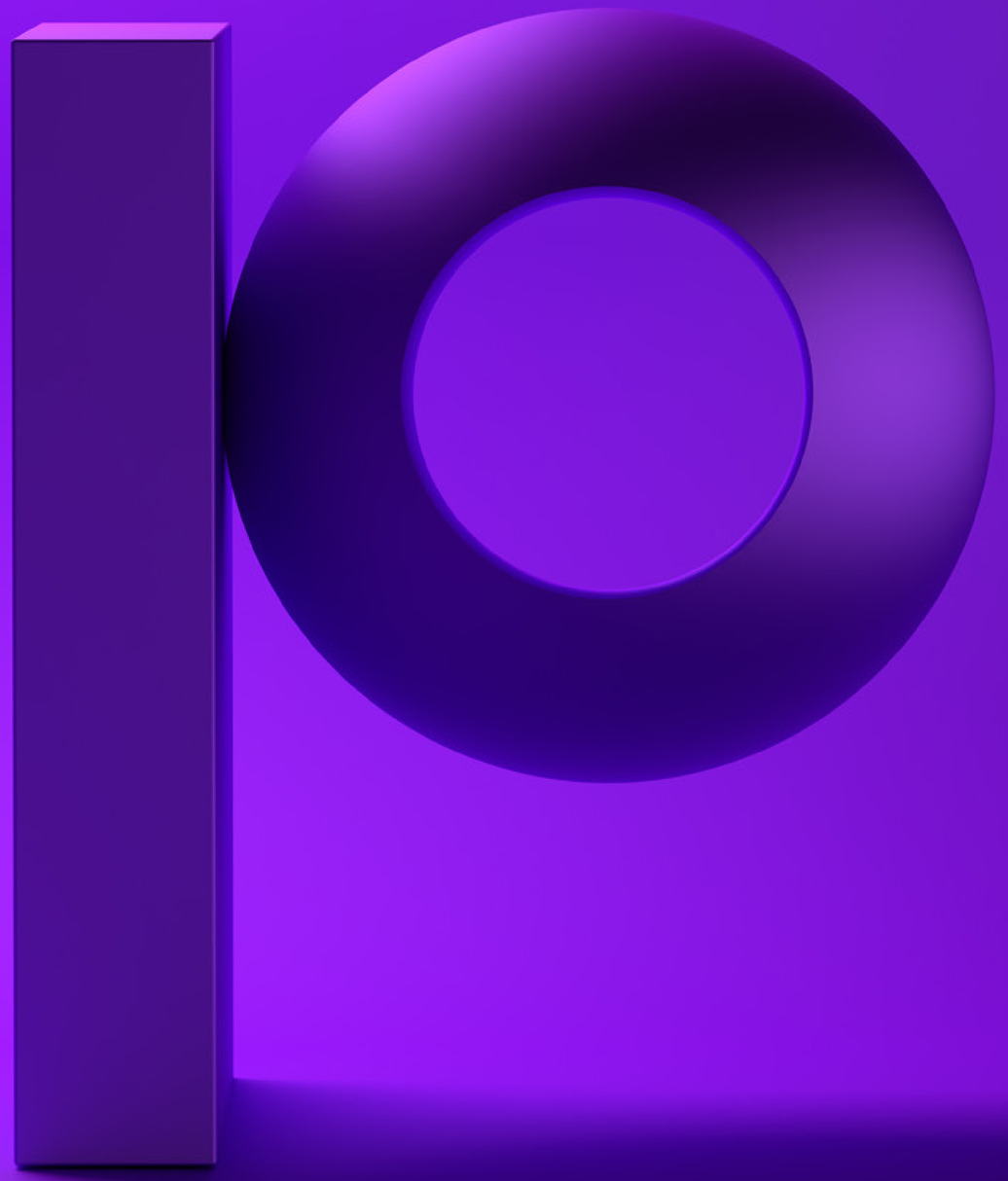
precisely

A Holistic Approach to Ransomware Protection for IBM i Systems

Integrate prevention, detection and recovery



Achieving Operational Resilience on IBM i

Maintaining robust operational resilience has always been a key goal in IT management. But it is no longer optional in a world where a tiny coding error within a commonly used utility app can result in global air traffic disruptions, nation-wide phone service outages, or snarled financial trading operations.

