WHITE PAPER

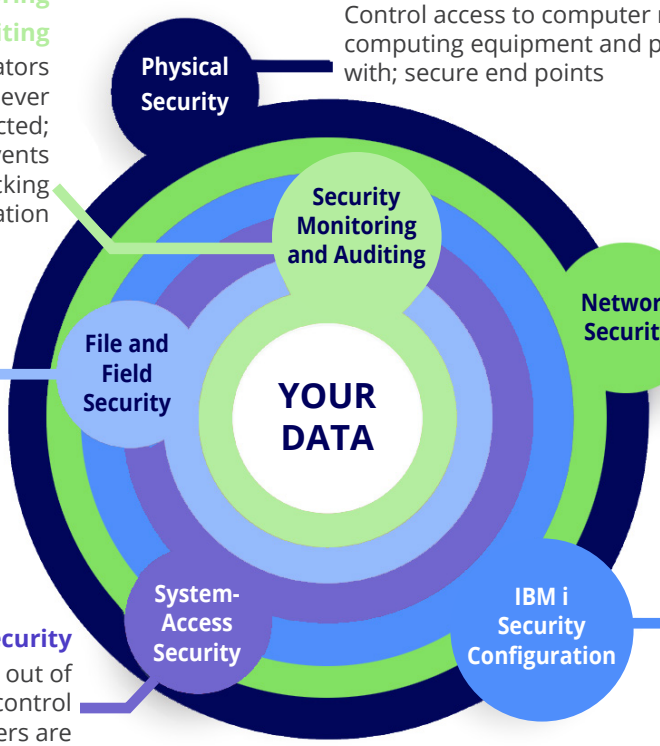
The Essential Layers of IBM i Security

Why a Comprehensive Protection of Systems and Data Requires Multiple Lines of Defense

Introduction

The increased frequency of high-profile breaches and the corresponding rise of new and expanded regulatory compliance requirements is putting enormous pressure on IT departments to assure their corporate executives that business-critical systems and data are secure. One particular statistic from a recently conducted Syncsort survey of IT professionals is revealing in that 69% of respondents said they were only "somewhat confident" (or worse) in the effectiveness of their company's IT security program. Given today's rapidly evolving security threats, even being "somewhat confident" doesn't cut it.

Improving confidence in one's IT security posture requires a solid understanding of all potential vulnerabilities as well as the most effective best practices and technologies in order to minimize the possibility of a breach. To help, Syncsort has created this white paper as a roadmap, grouping together important security best practices and technologies into six primary categories or "layers." These layers cover physical devices, networks, configuration of the IBM i OS, access to systems, protection of data at the file and field level, and monitoring and auditing of systems. The reason it's particularly helpful to view these security categories as "layers" is that, to some extent, each category overlaps with the others to provide multiple lines of defense. In other words, should one security layer be somehow compromised, there's a good chance that another layer will thwart a would-be intruder. The six layers of IBM i security are summarized in the following diagram and are detailed in the remainder of this white paper.



1) Physical Security
Control access to computer rooms and data centers; ensure computing equipment and peripherals cannot be tampered with; secure end points

2) Network Security
Implement intrusion prevention and detection technologies; group and protect related resources within network segments; encrypt network traffic

3) IBM i Security Configuration
Properly configure necessary security settings within the IBM i OS; keep the OS and PTFs up to date; closely manage user profiles

4) System-Access Security
Keep unauthorized users out of your IBM i; maintain tight control over what authorized users are able to do once logged in

5) File and Field Security
Ensure sensitive data cannot be seen by unauthorized individuals, whether internal or external

6) Security Monitoring and Auditing
Automatically alert administrators and security officers whenever suspicious activity is detected; log all security-related events for the purposes of tracking and documentation

Physical Security

More than just controlling access to computer rooms and data centers, a thorough physical security plan requires, among other things, that computing equipment be protected from theft, misuse, and intentional or accidental tampering.

- Servers and storage devices — Lock into place all servers and storage devices, lock front-panel covers to prevent intentional or accidental changes, and secure power and other cabling to prevent easy disconnection.

- Network devices — Lock into place physical firewalls, routers, switches, and other network devices; ensure power and other cabling can't be easily disconnected; watch for unauthorized configuration changes to network equipment, including covert installation of "sniffing" equipment; and use proper encryption for wireless networks (WPA, WPA2, etc.).