It should not be surprising to see the focus of new regulations shifting noticeably from data privacy and security rules such as GDPR, HIPAA and PCI DSS, toward more directly governing IT operations management. Recent examples include the SACA cyber security incident response and reporting regulation for U.S. infrastructure utilities and DORA, the EU's Digital Operations Resilience Act. And even more IT Ops-focused requirements are in development globally, many focusing on emerging risks related to AI systems, crypto currencies, and more.

So, what does all of this have to do with maintaining operational resilience on IBM i? With its gold-standard security capabilities and renowned reliability and uptime stats, isn't it enough to maintain journal logs and CDP backups and have HA/DR systems ready to go?

Sadly, the most honest answer is "No. It is not enough."

Anyone managing an IBM i environment can tell you that the platform is already highly connected to and interdependent with all other IT platforms and infrastructure. And the pace of that assimilation is only increasing. This reality only further confirms and intensifies the mandate to take a more comprehensive, multi-layered and highly integrated approach to achieving IBM i operations resilience.

Resilience Requires Data Protection... and Much More

At a minimum, maintaining resilience requires ensuring that your data is continuously protected against being damaged by malware or being locked up or exfiltrated by ransomware gangs. And that protection must extend beyond data that is in storage to include all your data, whenever and wherever it moves within and across systems or networks.

For example, given the current state of affairs, constant, ubiquitous application of anonymization techniques and strong, AES 256 encryption are needed to ensure that when (not if) your data is exfiltrated, ransomware demands and/or blackmail threats are rendered ineffective. Similarly, protecting your business against ransomware also requires implementing a well-considered set of additional security and operations analytics tools and solutions, and integrating them fully across IBM i and all other enterprise platforms and networks.

Ultimately, IBM i and overall IT resilience means that your organization is ready and able, 24/7, to respond effectively and rapidly to the inevitable. Confidently regaining control and bringing healthy systems back online under crisis conditions requires well planned, carefully orchestrated procedures that are informed and guided by a full understanding of the cause(s) and impact(s) of the event.

The bottom line is this: Resilience requires taking all possible precautions to Prevent data loss and corruption, vigilant and comprehensive monitoring to Detect any anomalies or indicators of compromise (IOCs) and being ready to rapidly and completely Recover from any incident, applying known-good data backups using well planned, tested and proven processes.

Prevent

Your organization is probably already doing a lot to protect your data from loss or corruption. For this discussion, we will assume that you are applying all of the key IBM i system and storage security features, especially those related to stringent management of elevated authorities.

In addition to securing your IBM i systems and storage, you have (hopefully!) been actively implementing all possible network related protections like multifactor authentication for IBM i user logon and storage access; Exit Point programs; and best practices like Zero Trust and logical and physical network segmentation and control.

Beyond these, in light of the growing frequency of ransomware attacks, if you have not already done so, it is also time to review and redouble your efforts with regard to applying strong, AES 256 encryption, building it into all of your data streams and data storage. It should be simply impossible for anyone to directly access and capture any of your data in the clear.

Having all of these measures in place provides you with good general data security. However, in order to respond effectively to the heightened expectations and requirements for IT and overall business resilience, there is still more which needs to be done.

Known-Good, Immutable Backup Data

Plans for recovery from a ransomware attack must assume that your systems are all 100% locked up and/or corrupted and will essentially require a bare-metal rebuild. Under those conditions, it is vital to have immediate and *guaranteed* access to effectively air-gapped, offline repositories of known-good, immutable system saves, FlashCopy snapshots and IBM i journals.

Thus, your first and most foundational step toward future-ready resilience capabilities is to develop and implement a full, structured set of processes for creating and securing those frequent, immutable backup files, along with their related file retention policies and controls. It is also essential that these processes also include consistent, programmatic auditing of recovery data files as they are created, to ensure that they are "known-good", useable and complete when your recovery plans are triggered. More on this to come later in this document.

Detect

The next aspect of resilience planning involves ensuring that your organization maintains the level of situational awareness and vigilance required to recognize and respond to today's more advanced and complex digital threats. Again, it is assumed that you already have a good foundation of security capabilities and procedures in place. So, the focus in this case is assessing and expanding those capabilities as needed to ensure that your IBM i security posture is as complete as possible and is also fully integrated with your enterprise-wide security operations.

Targeting IBM i

From the start, your security planning and management must be based upon the assumption that no matter what security methods and tools you deploy, at some point they will be defeated by human intelligence and nefarious creativity. And while it is totally valid to assume that your IBM i systems are not likely to be directly attacked, they are nonetheless being targeted from outside your organization and, potentially, by employees and other insiders with bad intentions.

The highest value that IBM i presents to ransomware gangs is as a point of ingress, a waypoint along a carefully planned path to their ultimate Wintel and open systems targets. The key bridge in this case is the connectivity between IBM i IFS and WinTel data storage. Specifically, from a "black-hat" systems surveillance perspective, IFS storage is as visible as any standard storage array, including having an assigned, and therefore targetable, IP address.

More broadly, any security weakness in any device or network connected to your overall IBM i environment can and will be exploited get inside your operations. So, it is vital to catalog, scrutinize, and actively manage everything that is in any way connected to your IBM i servers and SAN, including network or telephony devices, routers, VPN gateways, and anything that may possibly be running on backlevel firmware, especially any older, unsupported (EOL) devices.

Sec Ops and Artificial Intelligence

Returning to our earlier assumption that no matter how well you harden your IBM i-related environment, it must be assumed that it can and will be breached. So more must be done in order to detect and define any cyber threat as quickly and accurately as possible and to respond rapidly and effectively in order to thwart the attack, or to at least "limit the blast radius" of damage or data loss.

While IBM i security features create log files that provide highly detailed and traceable audit trails, countering modern cyber threats requires continuous and automated scanning of those logs using state of the art AI-powered security tools and deep, real-time integration with enterprise SEIM and overall IT SEC Ops.

Clearly, that integration will require a good bit of effort from a combined team of IBM i and SecOps team members to connect the logs and set up the required monitoring and integrated reporting. As a starting point, here are some of the most important elements of the IBM i audit layer to include in those efforts:

- Endpoint Telemetry
- Network Activity
- MFA Logs
- Exit Point Traffic
- IFS Object Changes
- CIS Benchmarks
- I/O Activity
- QAUDJRN
- IFS Object Journals
- Cloud Scanning
- FTP Endpoint File Scans
- Red Team Activity
- Remote CDP Journals
- Pen Testing

Recover

At the start of our discussion, we emphasized that resilience is completely dependent on having the data with which to rebuild your systems. The central strategy is therefore to have properly designed processes and known-good data files in hand, so that the situation can be addressed carefully and methodically... as fast as humanly possible.

With AI-enabled monitoring and alerting in place, you have a much better chance of identifying any Indicators of Compromise (IOCs) such as anomalous activity or processing on your systems, in short order. At that point, the real test of your resilience is how quickly and appropriately you can respond to the threat. While acknowledging that not every potential IOC identified will amount to a crisis situation, it is still vital that each one is addressed as quickly as possible.

The reason for this nervous-watchdog level of response is that today's cyber threats are not only proving to be stealthier and more cleverly executed, they are increasingly employing more advanced, AI-driven methods which do not need a human actor to guide their infiltration or to determine when to trigger their payloads. Essentially, even a small twitch should be enough to make the watchdog bark, or at least growl. And be it bark or growl, your response must still be immediate based on the assumption that you do not have the luxury of time.

With One Hand, Blindfolded

Clearly, there is also some risk involved in overreacting, acting too quickly or acting in a less-than-programmatic manner. This is especially true if and when an attack is clearly underway, and the pressure is on. Here is where the core tenet of the venerable ISO 9000 manufacturing quality standard applies: “Document what you do, then do what you documented.”

The classic proof of capability and unerring performance of a task is, as they say, to do it while blindfolded and with one hand tied behind your back, while someone else minds the stopwatch. This may sound a bit extreme until you experience a recovery from a major natural disaster or a ransomware attack.

The key to avoiding chaos and managing time pressures under such crisis conditions is to ensure that you and your team all know exactly what needs to be done to recover, by whom, and in what order. It also requires following a well thought out internal communications plan in order to avoid missteps and ensure proper sequencing and handoffs between IT teams (data management, networking, security etc.) as well as with other business operation leaders.

To that end, you should develop and document a complete, Recovery-focused Runbook. Note that this is not the same as your HA/DR switch/failover Runbook. This Runbook needs to include absolutely everything related to ransomware recovery/resilience procedures throughout your enterprise, including all your CDP and data storage processes.

When creating your Recovery Run Book, be sure that it clearly states the names of your recovery task owners, with provisions for delegation of responsibility and authority to account for absent staff.