- **Peripheral devices** — Keep within secure areas all printers and fax machines that output sensitive information. Make sure employees who do have access to this output are properly trained in how to prevent it from being seen by unauthorized personnel. Regulations such as HIPAA, GDPR, and others require that sensitive information be secured not only within databases but also when it appears on printed output.

- **End-point devices** — Educate employees on how to safely use desktops, laptops, and mobile devices, including taking care that these devices aren't lost or stolen. If a device, however, is lost, stolen, or simply repurposed, IT staff needs the ability to locally or remotely execute a secure-wipe process. Of course, end-point devices need to be kept up to date with anti-virus, anti-malware, and anti-ransomware protection.

Network Security

The networks to which an IBM i is connected must be carefully secured, and if any of these networks are connected to the Internet, extra vigilance is required as Internet-connected networks often see thousands of access attempts each day by bots, sniffers, and hackers.

- **Firewalls** — By examining the flow of data entering a network, firewalls prevent unauthorized traffic by allowing only network traffic that meets predefined firewall rules.

- **Intrusion-detection system (IDS) and intrusion-prevention system (IPS)** — These technologies go beyond traditional firewall capabilities by analyzing traffic within the network itself for suspicious patterns of activity and then triggering alerts when such activity is detected. IPS goes a step further than IDS by acting to prevent the suspicious activity from affecting the network.

- **Network segmentation** — A network-security best practice is to avoid putting all IT assets together within a single network. By grouping together within each network only the systems and components that are related to one or more specific applications, only those assets would be compromised should a breach occur.

- **Encryption of network data** — Any data that is sent across a network must be encrypted to prevent passwords and other sensitive information from being read "in the clear." This applies to any application that utilizes sockets (a secure socket must be used), web server applications, and any client/server application such as ODBC, JDBC, FTP, etc. Transport-layer security (TLS) is the industry-accepted network protocol that supports encryption; however, the TLS version must be 1.2 or higher, and currently accepted ciphers (encryption algorithms) must be used along with the acceptable TLS version.

IBM i Security Configuration

Foundational to sound IBM i security is the proper configuration of the IBM i OS and related resources, as well as keeping OS versions and PTFs up to date.

- **System values settings** — The QSECURITY system value that is used to specify the security level of the OS must be set to 40 or 50. Security levels 40 and 50 activate system-integrity protection for your IBM i, which includes object-domain checking, parameter validation, and object-hardware storage protection. Levels 40 and 50 also prevent direct access to objects, which means any user-written programs are required to utilize system interfaces (commands and APIs) in order to gain access to objects. It is also important to decide whether to enable QALWOBJRST, QFRCCVNRST, QVFYOBJRST, and other system values related to integrity and security.

- **IBM i server-configuration settings** — There are numerous servers on IBM i that allow a client system to connect over a network. Examples include FTP, TELNET, ODBC, JDBC, DRDA, the sign-on server, and many others. Starting all servers by default on an IBM i unnecessarily opens "doors" into the system, thus increasing security risks. Be sure to review all IBM i servers and deactivate any that aren't needed.

- **Controlling access to System Service Tools (SST)** — Many SST capabilities provide significant access to data; for instance, network trace tools can provide a view of data flowing over a network. Because of this, care should be taken when giving users SST access.

- **User authority settings** — Many companies unnecessarily have users with powerful profiles that include *SECADM authority, *ALLOBJ authority, command-line access, and other potentially dangerous capabilities. A best practice that stops the spread of powerful profiles is to assign limited privileges to the majority of user profiles and then, on a case-by-case basis, temporarily grant selected users the authority they need to do a particular task. Third-party solutions make it easier for administrators, security officers, and end users to temporarily obtain elevated privileges as required. In addition, these third-party solutions log all actions taken once a user has the temporarily elevated authority.

- **Staying current on OS releases and PTFs** — Running older releases of the IBM i OS can open a security risk within an enterprise. A particular risk comes from open-source packages that are no longer supported by the open-source community but that run on systems with older IBM i OS release levels. These include Java, OpenSSL/SSH, Samba, Lotus products, web and application servers, and more. Be sure to subscribe to IBM's security bulletins and tech notes for IBM i to keep informed about all known security issues and their corresponding PTFs.