The exact flow and details of your Recovery Run Book will, of course, be unique to your IBM i and overall IT environments. But it should definitely be designed to accommodate different levels of threat severity. Be sure to cover the who, what, when and how of:

- Notifications, roles and responsibilities
- Analysis of cause and determination of potential impacts (“Blast Radius”)
- The proper sequence of isolations, lock-downs, shut-downs (including network and storage devices)
- The communications plan for non-IT business leadership teams and employees

The Antidote for Cyber-Snakebites

When facing the worst-case scenario of a "successful" ransomware attack, your good, immutable data backup files are not just your insurance policy, they are the only known antidote. Maintaining a continuously updated set of good, immutable recovery data in highly secure, isolated storage is the minimum standard for IBM i resilience.

Providing a fully detailed guide for meeting this standard is beyond the scope of our discussion here. However, to help you frame your plans for ensuring effective IBM i resilience, we offer some key recommendations:

Immutable Recovery Data Files

The essential resources for resilience are regular and frequent SAVEs, FlashCopy Snapshots, and iOS Journal Receivers. Each of these has advantages and disadvantages for IBM i recovery, so the best advice is to ensure you have all three secured and available.

- **SAVEs**
  - Allow for the most granular restoration (file, library level)
  - Not suitable for IFS Directories
  - Require longer time to complete Restore
- **FlashCopy / Snapshot**
  - Usually faster to Restore than full SAVEs
  - Suitable for IFS Directories and Stream files
  - Completeness/Usability of data can be uncertain
  - Must be combined with Journal Receiver restore/application
- **Journal Receivers**
  - Natively Immutable
  - Application requires alignment with Save/Snapshot timestamp
  - Require Logical Replication software to apply

FlashCopy/Snapshot File Quality Control

The completeness, and therefore, useability of a FlashCopy/Snapshot can vary widely. Assessment of these files should be done routinely, at the time they are taken, to avoid an incomplete or failed restore. Best practice is to use one of the available applications for automated Snapshot evaluation and reporting in conjunction with administrative controls for archiving.

Determination of point of failure/corruption and/or point of malware ingress

While acknowledging that the inherent complexity in methods and timing used by malware and ransomware attacks can make it difficult, in order to avoid reintroducing the attack vector to your systems, it is vital to identify with as much certainty as possible the point in time at which your systems became compromised.

Note: Being able to conduct deep analysis into the timing and impacts of an attack is perhaps the most valuable advantage of integrating IBM i into AI-powered SecOps.

Protect your immutable recovery files while applying them

After successful system recovery, those files are still your current recovery set. Depending upon the nature of the original corruption (root cause), and the possibility that it was inadvertently reintroduced during system restoration, it is possible to have a repeat event.

Your recovery process must also ensure that you maintain regulatory compliant data

Your immutable recovery files need to be applied fully and methodically, not only to result in accurate, useable data on your restored systems, but to ensure that the restored data conforms to all regulatory requirements for retention and auditability.

This becomes very important in case a regulatory audit months or even years later uncovers data inconsistency or gaps in data lineage that are traceable back to the timeframe of a recovery event. The archive of the files you used for recovery is your resource for responding to the inquiry, and for correcting the issue, or at least proving due diligence during the restore process.

Let Precisely Help You Achieve Enterprise Resilience

Regulations mandating demonstrated IT resilience capabilities are coming into force now, and others are expected in the near future. Achieving overall IT and operational resilience for your multi-platform, hybrid cloud and on-premise enterprise requires a multi-faceted, multi-layered approach, one that fully integrates all the powerful security and data protection capabilities of your IBM i platform with those protecting your other systems and networks.

Precisely's Assure HA, Assure Security, and Ironstream solutions can provide the most complete and powerful capabilities available for achieving IBM i resilience, and are engineered for full, flexible, and seamless integration your enterprise SIEM and operations analytics platforms.

In addition to the market's most complete and trusted, journal-powered switching and failover capabilities, Assure solutions provide IBM i access control; elevated authority management; multi-factor authentication; alerting and reporting on system and database activity; AES-256 encryption, tokenization, and anonymization; secure file transfer capabilities; and much more.

Contact us to learn more about how Precisely can help you achieve comprehensive, enterprise-wide IT resilience.

precisely

About Precisely

As a global leader in data integrity, Precisely ensures that your data is accurate, consistent, and contextual. Our portfolio, including the Precisely Data Integrity Suite, helps integrate your data, improve data quality, govern data usage, geocode and analyze location data, and enrich it with complementary datasets for confident business decisions. Over 12,000 organizations in more than 100 countries, including 93 of the Fortune 100, trust Precisely software, data, and strategy services to power AI, automation, and analytics initiatives. Learn more at www.precisely.com

www.precisely.com