System-Access Security

The strategies and technologies associated with this layer of protection help keep unauthorized people out of IBM i environments while maintaining tight control over what authorized users are able to do once logged in.

- **Password management** — Weak passwords and dormant user profiles pose a significant security vulnerability. To counter this, it's important to regularly review the validity of user profiles as well as to activate the QPWD* system values that require strong passwords. In addition, using third-party password-self-service tools helps administrators audit password-reset activities. Finally, it's important to keep in mind that although passwords are well-protected on the IBM i, the hashed passwords saved to backup media by SAVSYS or SAVSECDTA operations are subject to brute-force attack if that backup media is not encrypted, and it is lost or stolen.

- **Multi-factor authentication** — In instances where users need to access IBM i environments containing especially sensitive data, third-party technologies can be implemented that require two or more identifying factors from users before access is granted. In addition to being used to control access to systems, multi-factor authentication solutions can typically be implemented via API calls to control access to specific databases, individual files, or even commands.

- **Network-access control** — Unauthorized access via sockets and network protocols (e.g., ODBC, FTP, DRDA, etc.) can be prevented through the use of rules-based exit programs that cover network and socket exit points. Because exit programs can be difficult to create and maintain, many shops choose to utilize third-party solutions that significantly streamline these tasks and provide the ability to trigger alerts should suspicious activity be detected.

- **Command control** — In addition to normal IBM i OS object-security controls, third-party solutions provide rules-based exit programs (trigged by command-specific exit points) that give administrators a more granular approach to locking down commands.

File and Field Security

Numerous regulations require companies in various industries to protect personally identifiable information (PII), personal health information (PHI), personal credit card information, and other sensitive data from being exposed should a breach occur. The following strategies and technologies are key to protecting files and data on the IBM i:

- **Object-level authority management** — For any file (*FILE or *STMF) containing sensitive data, it is critical that the authority designation is set to PUBLIC (*EXCLUDE). Once set, designated users can then be given specific authority to access these files through private authority or via application techniques that inherit additional authority, such as the use of program-adopted authority or profile swapping.

- **Row and Column Access Control (RCAC)** — Included with Db2 beginning with 7.2 of the IBM i OS, RCAC provides the ability to prevent selected users from viewing specified rows in a file and/or data in particular columns. For example, accounting staff should only be able to see rows in a file where the Department field equals "Accounting," or only select managers should be able to see the Salary column within a file. Note that RCAC cannot be used for IFS stream files.

- **File-access protection** — Building upon object-level authority management, various exit points can be used with rules-based exit programs to further control access to files in very specific ways; for instance, a particular file may only be accessed or a particular command may only be used during specific days or hours. Third-party solutions streamline the creation and management of these kinds of exit programs.

- **Encryption** — By combining one or more publicly available algorithms with a proprietary encryption key, human-readable data is transformed into unreadable "ciphertext." When the encrypted data needs to be decrypted for permitted users, the same encryption key is used. Encryption requires the careful management of encryption keys to ensure they don't fall into the wrong hands.

    - **Data at rest** — Third-party encryption solutions can encrypt sensitive data on the IBM i—such as credit card numbers—at the field level within databases. Technologies are also available that encrypt backup media and disk drives.

    - **Data in motion** — As described in the earlier section about the Network Security layer, TLS 1.2 or greater must be used to encrypt application data sent across networks. In addition, when entire files containing sensitive information need to be sent between systems or entities via FTP, they should always be encrypted, both during transit and when transfer files reside within send/receive staging areas. Secure file transfer processes are typically done with third-party solutions as they provide strong algorithms, sound encryption-key-management processes, and a variety of features that streamline and automate file transfer processes.

- **Tokenization of field data** — An alternative method of shielding sensitive data within applications and on printouts is to replace this data with non-sensitive substitute values called tokens. Third-party tokenization solutions utilize a database called a token vault (residing on a different server) to store both the sensitive data and information about the relationship between it and its replacement token. Because tokenization separates sensitive data from production databases via the token vault, the risk of sensitive data being exposed is significantly reduced should the production database be breached. Tokenization is often used to replace credit card numbers, social security numbers, and other personally identifiable information.

- **Anonymization** — Although similar to tokenization solutions, third-party anonymization solutions differ by eliminating the use of a token vault, thus permanently replacing sensitive data with a substitute value and making the original data unrecoverable. Anonymization is best utilized when production data is needed for development or test environments.

Security Monitoring and Auditing

While all of the previous layers of security address prevention, this security layer focuses on implementing functions that log security-related events for the purposes of tracking, documentation, and to automatically alert administrators and security officers whenever suspicious activity is detected.

- **System-audit journaling** — When properly activated and managed, the system-auditing functions of IBM i OS provide the ability to monitor and track system, object, and security configuration changes. These functions are controlled by the QAUD* system values and the CHGOBJAUD, CHGAUD, and CHGUSRAUD commands. When auditing is activated, audit records are generated and written to the QAUDJRN system-audit journal for those events selected for audit. More about system-audit journaling can be found in chapter 9 of the IBM Security Reference guide, located within the IBM i Knowledge Center.

- **File journaling** — Another important aspect of auditing is the ability of file journaling to track and monitor any changes made to sensitive data stored in either Db2 (*FILE) or stream file (*STMF) objects. With file journaling activated, whenever users or applications make a change to data within the designated files, a journal entry is written to record the change. The combination of system-audit journaling and file journaling can provide a complete audit trail of file-access and data-change activity.

- **Monitoring database-read activity** — In situations where it is important for administrators and security officers to know if a user accessed and viewed particularly sensitive data—regardless if the data was changed—third-party technologies exist that can record these activities, complete with a snapshot showing the precise data the user viewed.

- **Analyze and report on journaled information and generate alerts** — Once journaling is activated, it is important to have the ability to search for specific events, create reports, and set up alerts. Because information captured by journaling is recorded in a cryptic format, third-party solutions exist that make these important tasks significantly easier.

- **Save journaled data for compliance** — All logged information from both the system-audit journal and file journaling is kept within objects called journal receivers, which must be regularly saved and archived in a secure location. In the event a past security event needs to be investigated as part of an audit or otherwise, the data contained in these journal receivers will be essential. In addition, some regulations require companies to save system logs (in this case, journal receivers) for multiple years.

- **Forward journaled data to a SIEM solution** — For companies that utilize a security information and event management (SIEM) solution, third-party tools are available that filter and format journaled data for integration with a SIEM.

Syncsort Can Help

With proven security solutions for IBM i and a deep bench of experts whose focus is to stay up to date on security vulnerabilities, best practices, and mitigation technologies, Syncsort is here to help you build and optimize your own layers of IBM i security.

Syncsort Security Software for IBM i

Fortify your system-access security, file and field security, and security monitoring and auditing with our best-in-class software solutions that cover:

- Network-access, database-access, and command-access control
- Encryption, tokenization, and anonymization
- Secure file transfer
- Elevated-authority management
- Multi-factor authentication
- System and database monitoring and reporting
- Model-based compliance management
- SIEM integration
- And more

Syncsort also offers solutions and services for AIX, Windows, and Linux that address security and compliance-auditing needs.

Syncsort Professional Services for IBM i

Our security experts are here to assist your team in reinforcing your layers of IBM i security in numerous ways:

- Perform in-depth, periodic risk assessments on your IBM i environments. Using detailed findings from the assessments, we'll sit down with your IT and compliance managers to help formulate and implement a plan for remediating discovered vulnerabilities.
- Provide managed-security services that give your company dedicated IBM i security experts who, depending on the level of service chosen, regularly check security configurations, deliver status reports, monitor systems 24x7 for security events, adjust security configurations, and more.
- Assist your team during compliance or security audits by generating reports required by your auditors.
- Ensure a successful implementation of Syncsort security technologies and provide all needed training.

To learn more about all of our security products and services, visit **www.syncsort.com/assure**.

About Syncsort

Syncsort is the global leader in Big Iron to Big Data software. We organize data everywhere to keep the world working – the same data that powers machine learning, AI and predictive analytics. We use our decades of experience so that more than 7,000 customers, including 84 of the Fortune 100, can quickly extract value from their critical data anytime, anywhere. Our products provide a simple way to optimize, integrate, assure and advance data, helping to solve for the present and prepare for the future. Learn more at syncsort.com.

syncsort